NAVIGATING *the* CYBERSECURITY STORM

A Guide for Directors and Officers

BY PAUL A. FERRILLO

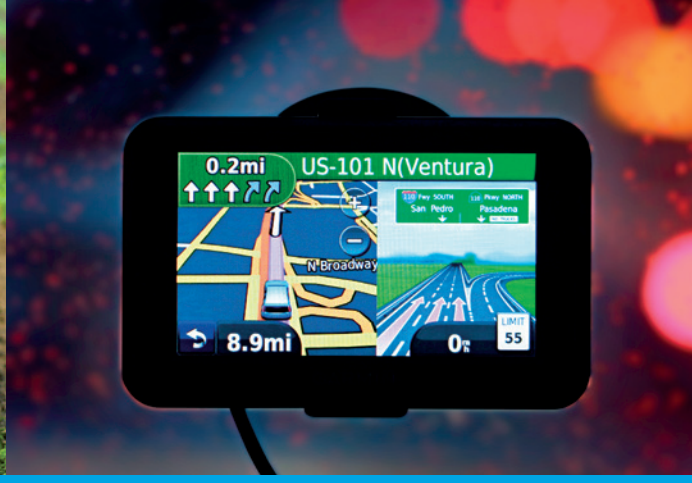
EDITED BY BILL BROWN

published by Advisen Transforming • Insurance™

sponsored by K2 Intelligence Investigations · Compliance Solutions · Cyber Defense

sponsored by AIG

To use the information contained in this book for a greater purpose or application, contact Paul A. Ferrillo via Paul.Ferrillo@weil.com



Is your company protected from the Internet of Risk℠?

With CyberEdge® cyber insurance solutions you can enjoy the Business Opportunity of Things.

20 billion objects are connected to the Internet, what everyone is calling the Internet of Things. This hyperconnectivity opens the door both to the future of things, and to greater network vulnerabilities. CyberEdge end-to-end cyber risk management solutions are designed to protect your company from this new level of risk. So that you can turn the Internet of Things into the next big business opportunity. To learn more and download the free CyberEdge Mobile App, visit www.AIG.com/CyberEdge

AIG®

Bring on tomorrow®

ABOUT PAUL A. FERRILLO

Paul Ferrillo is counsel in Weil's Litigation Department, where he focuses on complex securities and business litigation, and internal investigations. He also is part of Weil's Cybersecurity, Data Privacy & Information Management practice, where he focuses primarily on cybersecurity corporate governance issues, and assists clients with governance, disclosure, and regulatory matters relating to their cybersecurity postures and the regulatory requirements which govern them.

Mr. Ferrillo has substantial experience in the representation of public companies and their directors and officers in shareholder class and derivative actions, as well as in internal investigations. In particular, Mr. Ferrillo has coordinated numerous internal investigations on behalf of audit committees and special committees, and handled the defense of several significant securities class actions alleging accounting irregularities and/or financial fraud.

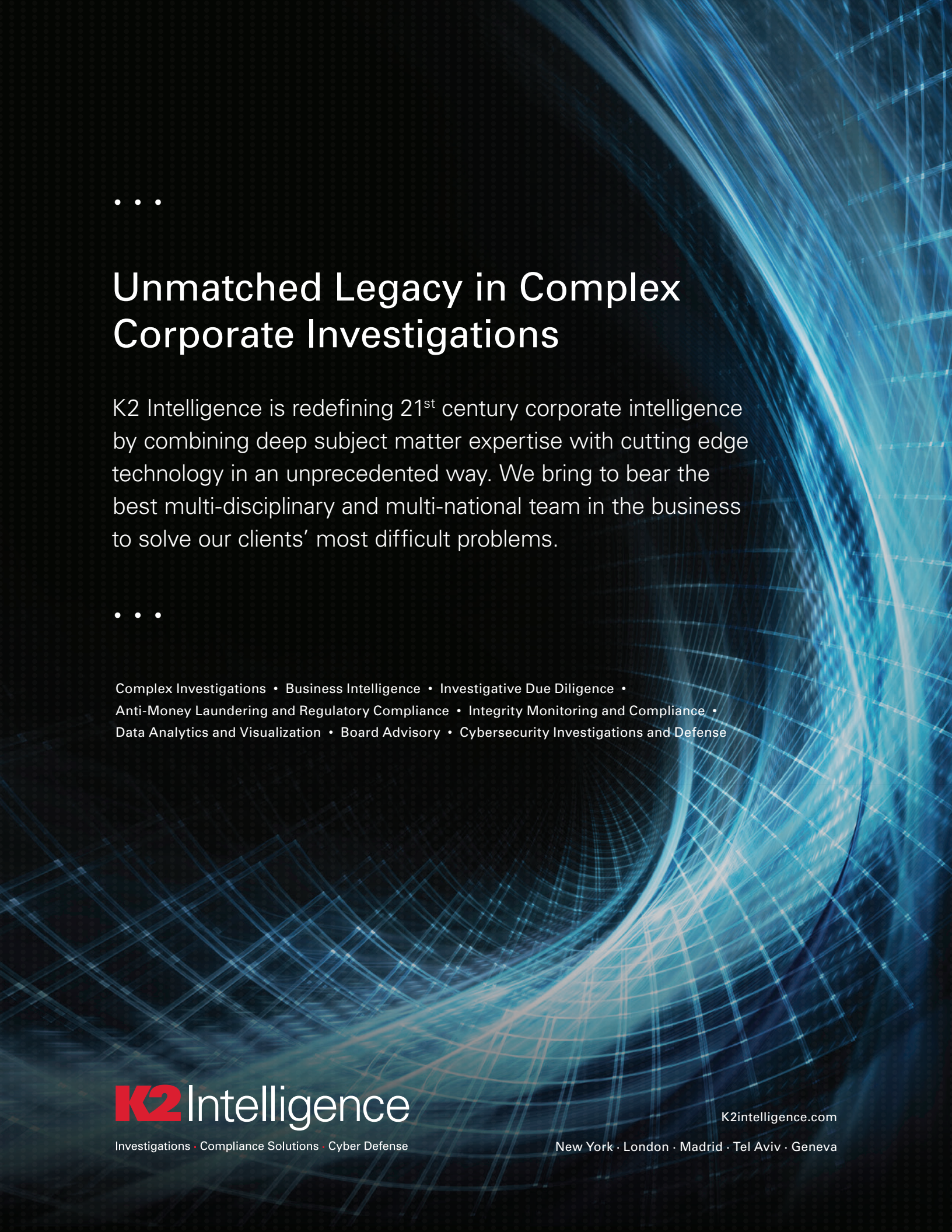
Mr. Ferrillo has represented companies in a wide range of industries, including retail, apparel, insurance, financial services, energy, oil and gas, and real estate.

Mr. Ferrillo also regularly counsels clients in the growing field of cybersecurity corporate governance, which is an increasingly important part of a Board's enterprise risk management function. Mr. Ferrillo also counsels clients on cyber governance best practices (using as a base the National Institute of Standards and Technology cybersecurity framework, which was announced on February 14, 2014), third-party vendor due diligence issues, cybersecurity regulatory compliance issues for Private Equity firms, Hedge Funds, and Financial Institutions that have been promulgated by the SEC, FINRA, the FTC, and the FDIC/OCC, the preparation and practicing of cybersecurity incident response plans, as well as evaluating and procuring cyber liability insurance to protect against losses suffered by Companies as a result the theft of consumer or personally identifiable information, or as a result of the destruction of servers and corporate infrastructure.

Outside of his D&O insurance practice, Mr. Ferrillo is a prolific writer, speaker, and commentator on a wide range of subjects. He is a frequent contributor of articles concerning securities, cybersecurity, corporate governance, and accounting fraud issues to the New York Law Journal, D&O Diary, Harvard Law School's Forum on Corporate Governance and Financial Regulation, and other national publications and forums, and is a frequent speaker on securities law, corporate governance, and directors' and officers' liability insurance issues for the ALI-ABA, the New York State Bar Association, the American Conference Institute, NACD, and the Directors' Roundtable. Mr. Ferrillo also is a co-editor of and contributor to *The 10b-5 Guide*, Weil's annual review of securities fraud litigation in the United States.

This book is provided "as is," with all faults, without warranties of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Paul.Ferrillo@weil.com | (212) 310-8372 Direct


Unmatched Legacy in Complex Corporate Investigations
K2 Intelligence is redefining 21st century corporate intelligence by combining deep subject matter expertise with cutting edge technology in an unprecedented way. We bring to bear the best multi-disciplinary and multi-national team in the business to solve our clients' most difficult problems.
Complex Investigations • Business Intelligence • Investigative Due Diligence • Anti-Money Laundering and Regulatory Compliance • Integrity Monitoring and Compliance • Data Analytics and Visualization • Board Advisory • Cybersecurity Investigations and Defense
K2 Intelligence
Investigations · Compliance Solutions · Cyber Defense
K2intelligence.com
New York · London · Madrid · Tel Aviv · Geneva

To my beautiful and courageous wife Patricia:
you are my rock, my Northstar, my everything.
Thank you for supporting me always.

— Paul

AUTHOR'S NOTE:

This book could not have come about without the help, support and guidance of so many people and firms, who I want to thank. First, my editor, Bill Brown, whose wisdom is well beyond mine, and who spent countless hours with me on drafts, and edits, and more drafts and edits. Jeff Cohen, from Advisen, who always believed in me and the book from Day One. Several partners at Weil Gotshal & Manges, LLP gave me an infinite amount of support and guidance, most especially Michael Epstein and Randi Singer (Randi of course, helping me with several chapters, including her excellent work on privacy). There are others to thank: K2 Intelligence (Austin Berglas), PwC (David Burg), Mandiant (Kevin Mandia), Levick Communications (Richard Levick), and countless other firms whose guidance and statistics I relied upon to help educate the readers on all that is going on in the cyber ecosystem. And thanks especially to John Doyle, Robert Schimek and Tracie Grella at the American International Group, Inc. - your support throughout the years has been invaluable, and most appreciated.

FOREWORD

As my close friends and family know, I am a big fan of Marvel Comics, and a huge fan of the Avengers series. In fact, one of my wife's cousins calls me Director Nick Fury (the boss of the Avengers). He's the guy who keeps his one good eye on everything and everybody. Always three steps ahead. Never behind. Always fighting for good. When thinking about it, I more identify myself as Captain America, the guy who always wears his heart (or the flag) on his sleeve. The guy who is never afraid. The guy who people want in their fox hole if anything bad happens to them. The guy who tries his best to get his friend, client, or company out of harm's way.

That is really the reason I wrote this book. Because I foresee more trouble ahead if things don't change. And change soon. Nearly two years after the Target cyber-attack, I still see companies getting hacked daily. I still see statistics saying people don't pay enough attention to cybersecurity. And I saw personally the damage the OPM hack caused to several of my friends, all of whom were retired government or military workers, whose personal information got stolen. They all called me for help. I did give them good practical advice about watching credit reports, bank accounts, etc. and generally how to protect themselves. But really the damage to their psyche was already done. Their personal information was stolen. My friends were both mad, and sad. And I don't like that.

I am not the world's most cyber knowledgeable lawyer. I don't pretend to be. Nor am I the most knowledgeable corporate governance lawyer in the world. I don't pretend to be that either. However, I am a student of history. I have lived and worked through the S&L crisis, the Tech boom and bust in 2000-2002, and the financial crisis of 2007-2008. I have seen bad things happen to good people. Really good people who cared greatly about their companies, their firms and their country. I care too. That is the reason I wrote this book.

In the pages ahead we try to pull together very difficult and complex topics regarding IT and informational management and distill them, from "tech speak" to plain English.

What are the right answers to those questions? I don't know. And it depends, as every company is different. I can only give you the questions. The challenge is for you to have those discussions internally with your company's C-Suite and IT staff, and come up with practical solutions. Answering our questions will take effort and a lot of communication. Answering our questions may take a lot of meetings, and may require a lot of advice from both IT experts, and

maybe even from us lawyers. As I said, I cannot assure you of what the right answers are. The one thing I can say is that by having these cybersecurity discussions and communications on a regular basis should help all companies come up with better ideas, better plans, and hopefully allow them to make better business judgments that may ultimately help their customers, their clients, and their investors and regulators understand they are doing everything possible to make the information they keep and store (whether internally or in the cloud) as safe and secure as possible from a cyber-attack.

And if your company is ultimately the subject of a cyber-attack, if your company takes "a cyber punch" to the head, we try and give practical advice on cyber incident response plans and procedures to help get you "off the canvas" and back on your feet as soon as possible. Again, no strategy and no incident response plan is perfect. Practice makes perfect. Train for the worst, and hope for the best. Perfection is probably not achievable here. Resiliency is probably the best approach. Just know that the Captain will be right behind you in your efforts.

The truth is we are all in the same foxhole. We need to work together. As Admiral Mike Rogers said last year, "cybersecurity is the ultimate team sport."

Thank you.

— PAF

TABLE OF CONTENTS

"Paul Ferrillo's new book on cybersecurity is exactly what today's marketplace so desperately needs: the insights of a great legal mind guided by a keen sense of the reader's business needs. Here are the specific questions each officer and director needs to be asking. There's a lot being published these days on this most urgent of issues, but Ferrillo's is one book that should sit in every C-Suite and boardroom."

— Richard S. Levick, Chairman & CEO, LEVICK

"This elegantly-written treatise is a tour de force. Paul Ferrillo explains zero day attacks, threat vectors and wiperware in simple terms and then describes their potentially awesome impact on every aspect of our lives."

— Peter J. Beshar, Executive Vice President and General Counsel, Marsh & McLennan Companies, Inc.

"Paul Ferrillo is the lawyer crisis manager I would turn to if I had a crisis - and this book tells you why he is so widely respected where law and media risk intersect. It is a must read for lawyers and PR specialists who by now should understand that taking risks to be proactive to get your facts out usually is the best course."-

— Lanny J. Davis, Former special counsel to President Clinton 1996-98

"Paul Ferrillo is spot-on in pointing out that network defenders are face-to-face with nation states and highly resourced cyber criminals. Paul's challenge to directors to think differently about IT security strategy could not be more timely as current cyber security spending, while ever-increasing, is proving to be less than effective against today's threats. Paul has done us all a great service by outlining, in a concise and understandable format, the best practices corporate boards need to focus on to get the most out of their security investments. Paul's guide is especially effective in highlighting the need to prepare for a cyber incident well in advance. His succinct and carefully researched guidance on incident response should be the starting point for every director and officer who needs to get smart on the issue."

— Leo Taddeo, Chief Security Officer, Cryptzone - Former Special Agent in Charge, Cyber/Special Operations Division, Federal Bureau of Investigation, NYC

"Long overdue and timely, Paul Ferrillo has delivered a concise, no nonsense cybersecurity resource written in an easily accessible style for directors and senior executives. From my perspective as both an independent director and cybersecurity professional, this book should be required reading for all board members and CEOs. Paul covers the most important concepts including focus areas of regulators, pragmatic regulatory advice and red flags that every director should recognize. This book strikes the perfect balance of breadth and depth, giving readers a solid understanding at a strategic level while illuminating key tactics. The book is rich with valuable content and well researched, with extensive links to original sources including key regulatory communications, reference materials, articles, and industry white papers. Armed with the knowledge contained in this book, directors can confidently execute their duty of care with regard to cybersecurity in an informed manner.

— George E. Thomas, Jr. - Independent Director & Executive Vice President Americas - Fifth Step

"Paul Ferrillo's book is an insightful resource on a very significant business issue. By any measure, cybersecurity is the biggest and most common threat organizations face, and one of the most vexing aspects of cyber threats is that they are constantly evolving. Empowered with the knowledge about what the threats are and how to mitigate them, businesses will have the tools to help turn the table on threat actors."

— David Burg, Global and US Cybersecurity Leader, PricewaterhouseCoopers LLP

CHAPTER 1 :

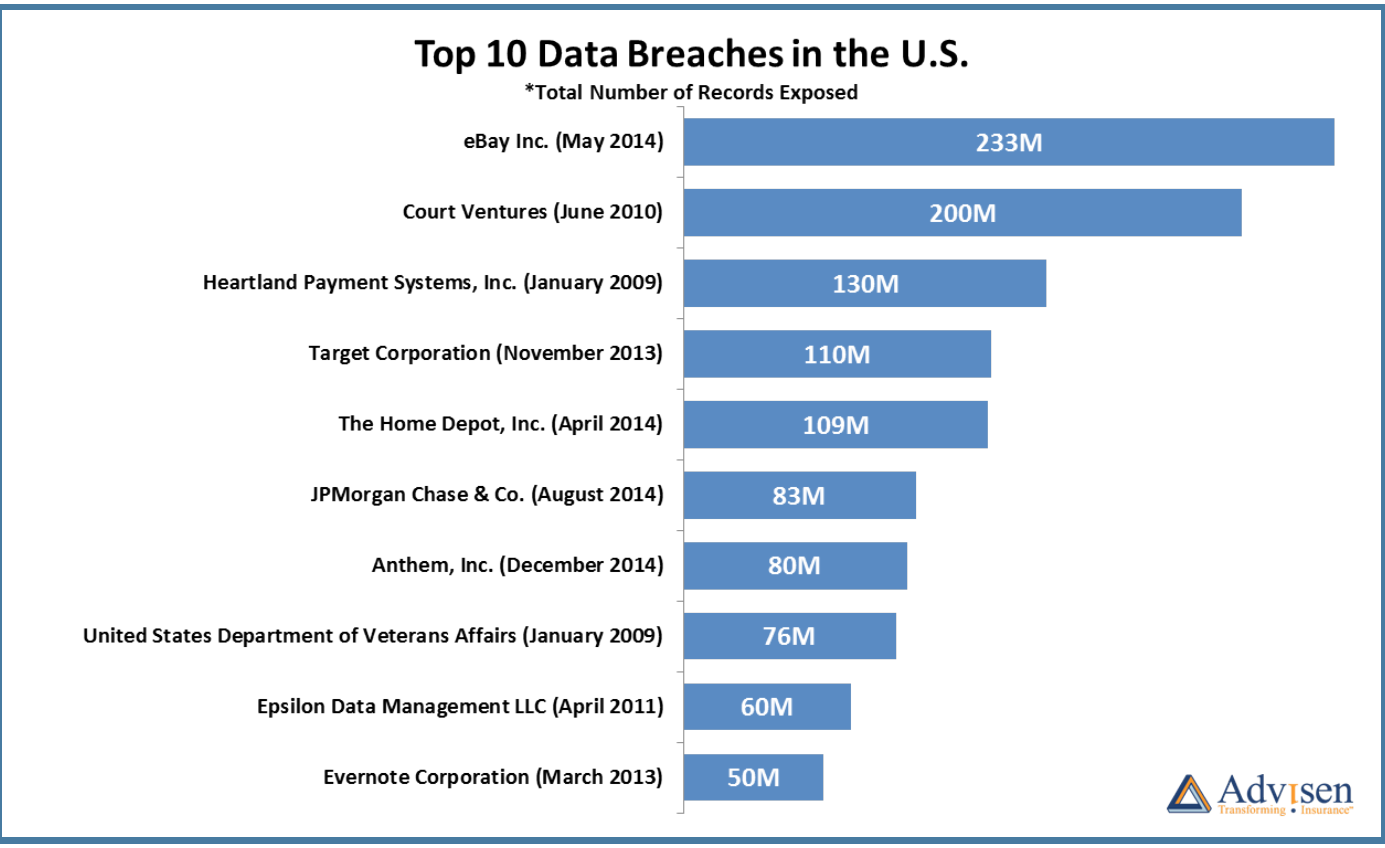
CYBERSECURITY THREAT ACTORS, THREAT VECTORS AND A TARGET RICH ENVIRONMENT

PURPOSE OF THIS CHAPTER:

1. Identify Today's Key Cybersecurity Issues.
2. Identify the Threat Actors Attacking Corporate America.
3. Identify the Threat Vectors Being Used by the Attackers.
4. Identify Which Industry Sectors Are Suffering Severe Cyberattacks and Are Most Vulnerable.
5. Identify the Top 10 Questions the Board Should Be Asking.

Yes, I have to admit this chapter has a really cool and catchy title. Purposefully so. But what is happening to corporate America today with respect to the repeated cybersecurity breaches being reported nearly every day in the media is anything but "cool." The effects of the constant barrage of cyber-attacks on US public companies like Experian and United Airlines,[1] the White House,[2] the awful data breach at the Federal Office of Personnel Management ("OPM"), [3] the Internal Revenue Service[4] and now even the hack of the 2015 Jeep Cherokee are frightening to think about, and things appear to be getting worse every day.[5] Even companies thought to have a very mature cybersecurity culture have been hacked.[6] If left unchecked, cybersecurity and cybercrime could severely threaten the future growth of our great country. Indeed, in PricewaterhouseCooper's 18th Annual Global CEO Survey 2015, for example, 87% of US chief executives said they were worried that cyber threats could impact growth prospects, up from 69% the year before.[7] None of these executives, we are sure, want their companies to end up "in the cybersecurity ditch" as a result of a sophisticated cyber-attack.

Starting in November 2013 with the Target cybersecurity breach,[8] corporate America has really never seen a crisis of this shape and this magnitude. Yes, the 2007-2009 Financial Crisis was itself a profound crisis, but it was not necessarily generated by third party actors' intent to do harm (or worse). Similar to the end of the tech boom (in 2001-2002), which concluded with the failures and bankruptcies of companies like Enron, WorldCom and Global Crossing, all of those economic crises were driven by various economic conditions precipitated by overheated or unrealistic free market expectations, coupled with an overconcentration of risk in one particular area or sector (e.g., technology or residential real estate).



Not so for the cybersecurity crisis we face today. Never before have nation states "bombed" each other with state-of-the-art malware,[9] distributed denial of service attacks (hereinafter referred to as "DDoS"), spearphishing[10] or other hacking attempts (which are cumulatively called "threat vectors") aimed at financially crippling the target of the attack (like the 2014 attacks on the Las Vegas Sands and Sony Pictures[11]), or stealing state secrets or critical intellectual property.[12] Never before have nation-states or private actors (called in the cyber world, "threat actors"), with or without nation-state approval, attacked private industries and most especially the health care industry to both randomly steal their most valuable business information, while crippling their reputations among consumers and patients, who are rightly angered that their credit card information, health care records,[13] or personal information including social security numbers has been stolen and is now up for sale on the black market. To many individuals, this is simply a breach of trust and totally unacceptable cybersecurity for the stores they frequent, the employers they work for, or the places they rely on for medical care.

In their recent study, "2015 US State of Cybercrime Survey," PriceWaterhouseCoopers LLP ("PwC") summed up 2014 extremely well:

> "Globally, a record 1 billion data records were compromised in 2014, according to a report by security firm Gemalto. Many of those security incidents were very widely reported. The year 2014 saw the term "data breach" become part of the broader public vernacular, with The New York Times devoting more than 700 articles related to data breaches, versus fewer than 125 the previous year."[14]

A more recent study, published in September 2015, noted that, "the Breach Level Index for the first six months of 2015, revealing that 888 data breaches occurred, compromising 246 million records worldwide."[15] And the year is not over yet!

Thinking historically, what previous economic crises and today's global security crisis have in common, is the potential liability of the boards of directors. Like the boards of directors of companies which failed during the Financial Crisis, these boards of directors have generally accepted fiduciary duties to shareholders and other investors. One of the duties is the oversight of the company's enterprise risk management (called "ERM") function. And one of the ERM oversight functions is the oversight of a company's cybersecurity procedures.

We start here at the beginning, not to scare, scold, or offend, but to identify the problems we face: who are the threat actors, what are the threat vectors, and what industries are being attacked the most by cyber intrusions. It's important to identify the problem first. Then we hope to identify some solutions in later chapters.

WHO ARE THE THREAT ACTORS?

"There are those [companies] who've been hacked by the Chinese, and those who don't know they've been hacked by the Chinese... They are extremely aggressive and widespread in their efforts to break into American systems to steal information that would benefit their industry."

— FBI Director James Comey, on TV news show, "60 Minutes," October 5, 2014.[16]

"Look, we have a lot of concerns about the sources of [cyber] attacks because there are many different sources...I don't think there's a CEO in the financial sector that doesn't wake up in the morning with this on their mind. Now the fact of the matter is that cyber attacks don't have to come from big, well-organized forces. You know, one smart person and one bad person can do an awful lot of damage. It's something that we have to pay attention to every day."

United States Treasury Secretary Jack Lew, October 5, 2014.[17]

"[Cyber attackers] can just do literally almost anything [they] want, and there isn't a price to pay for it...."

— Admiral Mike Rogers testimony before the House Intelligence Committee, Nov. 20, 2014.[18]

"What worries me most is that ISIL's investment in social media — which has been blossoming in the last six to eight weeks in particular — will cause a significant increase in the number of incidents that we will see… That's what I worry about all day long. "ISIL is changing [the] model entirely because ISIL is buzzing on your hip," he continued, referring to smartphones. "It's pushing its message 'all day long' on Twitter."

— Director of the FBI, James Comey, July 22, 2015.[19]

Who are the main threat actors? First, despite vehement denials from its government, many sources contend that the Chinese have been the most industrious nation when it comes to cyber-attacks, both in breadth and scope. See FireEye/Mandiant Trends Report, "Beyond the Breach" (hereinafter the "Mandiant Report"[20]). The Mandiant report further states that these intrusions have not just plundered agencies like the US Department of Defense, and weapons systems like the F-35 fighter jet,[21] but more importantly basic "how to conduct business information" in various industries. These persistent intrusions led to the indictment of five officers of the Chinese People's Liberation Army on charges of cyber espionage.[22] To date, rumors persist that China may have some involvement in both the Anthem breach and the OPM breach.[23] The FBI recently released a study of 165 companies that reported a data breach by foreign sources. In 95% of those cases, the companies suspected that China was to blame.[24]

The Russian government has also been rumored to have been involved in several attacks (one being the White House hack mentioned above), and most recently in hacks on NATO.[25] Then come a variety of other nation-state actors including North Korea,[26] Iran[27] and Syria.[28] North Korea's defining moment as a nation-state hacker came with attribution of the Sony wiper ware attack. At the time, one expert noted:

> "The North Korean attack on Sony was absolutely a watershed moment for everybody. Because within hours, they saw Sony pull a movie, and the President was on TV" talking about it, Meyers says. "It was a major international incident. They didn't have to launch a bomb … all they had to do was [plant] malware, after malware."[29]

Excluding nation-state actors, there have been a variety of public reports of various private actors (more likely termed "cyber criminals") who have, most notoriously, devastated the US retail sector with repeated attacks on these retailers' point-of-sale (POS) systems using a variety of different methods,[30] which will be explained below. Indeed, according to the most recent Ponemon Institute/IBM 2015 Estimated Cost of Data Breach Study[31] (hereinafter, the "Ponemon Report," which surveyed data breaches over calendar year 2014 in 11 countries), 47% of all data breaches surveyed stem from malicious or criminal attack. The average cost of a data breach due to malicious or criminal attacks increased from $159 per compromised record in 2013, to $170 in 2014. In the United States alone, the cost per comprised record was approximately $217.[32] Note that is the "per record" cost, and the total damages for some of the major breaches reported in 2014 could easily reach into the 8 or 9 figures.[33]

A further key take-away from many of these attacks is that it has taken companies sometimes up to six months to realize they have been breached.[34] And in many cases, the victims did not discover the breach on their own. They were told about the breach by either a governmental authority (principally, the FBI or Secret Service) or a third-party (like a banking institution).[35] In a few cases, breaches were even first reported by a famous cyber investigative blogger and noted cybersecurity authority, Brian Krebs.[36]

WHAT ARE THE THREAT VECTORS?

First, what is a threat vector? It is a path, or a tool that a threat actor uses to get at a target. In this chapter we are going to use the word "target" to mean "target industry," but in reality a target is more than that. Targets "are anything of value to the Threat Actor," e.g., control of your server (and its secrets), your computer, your iPad, your social media accounts, your passwords, or your bank account.

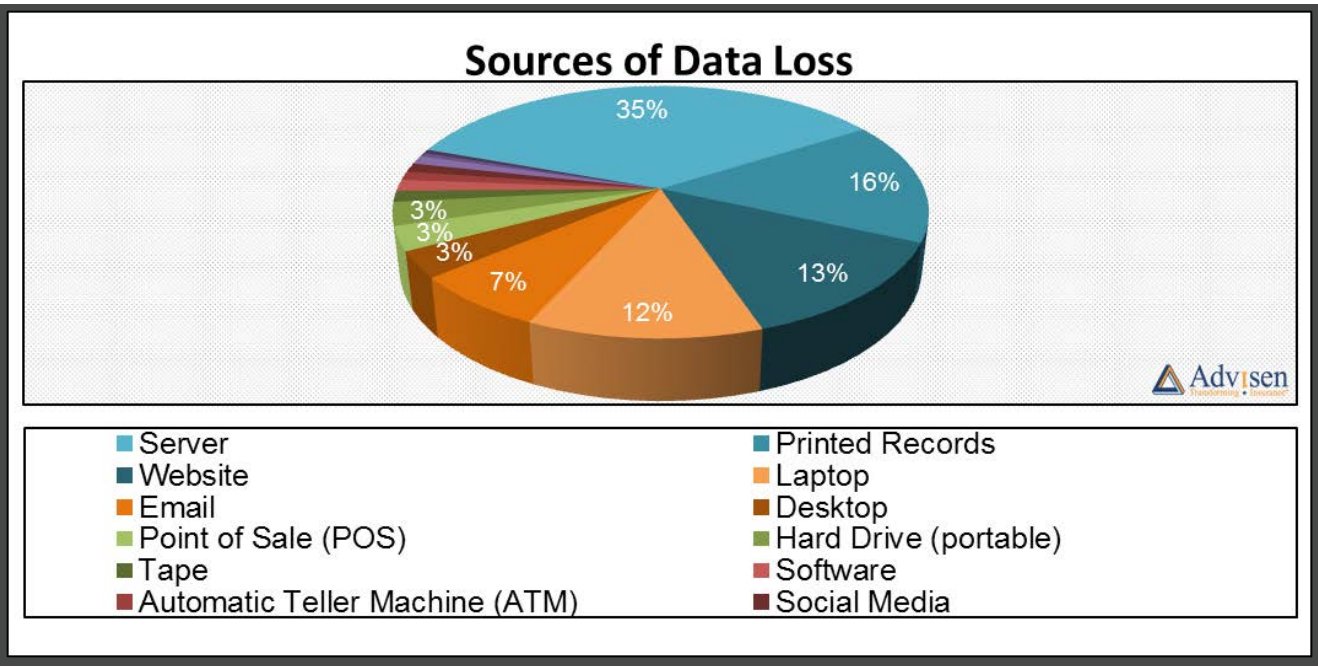
The 2015 Verizon Data Breach Investigations Report,[37] ("the Verizon Report"), which reviews and summarizes a confirmed 2,122 data breaches (where there was disclosure or potential disclosure of confidential information) in 61 countries over the 2014 calendar year, does a very good job in pin-pointing the exact type of threat vector used in any given cyber assault. It is not necessary to go into exhaustive detail on each type of threat vector identified in the Verizon Report (in fact many are way too complicated for the layperson director or officer to understand), but we think it's important to identify the trends involved since they correlate with both the types of industries being attacked, as well as the governance and risk issues that we will explore in later chapters. Here are the top threat vectors and a short description of how they generally work:

1. Point-of-Sale ("POS") Intrusions:

These are the big cybersecurity breaches you read about almost every day in the newspaper or in your Twitter feed. The basic premise of a POS attack is to implant some variant of malware onto a retailer's credit card processing system to collect credit card information via some sort of a "RAM" scraper at a POS terminal (like the card-swiping machine at your local department or food store). The credit card data (account numbers, expiration dates and cardholder information) on the magnetic stripe of the card is then collected via the malware-compromised server and sent (the technical term used is "exfiltrated") outside the network to a third party. There have been many variants to malware used to accomplish this task, and many vectors used to deliver the malware, including spam, phishing and now even botnets.[38] The malware has been difficult to find (sometimes taking months for a retailer to become aware it has suffered a breach).

2. Web Application Attacks:

A web application attack is defined generally as when any web application is used as the vector of an attack. Generally the malicious actor will by various methods attempt to gain access to various applications



on a company's server through a variety of methods, like phishing and spear phishing,[39] password and credential compromises, finding code vulnerabilities within certain popular network applications, or the injection of code into an application to attempt to compromise the company's network. A recent study found 40% of all SQL injection attacks and 64% of all malicious HTTP traffic campaigns target retail websites. "Our study shows that retail sites are a big target for hackers. This is largely due to the data that retail websites store - customer names, addresses, credit card details - which cyber criminals can use and sell in the cyber crime underworld."[40]

3. Software Vulnerability or "Zero Day" Attacks:

A zero day vulnerability (or a "Common Vulnerability Exposure" or "CVE") refers to a "hole" in software that is unknown to the vendor. This security hole is then exploited by hackers to install malware on the subject server before the vendor becomes aware and hurries to fix it—this exploit is called a zero day attack because the developer/vendor has zero days to fix it. Exploits using software vulnerabilities can be extremely harmful if not caught early.[41] As of October 2015, 15 zero-days have been discovered in 2015, making it likely that the total 2015 number will exceed the 25 discovered in 2014. The 2015 zero-day attacks to date were all discovered in popular software products widely in use across private and professional IT systems."[42] Vulnerabilities are rated under a Common Vulnerability Scoring System ("CVSS") which attempts to measure the potential severity of the vulnerability.[43]

Once found or discovered (very typically by third party forensic analysis), a patch is issued by the software company to "fix" the vulnerability. The problem here is that some companies do not have the resources internally, or regimented patching schedules (ASAP patching for critical vulnerabilities), thus leaving them susceptible to attacks for days, months or even years before being patched. Patching alerts and updates seem to occur now on almost a daily basis.[44] Unfortunately many of the alerts for some reason or another are not timely remediated, allowing attackers even more time to successfully exploit the vulnerability to their own advantage.[45] Indeed, one recent study of software vulnerabilities stated:

> "The analysis showed that over 15,000 (7.5%) of the open source components being consumed by these organizations in 2014 had known security vulnerabilities. Of those 15,000 components, an average of 66% (9,900) had known vulnerabilities dated 2013 or older. That means, they were known vulnerable components ('bad') before they were downloaded."[46]

4. Cyber-Espionage Attacks:[47]

These are what the category indicates: blatant, yet highly-disguised and nearly undetectable methods used by nation states and third party actors to steal valuable information by a variety of methods: injection of malware, phishing, maladvertising,[48] watering hole attacks,[49] spearphishing, finding network and software vulnerabilities[50] and creating backdoors to exfiltrate information, and simply by brute force attacks. The methods all vary from actor to actor. Here are the lengths that one nation-state hacker allegedly went to in order to steal data from US victims:

> "The campaign, called "Newscaster" by iSight Partners researchers, employed "social engineering." Hackers used a dozen fake personas and connected with victims over Facebook, LinkedIn, Twitter and YouTube. They sent their targets malicious links, which downloaded malware onto their machines, or directed them to fake login screens to steal the usernames and passwords.

"Among the fake personas employed by the hackers were the names of real journalists. In one case, hackers purported to be Sandra Maler, a Reuters reporter. In others, they claimed to be employees at military contractors, a tax adviser and reporters for NewsOnAir.org, a fake news organization set up by the hackers. They tried to make the site look legitimate by copying and posting news articles and swapping out the real bylines with one of the fake names."[51]

5. Card Skimmers:

Card skimmers are a little different from retail POS attacks in that they generally involve some device installed, for instance on an ATM or gas pump, to skim credit card data and send it to a third party. The types of card skimmers vary. They are generally very hard to detect.[52]

6. Misuse of Passwords and Privileges - One Phish, Two Phish, Red Phish, Blue Phish:

Insider misuse of IDs and passwords is relatively simple to explain. One of your employees uses his ID, password, or network privileges to gain information he either has access to, or should not have access to because of "over-privileging" and then uses it or sells it for his own financial gain.[53] The malicious use of passwords and privileges often happens with a third party involved, like a former employee, cyber-criminal or competitor who somehow gains access to your network through a phishing or spearphishing attack and steals information for his gain, and your loss.[54]

Because of the vast amount of information available on the Internet, phishing and spear phishing attacks have taken great predominance in the US cyber ecosystem, and have become the primary threat vector facing US companies. Approximately 91% of all cyber-attacks start with a spear phishing email.[55] The Verizon Report notes that approximately 23% of all users now open phishing messages, and 11% click on attachments.[56] The attachment or links may lead to the seeding of malware on the recipient's computer or even ransomware, like CryptoLocker or Cryptowall.[57] Socially-engineered spear phishing attacks thus present a tremendous problem. We discuss spearphishing mitigation and employee training tactics in later chapters.

7. Wiperware Attacks:

This type of attack that has surfaced more recently: "wiper" malware. Wiper malware is "designed to erase data from PC and file-server hard drives and delete the master boot record, so the machines cannot boot."[57] Simply put, wiper malware can wipe away all the data on multiple servers infected at a target company. In two recent cases, called "Shamoon" and "Dark Seoul", over 30,000 servers were essentially deleted.[59] Apparently a variant of Shamoon called "Destover" attacked the servers at Sony Pictures. "Destover, and the like, are much more dangerous in that they overwrite the master boot record on a computer, not only rendering the computer useless after robbing it blind, but also leaving few bread crumbs for investigators to follow."[60] Another variant of wiper malware was apparently used to attack the Las Vegas Sands in February 2014, rendering thousands of servers useless.[61]

8. Distributed Denial of Service ("DDoS") Attacks:

A final method hackers have used to wreak havoc on US companies is the DDoS attack. This attack involves a situation where the attacker, through the use of Botnets,[62] creates an "army of computers"

who then attack a particular website, with a typical bandwidth and a typical duration. Botnets, a very typical threat vector in the financial services and retail space, can tie up a computer network for hours (and sometimes days), throwing the company off-line, frustrating users and customers. The most famous botnet attack of 2014 was the "Grinch-like" attack by the Lizard Squad on the Sony and Microsoft gaming networks on Christmas day, knocking users off-line for hours.[63] Other DDoS attacks have targeted financial institutions.[64] Indeed, the Lizard Squad has been very active, taking down the UK National Crime Authority website for a period of time with a DDoS attack.[65] A recent report issued by cybersecurity company Akamai noted that:

> "For the past three quarters, there has been a doubling in the number of DDoS attacks year over year. And while attackers favored less powerful but longer duration attacks this quarter, the number of dangerous mega attacks continues to increase. In Q2 2015, there were 12 attacks peaking at more than 100 Gigabits per second (Gbps) and five attacks peaking at more than 50 Million packets per second (Mpps). Very few organizations have the capacity to withstand such attacks on their own."[66]

WHO ARE THE TARGETS OF THE CYBER ATTACKS?

The Verizon Report gives a very good summary of the industry segments most affected by cyber incidents and data breaches in calendar year 2014. Leaving aside the number of cyber breaches affecting the public sector (like federal and state governments[67]), here are the industry segments having the highest number of security incidents with confirmed data losses:

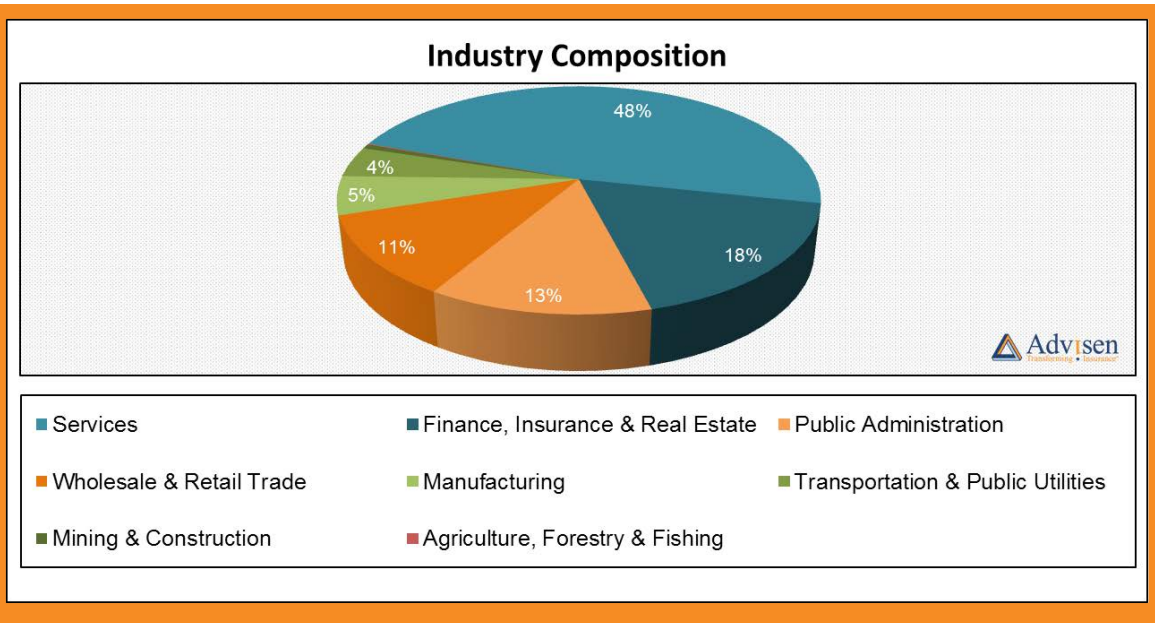
1. **FINANCE** - no surprise here - high value personal and business information, and high proprietary trading data, algorithms and M&A data. Finance organizations faced cyber threats from both malicious insiders and third parties.[68]

2. **RETAIL** - also no surprise given the prevalence of POS attacks - high value personal information and credit card data as we saw in the Target and Neiman Marcus breaches.

3. **ACCOMMODATION (HOTELS, MOTELS)** - same as retail - high value personal information and credit card data.[69] As an added bonus, there may be many people accessing the hotel's wifi system.

4. **UTILITIES** - especially scary - vital infrastructure industry sector being attacked by both hacktivists and nation states for business data - and to terrorize Americans.[70] In a recent Aspen Institute/ Intel Study, the report noted that "Despite high confidence in their own defenses, US and French respondents in particular rate a serious cyberattack affecting critical services and causing loss of life as highly likely within the next three years. Respondents from the transportation and energy sectors were more likely than their counterparts in other sectors to deem the possibility of such an attack (likely or highly likely).[71]

5. **PROFESSIONAL SERVICE FIRMS (LIKE LAW FIRMS, ACCOUNTING FIRMS, AND CONSULTANTS)** - perceived to be "soft targets" not necessarily concerned about cyber attacks, but an industry segment that typically stores a high volume of both the intellectual property and business data of its clients.



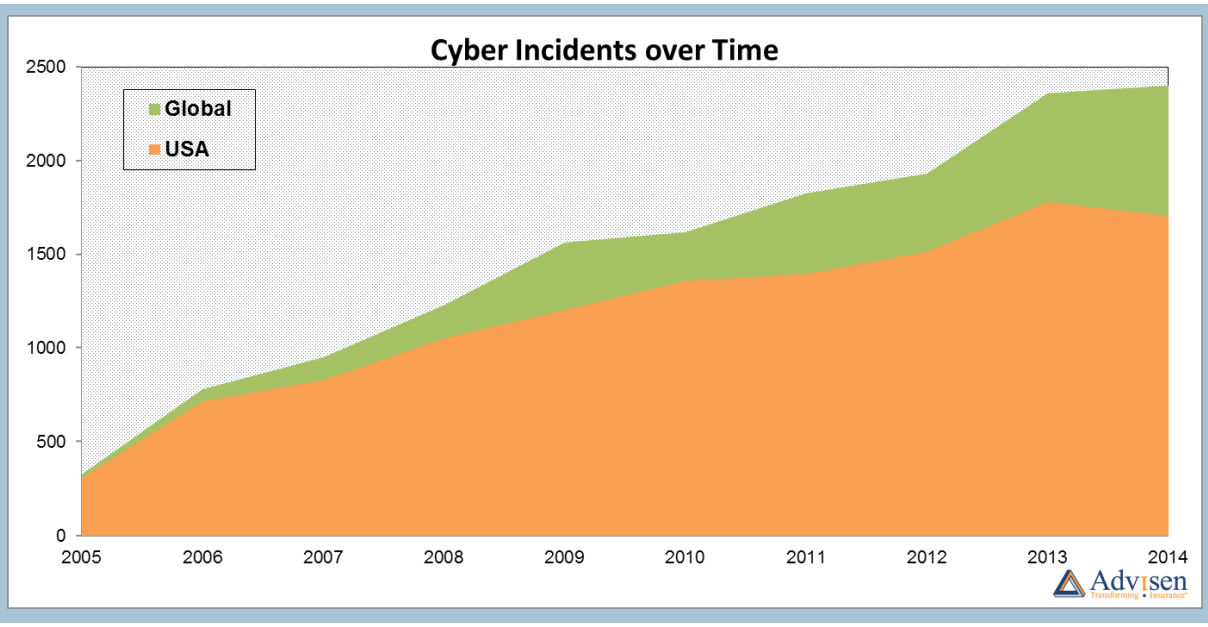
6. **HEALTHCARE** - no surprise - high-value personal information, e.g., Anthem, Premera, Carefirst, UCLA Healthcare System, and Excellus Healthcare.[72]

7. **EDUCATIONAL INSTITUTIONS** - where hackers have recently mined data at institutions such as Harvard, Penn State, the University of Virginia and Rutgers.[73]

A thorough reading of all of the data breach reports we cite above could lead one to five broad conclusions (supported by concrete public data) that all directors and officers of public and private companies must focus on in guiding their companies through the wave of cyber assaults to come:

- Cyber attacks continue to increase year over year (including the first 8 months of 2015) despite increased spending on cybersecurity defensive measures;[74]
- The severity and sophistication of these attacks is increasing;
- Most companies don't detect breaches themselves; they are told by third parties;
- It takes companies on average 205 days to discover a breach on their network; this time lag allows attackers to move laterally within networks and cause more damage and open up additional layers of information which then can be stolen;
- Even companies using a multi-layered defense-in-depth approach to cybersecurity could not protect themselves from a cyber attack.[75]

So then, the question must be asked, do US companies have any idea what they are doing when it comes to cybersecurity? Or as a recent article from BlackHat USA 2015 recently stated (somewhat in jest, somewhat not), "Abandon All Hope, Ye Who Log On Here."[76] Another recent survey, the "BlackHat



Attendee Survey: Time to Rethink Enterprise IT Security," stated similarly "As enterprises continue to struggle with online attacks and data leaks, many are asking one common question: What are we doing wrong?"[77]

In truth, while these may be over-generalizations to some companies, they really do not apply to the vast majority, who are both very sophisticated when it comes to cybersecurity, and who spend tens of millions of dollars a year on cybersecurity systems. But the truth also is that though these companies try extremely hard to protect their most valuable data, the "bad guys" always seem to be one step ahead, coming up with ever-increasing sophisticated threat vectors that can invisibly and silently lurk for months on a company's network, doing ever-increasing harm to the company's business and financial fortunes by continually stealing IP and customer data. And these attackers can do so mostly without the fear of financial or criminal consequences. Hackers only need to be successful once. But companies need to be successful repelling or defending against these attacks all the time.

So, should we just waive the white flag? Not at all. That is not what this book is about.

This book is about raising corporate awareness at the most senior levels of companies to the problem we all face: we are not winning in cyber warfare. We are losing big time. And the statistics prove the point.

WHAT ARE THE TOP 10 QUESTIONS THE BOARD SHOULD BE ASKING REGARDING THEIR COMPANY'S CYBERSECURITY POSTURE?

KEY:

This book is about using the extraordinary amount of data and knowledge we have on the types and methods of cyber attacks, the superb knowledge we have today which has led to major advances in intrusion detection systems, and the new National Institute of Standards and Technology Cybersecurity Framework (announced by the United States Government in February 2014),[78] to stimulate incredibly important discussions within companies and especially at the board of directors level about several of the most guiding fundamental principles of cybersecurity which hopefully, if discussed and acted upon, should potentially limit or severely decrease the damage that could result from a sophisticated cyber-attack:

1. What are the most valuable intellectual property and customer-based informational assets we need to protect within our company; and on a scale of 1-10, how do we categorize and rate these assets in terms of importance to the business that we are in?
2. Where are these assets housed (in house, in the US, in another country, or in "the cloud,")? Are all assets (despite differing values or classification) housed on the same network server, thus rendering them subject to a cyber attacker laterally moving within our network?
3. What cybersecurity risk assessments, vulnerability assessments and/or compromise assessments has the company done in the past year to make sure our network cybersecurity measures are protecting our "crown jewel" to the best extent possible?
4. How best do we protect our most important assets by allocating the right financial, hardware, software and people resources to the company's cybersecurity infrastructure?[79]
5. How best do we train our employees to deal with the sophisticated cyber attacks we are facing?
6. Are we doing due diligence of our third party or outsourced vendors to make sure they cannot be a source of a cyber attack against our firm by having too much access to our network, or can respond to and recover from a cyber-attack against their own network?[80]
7. How can we improve upon (and regularly practice) our Cyber Incident Response plan so we are able to quickly identify, respond to and "clean up" the effects of a sophisticated cyber-attack in full cooperation with law enforcement[81] so that our business operations and corporate reputation will remain intact?
8. Is the company participating daily in some "threat sharing" organization, like the FS-ISAC,[82] or a private vendor driven information sharing group in order to stay on top of what threats our peers are facing daily?
9. How can we improve upon (and regularly practice) our Cyber Business Continuity Plans so that if the worst happens (a serious data breach, or attempted network take-down (e.g., Sony Pictures) or a prolonged DDoS interruption), we can resume our business operations in the quickest

possible time so that the business and our corporate reputation will remain intact? And finally -

10. How can my company use cybersecurity insurance to transfer some of the risk of a cyber attack to a willing insurance company in order to protect my company and my investors from a substantial balance sheet loss that I most definitely will incur if I face a sophisticated cybersecurity attack?

In the world of cybersecurity there are no 100% guarantees. There is no 100% solution. There is no "magic bullet". But we posit the following: If companies engage in regular and diligent communications of the above principles, document them, and make informed and timely business judgments about how to respond to the cybersecurity "problem", then even in the face of inevitable attacks, it will be hard to criticize these companies (and successfully sue them) and their boards of directors for not "trying to do their best." Further, we preach and hope to teach cyber-resiliency - the creation and use of a holistic cyber-security and incident detection and response program designed to catch cyber incidents at their earliest possible moment, disable them and repair your networks quickly before the incident can do horrendous damage to your information management network, your balance sheet and your reputation with customers, employees and investors. That is what this book is about!

Where do we go next? Hopefully you will answer, "The next chapter." Because frankly, if you are a director or officer of a public company, or a managing director of a private equity or hedge fund, you really need to turn the page and read on!

ENDNOTES

[1] See "China-Tied Hackers That Hit U.S. Said to Breach United Airlines," available at http://www.bloomberg.com/news/articles/2015-07-29/china-tied-hackers-that-hit-u-s-said-to-breach-united-airlines.

[2] See "Russia reportedly suspected of being behind breach of White House computers," available at http://www.foxnews.com/politics/2014/10/29/russia-reportedly-suspected-being-behind-breach-white-house-computers/.

[3] See "OPM says second hack affected more than 21M Americans," available at http://www.usatoday.com/story/news/nation/2015/07/09/obama-hack-office--personnel-management/29921919/; "Valerie Plame: OPM breach is 'absolutely catastrophic' to security," available at http://www.usatoday.com/story/news/politics/2015/07/20/valerie-plame-opm-breach-absolutely-catastrophic-security/30431191/.

[4] See "Hacking of Tax Returns More Extensive Than First Reported, I.R.S. Says," available at http://www.nytimes.com/2015/08/18/us/politics/hacking-of-tax-returns-more-extensive-than-first-reported-irs-says.html?_r=0.

[5] See "Update: Chrysler recalls 1.4M vehicles after Jeep hack," available at http://www.computerworld.com/article/2952186/mobile-security/chrysler-recalls-14m-vehicles-after-jeep-hack.html.

[6] See "Netflix Ultra HD Copy of 'Breaking Bad' Hacked, Pirated," available at http://variety.com/2015/digital/news/netflix-breaking-bad-ultra-hd-hacked-pirated-1201580702/.

[7] See "US cybersecurity: Progress stalled: Key findings from the 2015 US State of Cybercrime Survey," available at http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf.

[8] See "Target cyber breach hits 40 million payment cards at holiday peak," available at http://www.reuters.com/article/2013/12/19/us-target-breach-idUSBRE9BH1GX20131219.

[9] See "New Shifu Banking Trojan An 'Uber Patchwork' Of Malware Tools," available at http://www.darkreading.com/vulnerabilities---threats/new-shifu-banking-trojan-an-uber-patchwork-of-malware-tools/d/d-id/1322039?.

[10] See "Pentagon Hack 'Most Sophisticated' Ever," available at http://www.thedailybeast.com/cheats/2015/08/05/joint-chiefs-of-staff-hacked.html; http://www.cnbc.com/2015/08/06/russia-hacks-pentagon-computers-nbc-citing-sources.html.

[11] See "Now at the Sands Casino: An Iranian Hacker in Every Server," available at http://www.businessweek.com/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas; "Data Breach Sets Off Upheaval at Sony Pictures," available at http://www.wsj.com/articles/data-breach-sets-off-upheaval-at-sony-pictures-1417657799.

[12] See "Sony Pictures employees get threatening email from alleged hacker," found at http://fortune.com/2014/12/05/sony-pictures-hack-threats/; "Sony cyber attack reveals hackers changing their stripes," found at http://www.ft.com/cms/s/0/1c967b94-7c0d-11e4-a7b8-00144feabdc0.html#axzz3L9ivPhJB; See "Obama Had Security Fears on JPMorgan Data Breach," found at http://dealbook.nytimes.com/2014/10/08/cyberattack-on-jpmorgan-raises-alarms-at-white-house-and-on-wall-street/?_php=true&_type=blogs&_r=0; "Cybersecurity lapses leave government agencies vulnerable to hackers," available at http://www.washingtontimes.com/news/2014/nov/23/cybersecurity-lapses-leave-us-government-agencies-/.

[13] See "Home Depot data breach lawsuits rise to 44," available at http://www.bizjournals.com/atlanta/news/2014/11/25/home-depot-data-breach-lawsuits-rise-to-44.html?page=all; "Insurance giant Anthem hit by massive data breach," available at http://money.cnn.com/2015/02/04/technology/anthem-insurance-hack-data-security/; "Premera Blue Cross sued over data breach," available at http://thehill.com/policy/cybersecurity/237181-premera-blue-cross-sued-over-data-breach; "Second Lawsuit Filed Over Community Health Systems Data Breach," available at http://www.ihealthbeat.org/articles/2014/10/14/second-lawsuit-filed-over-community-health-systems-data-breach.

[14] The PwC Survey is available at http://www.pwc.com/us/en/increasing-it-effectiveness/publications/us-cybercrime-survey-2015.jhtml.

[15] See "Gemalto Releases Findings of First Half 2015 Breach Level Index," available at http://globenewswire.com/news-release/2015/09/09/766885/10148574/en/Gemalto-Releases-Findings-of-First-Half-2015-Breach-Level-Index.html#sthash.BkPk9QkD.dpuf.

[16] See "FBI director on threat of ISIS, Cybercrime," found at http://www.cbsnews.com/news/fbi-director-james-comey-on-threat-of-isis-cybercrime/

[17] See "'This Week' Transcript: Treasury Secretary Jack Lew," found at http://abcnews.go.com/ThisWeek/week-transcript-treasury-secretary-jack-lew/story?id=25946701&singlePage=true.

[18] See "NSA Director Warns of 'Dramatic' Cyberattack in Next Decade," available at http://www.wsj.com/articles/nsa-director-warns-of-dramatic-cyberattack-in-next-decade-1416506197

[19] See "ISIL Keeps FBI Director Awake At Night," available at http://www.refinery29.com/2015/07/91202/james-comey-isis-biggest-fears.

[20] See "FireEye Releases Annual Mandiant Threat Report on Advanced Targeted Attacks," found at http://www.fireeye.com/news-events/press-releases/read/fireeye-releases-annual-mandiant-threat-report-on-advanced-targeted-attacks.

[21] See "Theft of F-35 design data is helping U.S. adversaries -Pentagon," found at http://www.reuters.com/article/2013/06/19/usa-fighter-hacking-idUSL2N0EV0T320130619; "Chinese Hacked U.S. Military Contractors, Senate Panel Says," available at http://www.wsj.com/articles/chinese-hacked-u-s-military-contractors-senate-panel-says-1410968094.

[22] See "Attorney General Eric Holder Speaks at the Press Conference Announcing U.S. Charges Against Five Chinese Military Hackers for Cyber Espionage," available at http://www.justice.gov/opa/speech/attorney-general-eric-holder-speaks-press-conference-announcing-us-charges-against-five

[23] See "Nation-State Cyber Espionage, Targeted Attacks Becoming Global Norm," available at http://www.darkreading.com/attacks-breaches/nation-state-cyber-espionage-targeted-attacks-becoming-global-norm/d/d-id/1319025.

[24] See "FBI Probes 'Hundreds' of China Spy Cases," available at http://www.thedailybeast.com/articles/2015/07/23/fbi-probes-hundreds-of-china-spy-cases.html (one FBI official recently noted that "The predominant threat we face right now is from China,").

[25] See "Russian hackers target NATO, Ukraine through Windows zero-day exploit," found at http://www.zdnet.com/russian-hackers-target-nato-ukraine-through-windows-zero-day-exploit-7000034639/.

[26] See "Update on Sony Investigation," available at http://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation; "FBI: North Korea to Blame for Sony Hack," available at http://krebsonsecurity.com/2014/12/fbi-north-korea-to-blame-for-sony-hack/.

[27] See "Now at the Sands Casino: An Iranian Hacker in Every Server," available at http://www.businessweek.com/articles/2014-12-11/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas; "Iran hackers targeted airlines, energy firms: report," available at http://www.reuters.com/article/2014/12/02/us-cybersecurity-iran-idUSKCN0JG18I20141202; "Iran-Linked Espionage Group Continues Attacks on Middle East," available at http://www.securityweek.com/iran-linked-espionage-group-continues-attacks-middle-east.

[28] See "Syrian Electronic Army Claims to Have Hacked U.S. Army Website," available at http://www.newsweek.com/syrian-electronic-army-claims-have-hacked-us-army-website-340874.

[29] See "Nation-State Cyber Espionage, Targeted Attacks Becoming Global Norm," available at http://www.darkreading.com/attacks-breaches/nation-state-cyber-espionage-targeted-attacks-becoming-global-norm/d/d-id/1319025.

[30] See e.g., "Berkshire-owned Dairy Queen says customer data hacked in 46 states," found at http://www.reuters.com/article/2014/10/10/us-usa-dairy-queen-cybersecurity-idUSKCN0HZ1TM20141010; "Target Now Says 70 Million People Hit in Data Breach,' available at http://www.wsj.com/articles/SB10001424052702303754404579312232546392464.

[31] See "2014 Cost of Data Breach Study: Global Analysis," available at http://www-935.ibm.com/services/multimedia/SEL03027USEN_Poneman_2014_Cost_of_Data_Breach_Study.pdf.

[32] See 2013 Ponemon Cost of Breach Report Study, found at https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf

[33] See "Target's data breach fraud cost could top $1 billion, analyst says," available at http://www.bizjournals.com/charlotte/news/2014/02/03/targets-data-breach-fraud-cost-could-top-1-billion.html. The cost of replacing the compromised credit cards could alone total $400 million or more. See "Banks' Lawsuits Against Target for Losses Related to Hacking Can Continue," available at http://bits.blogs.nytimes.com/2014/12/04/banks-lawsuits-against-target-for-losses-related-to-hacking-can-continue/?_r=0.

[34] See "Fewer Companies Able to Detect a Cyber Breach," available at http://ww2.cfo.com/cyber-security-technology/2015/02/fewer-companies-able-detect-cyber-breach/ (noting that according to Mandiant, in 2014 it took companies an average of 205 days to detect a breach.

[35] Id. The Mandiant report further reports that only 31% of companies were able to discover breaches on their own.

[36] See "Dairy Queen Confirms Breach at 395 Stores," available at http://krebsonsecurity.com/2014/10/dairy-queen-confirms-breach-at-395-stores/.

[37] Available at http://www.verizonenterprise.com/DBIR/2015/.

[38] See "New point-of-sale malware distributed by Andromeda botnet," available at http://www.cio.com/article/2949334/new-pointofsale-malware-distributed-by-andromeda-botnet.html.

[39] See "Anatomy of an Attack: From Spear phishing Attack to Compromise in Ten Steps," found at https://www.mandiant.com/threat-landscape/anatomy-of-an-attack/.

[40] See "Nearly half of all web application cyber attacks target retailers, study shows," found at http://www.computerweekly.com/news/2240235253/Nearly-half-of-all-web-application-cyber-attacks-target-retailers-study-shows.

[41] See "BlackEnergy Malware Plug-Ins Leave Trail of Destruction," https://threatpost.com/blackenergy-malware-plug-ins-leave-trail-of-destruction/109126#sthash.2zz6Trah.dpuf; see also "Sandworm APT Team Found Using Windows Zero Day Vulnerability," https://threatpost.com/sandworm-apt-team-found-using-windows-zero-day-vulnerability/108815#sthash.n3Mr8nBo.dpuf.

[42] See "Vulnerabilities in 2015: 0-days, Android vs iOS, OpenSSL," available at http://www.net-security.org/secworld.php?id=18732.

[43] See "Common Vulnerability Scoring System, V3 Development Update," available at https://www.first.org/cvss.

[44] See "Setting priorities with July's huge Patch Tuesday," available at http://www.computerworld.com/article/2947756/application-security/huge-july-patch-update-with-critical-update-to-ie-and-windows.html.

[45] See "Sixty Percent of Enterprise Application Vulnerabilities Go Unmitigated," available at http://darkmatters.norsecorp.com/2015/07/13/sixty-percent-of-enterprise-application-vulnerabilities-go-unmitigated/ (noting that many organizations take three to six months to remediate a known vulnerability).

[46] See "When Good Code Goes Bad," available at http://www.infosecurity-magazine.com/blogs/when-good-code-goes-bad/.

[47] In this section, we have not used the acronym "APT" or "advanced persistent threat" for a reason. An APT is not a per se "vector." It is a type of actor (very often nation-state sponsored) that makes a concerted effort to dig deep into a Company's network to collect sensitive information about a person, place, or secret (like the plans to the F-35 Fighter Jet) by silently moving laterally through a Company's network. See "Catch Me If You Can: How APT Actors Are Moving through Your Environment Unnoticed," available at http://blog.trendmicro.com/catch-me-if-you-can-how-apt-actors-are-moving-through-your-environment-unnoticed/?utm_source=twitterfeed&utm_medium=twitter&utm_campaign=information_security. FireEye/Mandiant and other recognized cyber threat analysts do a good job tracking these threats and the threat signatures to alert others. See e.g., "Threat Actor Tactics and Targeting Predictions for 2014," available at https://www.mandiant.com/blog/threat-actor-tactic-targeting-predictions-2014/#sthash.5m78hMkR.dpuf.

[48] See "Yahoo Malvertising Attack Points To More Flash Problems," available at http://www.informationweek.com/software/enterprise-applications/yahoo-malvertising-attack-points-to-more-flash-problems/a/d-id/1321626; See also "Cyphort Labs Issues Special Report on the Rise in Malvertising Cyber Attacks," available at http://www.darkreading.com/attacks-breaches/cyphort-labs-issues-special-report-on-the-rise-in-malvertising-cyber-attacks/d/d-id/1321902 (noting that "Cyphort researchers found that malvertising campaigns carried out by hackers increased 325 percent in the past year.").

[49] See "BlackHat 2015: 2FA key to defence against cyber espionage groups," available at http://www.computerweekly.com/news/4500251145/BlackHat-2015-2FA-key-to-defence-against-cyber-espionage-groups.

[50] See "Symantec uncovers Morpho cyber espionage operation," available at http://www.computerweekly.com/news/4500249597/Symantec-uncovers-Morpho-cyber-espionage-operation.

[51] See "Cyberespionage Attacks Tied to Hackers in Iran," available at http://bits.blogs.nytimes.com/2014/05/29/cyberespionage-attacks-tied-to-hackers-in-iran/?_r=0.

[52] See e.g., "Skimmer Innovation: "Wiretapping ATMs," found at http://krebsonsecurity.com/.

[53] A very recent study of IT decision makers reported that only 68% of the companies surveyed felt that their company was making an adequate investment in technology designed to monitor activities of users with elevated or privileged access rights. See "2015 Cyberthreat Defense Report, North America and Europe," available at http://www.brightcloud.com/pdf/cyberedge-2015-cdr-report.pdf.

[54] See e.g., "JP Morgan Found Hackers through Breach of Corporate Event Website," found at http://www.moneynews.com/Companies/JP-Morgan-Hackers-Breach-Website/2014/11/02/id/604663/.

[55] See "White House hack: By way of Russia with help from spear phishing," available at http://searchcio.techtarget.com/news/4500244197/White-House-hack-By-way-of-Russia-with-help-from-spear-phishing.

[56] See The Verizon DBIR at 13.

[57] See "IBM X-Force Threat Intelligence Quarterly, 3Q 2015," available at https://www-01.ibm.com/marketing/iwm/dre/signup?source=swg-WW_Security_Organic&S_PKG=ov38487&S_TACT=C41303YW&dynform=20131.

[58] See "Sony Hack: Ties to Past 'Wiper' Attacks?" available at http://www.bankinfosecurity.com/sony-hack-ties-to-past-wiper-attacks-a-7644/op-1.

[59] Id.

[60] See "Details Emerge on Sony Wiper Malware," available at http://threatpost.com/details-emerge-on-sony-wiper-malware-destover/109727.

[61] See "Las Vegas Sands' network hit by destructive malware in Feb: Bloomberg," available at http://www.reuters.com/article/2014/12/12/us-lasvegassands-cybersecurity-idUSKBN0JQ04520141212.

[62] A "bot" is "A type of malware that allows an attacker to take control over an affected computer. Also known as "Web robots", bots are usually part of a network of infected machines, known as a "botnet", which is typically made up of victim machines that stretch across the globe" infecting thousands, if not hundreds of thousands of computers. See "Bots and Botnets—A Growing Threat," available at http://us.norton.com/botnet/.

[63] See "Lizard Stresser Runs on Hacked Home Routers," available at http://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/.

[64] See "Cyber attack hits RBS and NatWest online customers on payday," available at http://www.theguardian.com/business/2015/jul/31/rbs-and-natwest-customers-complain-of-online-problems.

[65] See "Stressed out: Lizard Squad takes down UK law enforcement website in latest DDoS attack," available at http://siliconangle.com/blog/2015/09/02/stressed-out-lizard-squad-takes-down-uk-law-enforcement-website-in-latest-ddos/.

[66] See "Akamai Releases Q2 2015 State of the Internet - Security Report," available at http://prwire.com.au/pr/53743/akamai-releases-q2-2015-state-of-the-internet-security-report.

[67] There were 61,000 reported cyber attacks against the federal government reported in 2013 according to one report. See "Government hacks and security breaches skyrocket," available at http://www.cnn.com/2014/12/19/politics/government-hacks-and-security-breaches-skyrocket/.

[68] See "Corporate Espionage Risk Management For Financial Institutions," available at http://www.tripwire.com/state-of-security/risk-based-security-for-executives/risk-management/corporate-espionage-risk-management-for-financial-institutions/.

[69] See "Donald Trump's Hotels Have Reportedly Been Hacked," available at http://www.nationaljournal.com/tech/donald-trump-s-hotels-have-reportedly-been-hacked-20150701.

[70] See "Chinese Cyber Attack Could Shut Down U.S. Electric Power Grid," found at http://www.forbes.com/sites/robertlenzner/2014/11/28/chinese-cyber-attack-could-shut-down-u-s-electric-power-grid/.

[71] See "Critical Infrastructure Readiness Report: Holding the Line Against Cyberthreats," available at http://www.mcafee.com/us/resources/reports/rp-aspen-holding-line-cyberthreats.pdf.

[72] See "Cyber breach hits 10 million Excellus healthcare customers," available at http://www.usatoday.com/story/tech/2015/09/10/cyber-breach-hackers-excellus-blue-cross-blue-shield/72018150/.

[73] See "Harvard says data breach occurred in June," available at https://www.bostonglobe.com/metro/2015/07/01/harvard-announces-data-breach/pqzk9IPWLMiCKBl3IijMUJ/story.html; "Who hacked Rutgers? University spending up to $3M to stop next cyber attack," available at http://www.nj.com/education/2015/08/who_hacked_rutgers_university_spending_up_to_3m_to.html.

[74] The trend continues in 2015. See "Data Breaches by the Numbers," available at http://www.securityweek.com/data-breaches-numbers ("The data is clear and powerful. First, based on the number of records compromised, breaches are on the rise. In security circles, 2014 was known colloquially as "the year of the breach." However, 2015 almost doubled the 2014 tally of breached records, and has done so in the first eight months).

[75] See "Cybersecurity's Maginot Line: A Real-World Assessment of the Defense-in-Depth Model," available at http://www2.fireeye.com/rs/fireye/images/fireeye-real-world-assessment.pdf (noting that in a test of over 1200 companies, FireEye was able to determine that 97% had been breached even though they employed a defense-in-depth multi-layered cybersecurity posture).

[76] This tongue in cheek article is available at http://www.buzzfeed.com/josephbernstein/so-fing-fd?utm_content=buffer3af08&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer#.leWrL9VJWy.

[77] The BlackHat Attendee Survey is available at https://www.blackhat.com/docs/us-15/2015-Black-Hat-Attendee-Survey.pdf.

[78] See "Framework for Improving Critical Infrastructure Cybersecurity," found at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[79] See "Cyber Governance: What Every Director Needs to Know," available at http://blogs.law.harvard.edu/corpgov/2014/06/05/cyber-governance-what-every-director-needs-to-know/.

[80] See "Outsourcing: How Cyber Resilient Are You?" available at http://corpgov.law.harvard.edu/2015/07/26/outsourcing-how-cyber-resilient-are-you/.

[81] See "Best Practices for Victim Response and Reporting of Cyber Incidents," available at http://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents2.pdf.

[82] See "Financial Services Information Sharing and Analysis Center," available at https://www.fsisac.com/.

CHAPTER 2:
PROTECTING DATA STORED ON NETWORK SERVERS

PURPOSE OF THIS CHAPTER:

1. **Identify what network security devices are currently available to protect your Company's network servers, and how do they work.**
2. **Identify the importance of intrusion detection devices.**
3. **Identify the importance of password and network authentication.**[1]

Suppose you are a brand new internet business ramping up to sell GPS wrist bracelets for kids to consumers around the globe so they can monitor their children's every move through their home computers, iPads and iPhones, and protect them if they venture into the wrong areas or places. You anticipate the demand for these GPS wrist bracelets will be extremely high, especially in urban, industrialized markets where the safety of children is high on the list of every parent. You own the patent on these wrist bracelets. Your "ace in the hole" is a full licensing agreement which will allow each bracelet to be personalized for each child wearing one with his or her favorite cartoon character.

Your business will be entirely Internet-based (the bracelets will not be sold in third party stores other than your own company owned stores), and you anticipate collecting a large amount of personal data and credit card information not only from interested parents, but from their kids who will wear the bracelets, including their ages, social security numbers and wrist sizes.

These GPS wrist bracelets will be manufactured by a third party vendor overseas in an Asian market, who you will need to stay in constant contact with regarding orders, manufacturing and shipments. You anticipate using a third party vendor to direct ship the wrist bracelets to each parent. You also anticipate having regional sales offices, staffed by at least 30 employees, in the major urban markets (e.g., New York City, Boston, Washington DC, Orlando, Chicago, San Francisco and Los Angeles) and stores in high traffic malls to bring attention to your state of the art bracelets. Your home office will be in New York City, where you, along with executive staff and finance/executive sales staff of 20 people, will run the business. Lastly, you will enter into a credit card processing agreement with a third party vendor to process your sales orders.

You then go to a highly-regarded computer consultant and say, "help me plan out my business because I anticipate it's going to be a huge success." The consultant, all too happy to help, sells you not only the servers and routers you need, but the personal computers and mobile devices you will need to monitor your business, sales and shipments.

Because you have read about all of the major retail cybersecurity breaches in 2013 and 2014, and because you will be collecting personal and financial information from your potential customers, you say to the consultant, "I am going to need something to protect my data from intrusions by third-party bad guys."

The above scenario, though basic in nature, is illustrative of the problem that not only major businesses have every day of the week, including health care providers, health care insurers and hospitals, as well as private companies and small businesses - how do I best protect the personal data I collect in my day-to-day operations (and transmit between my offices and my vendors) so I don't end up on the front page of the New York Times after I report (like dozens of other companies before me) that my most valuable information (the personal information of my customers) has been hacked by a third party? Indeed, what a daunting question for the GPS bracelet entrepreneur, who has such a great idea to protect children, but who has no idea about how to protect all of the personal and financial data he hopes to collect if his product is a success.

These are undoubtedly complicated questions. And no director, unless he or she is a former CIO or CISO of a large company, could be expected to know all the answers. So what we will do here is raise several questions directors can explore with their IT management that involve basic cybersecurity tools and methods that can be employed in ground-based, company-owned computer networks to help secure informational assets.

As we noted in our introduction, there are no "perfect" or "right answers" here. History has proved that no network is impenetrable. Even sovereign governments like the United States have been regularly hacked. Network security systems must be looked at holistically in terms of not only hardware and software used, but also with a view towards password protection, employee training, and most important, resiliency and recovery if and when you suffer a cyber-security breach. We focus here on basic areas that any corporate officer, executive, or business owner should be concerned about when thinking about the concept of properly "layered" network security within their company. In later chapters, we will focus on the necessity that concepts of network security should be "owned" and "directed" by a company's board of directors as part of its basic responsibilities over enterprise risk management.

BASIC NETWORK SECURITY PRINCIPLES

The National Institute of Standards and Technology (or the "NIST") defines computer security as

> "the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (this includes hardware, software, firmware, information/data, and telecommunications).... Security should be appropriate and proportionate to the value and degree of reliance on the computer system and to the severity, probability and extent of potential harm. Requirements for security will vary depending on the particular organization and computer system."

Though this is certainly a broad definition, there are certain existential core concepts built in which should be the focus of any network security program. An additional concept built into the NIST definition is that no two organizations are alike. Our internet-based GPS bracelet business might require one level of network security. A technology-based public company would require a network security computer system that is light-years more complex. We leave the corporate governance aspects of enterprise risk management and network cybersecurity for later chapters.

Protect the Physical Security of Your Hardware

Physical security is what it says: controlling physical access to your server hardware so that it cannot be tampered with by unauthorized employees, third parties, or disgruntled former employees. Further, your computer hardware needs to be protected from environmental threats as well, including power interruptions, humidity, fire, and loss of air conditioning.

Network Security

Network security is a complicated mix of both hardware and software solutions that protect data from intrusions both internally and externally, and when data is transported from location to location within one's own computer network. Network security today is also a function of assessing the security and intrusion capability of third party vendors (as well as cloud service providers) with whom interaction is often necessary to run your business.[2] It is a holistic problem, which requires a holistic solution that might involve a wide-range of products that can meet today's most sophisticated threats.[3] Some people call it a "defense-in-depth" approach to cybersecurity.[4] Other people call it a "layered approach" to cybersecurity. Whatever the correct terminology is, traditional network security normally involves many elements and is constantly evolving in response to threats.

Firewalls

Firewall technology can be thought quite simply as the 16th century moat that was often built around castles to protect them and their occupants from attack, complete with armored guards to repel those who were not welcome.[5] In the 21st Century, firewalls are a system or set of systems that control access between your internal network and some external network (usually the Internet) according to a written security policy. According to a recent Dell SecureWorks Memo, "a firewall refers to a network device which blocks certain kinds of network traffic, forming a barrier between a trusted and an untrusted network."[6]

In other words, this mean forming a "barrier" between your network and outside internet connections, which blocks messages which do not meet your security criteria.

In general, there are two types of firewalls: hardware (like a router device) and software.

- **HARDWARE** - Typically called network firewalls, these external devices are positioned between your computer or network and your cable or DSL modem. Many vendors and some Internet service providers (ISPs) offer devices called "routers" that also include firewall features. Hardware-based firewalls are particularly useful for protecting multiple computers, and they also offer a high degree of protection for a single computer. If you only have one computer behind the firewall, or if you are certain that all of the other computers on the network are up to date on patches and are free from viruses, worms, or other malicious code, you may not need the extra protection of a software firewall.

- **SOFTWARE** - Some operating systems include a built-in firewall; if yours does, consider enabling it to add another layer of protection even if you have an external firewall. If your company does not have a built-in firewall, you can obtain a software firewall for relatively little or no cost from your local computer store, software vendors, or ISP. Because of the risks associated with downloading software from the Internet onto an unprotected computer, it is best to install the firewall from a CD or DVD.[7]

The above outline is only the start of "how to build" an effective firewall. There are then different types of firewalls within these two groups that offer different levels of protection:

PACKET FILTERING FIREWALL

This type of firewall has a list of firewall security rules which can block traffic based on IP protocol, IP address and/or port number. Under this firewall management program, all web traffic will be allowed, including web-based attacks. In this situation, you need to have intrusion prevention, in addition to firewall security, in order to differentiate between good web traffic (simple web requests from people browsing your website) and bad web traffic (people attacking your website).[8]

"STATEFUL" FIREWALL

This is similar to a packet filtering firewall, but it is more intelligent about keeping track of active connections, so you can define firewall management rules such as only allow packets into the network (governed by firewall rules) that are part of an already established outbound connection. You have solved the established and known connection issue described above, but you still can't tell the difference between "good" and "bad" web traffic. You need intrusion prevention to detect and block web attacks.[9]

DEEP PACKET INSPECTION FIREWALL

A deep packet firewall actually examines the data in the packet or "unit of data" crossing the network, and can therefore look at application layer attacks or malware, viruses or other potentially malicious activity. This kind of firewall security is similar to intrusion prevention technology, and, therefore, may be able to provide some of the same functionality.[10]

APPLICATION-AWARE FIREWALL

This is very similar to deep packet inspection firewalls, except that the firewall understands certain protocols and can parse them, so that signatures or rules can specifically address the information being inspected. The flexibility of this approach to computer firewall protection is great and permits the signatures or rules to be both specific and comprehensive. There are no specific drawbacks to this approach to firewall security as generally it will yield improvements over a standard "deep packet inspection" approach. However, some actual attacks may be overlooked (false negatives) because the firewall security parsing routines are not robust enough to handle variations in real-world traffic where not all attack signatures are alike.[11]

Despite initial "firewall envy" about building the biggest and tallest firewall so that hackers cannot scale them, we know today that firewall envy is misplaced. A secure, holistically sound firewall is just one piece of the puzzle. And even next generation firewalls (which generally combine various of the elements

of deep-packet and application filtering) are only as good as their administrator, who is tasked with drafting rules and data interaction policies. Finally, today's malware may not contain any recognizable piece of data, code or signature that will allow even state of the art firewalls to catch it since the code might look like a legitimate piece of software.[12] It acts like the stealth fighter. Before you even know what hits you, a Side Winder missile is on your tail. As one expert recently noted, "Firewalls aren't really even part of the equation when you think about the threats that are out there….At the other end of every piece of malware, at the other end of every phishing campaign, is a person…The way we defend that is with people."[13]

ANTI-VIRUS SOFTWARE

Anti-virus software protects your network from an inbound attempt to implant a virus on your server. For the layperson, think of it as the flu shot you are supposed to get to ward off the flu each cold and flu season. There are many different types of anti-virus software available on the market. Here are the various capabilities of anti-virus software:

- **WATCHING** real-time activities on systems to check for suspicious activity; a common example is scanning all e-mail attachments for known viruses as e-mails are sent and received. Anti-virus software should be configured to perform real-time scans of each file as it is downloaded, opened, or executed, which is known as on-access scanning.
- **MONITORING** the behavior of common applications, such as e-mail applications, Web browsers, file transfer programs, and instant messaging software. Anti-virus software should monitor activity involving the applications most likely to be used to infect systems or spread malware to other systems.
- **SCANNING** files for known viruses. Anti-virus software on systems should be configured to scan all hard drives regularly to identify any file system infections and, optionally, to scan other storage media as well. Users should also be able to launch a scan manually as needed, which is known as on-demand scanning.
- **IDENTIFYING** common types of malware, viruses, worms, Trojan horses, malicious mobile code, and blended threats as well as attacker tools such as keystroke loggers and backdoors.
- **DISINFECTING** files, which refers to removing malware from within a file, and quarantining files, which means that files containing malware are stored in isolation for future disinfection or examination. Disinfecting a file is generally preferable to quarantining it because the malware is removed and the original file restored; however, many infected files cannot be disinfected. Accordingly, anti-virus software should be configured to attempt to disinfect infected files and to either quarantine or delete files that cannot be disinfected.[14]

Like the flu shot, having anti-virus software doesn't mean you will under no circumstances get a virus. Anti-virus software is designed to protect against a known set of viruses that "could" infect your network. It is not infallible.[15] It might not be able to catch "one of a kind" data signatures.[16] And very often it needs to be updated ("patched") as new viruses are detected and the anti-virus software needs to be updated. Companies need to develop written protocols around software updates and patching so that "immediate" fix patches, sometimes broadcasted by the federal government and software providers get brought into production at the earliest possible moment.[17] But as we further explain below, firewalls and anti-virus solutions are not the only solutions available.[18]

INTRUSION DETECTION DEVICES

Intrusion detection devices or systems are probably the most important part of a network security system given the fact that you are most certainly going to suffer an attempted data breach at some point in your business cycle. Simply put, "*Intrusion detection* is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible *incidents*, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices." [19]

Intrusion detection technology is very difficult to describe fully in a paragraph or two. There are two basic types of intrusion detection systems: host-based intrusion detection systems versus network-based intrusion detection systems. The difference is important. In general, a host-based network intrusion detection (HIDS) system monitors information on a secure network computer system or device for intrusions. One can think of a HIDS as an armed robotic guard that monitors whether anything or anyone, whether internal (i.e., a malicious insider) or external, has circumvented the system's security policy and inspects whether or not an intruder has left some trace of his intrusion like some evidence of malicious activity or software, or some modification to the network which leaves the intruder a back door to return someday to create more mischief. A HIDS keeps detailed logs of the captured event (like port and IP addresses) which can later be examined for evidence that a potentially malicious event occurred.

A network-based intrusion detection system monitors information transmitted across the network as the data source, i.e., meaning that by virtue of sensors it captures all network traffic. In theory, having these sensors, the network-based intrusion systems monitor information packets that cross the sensors to determine the nature of the electronic signature they carry. These signatures and other network information are captured via extensive logging of time, date, source and destination IP addresses, and number of bytes transmitted during the session. If electronic signatures are captured, they may be indicative of a possible attack. Some may not be so indicative, and may be disguised to "look and feel differently." A good network-based intrusion system is able to compare benign signatures with "cancerous" ones, and hopefully alert the guard to investigate a potential breach. An even better network-based intrusion system will automatically scan tens of thousands of logs and signatures a day looking for unusual activity which might signify an intrusion. [20]

As noted above, though network-based intrusion detection systems are important, they also are not infallible. Though certainly the major security companies know many "bad" electronic signatures, they do not know all of them. Today's malware is sneaky. It can look and feel to a normal computer technician like an innocent pizza delivery boy, when in reality it is a trained malware ready to wreak havoc on your network.

For this reason, the newest network-based intrusion detection systems are called "signature-less" or "anomaly-based" intrusion systems. They do not look for signatures per se. They look for unusual network behavior and identify unusual network traffic that may have no identifiable malware signature. Simply put, these systems look for anomalies in network traffic which may, when investigated, be indicative that something bad is occurring. As recently noted in a post-mortem report on the massive OPM data breach:

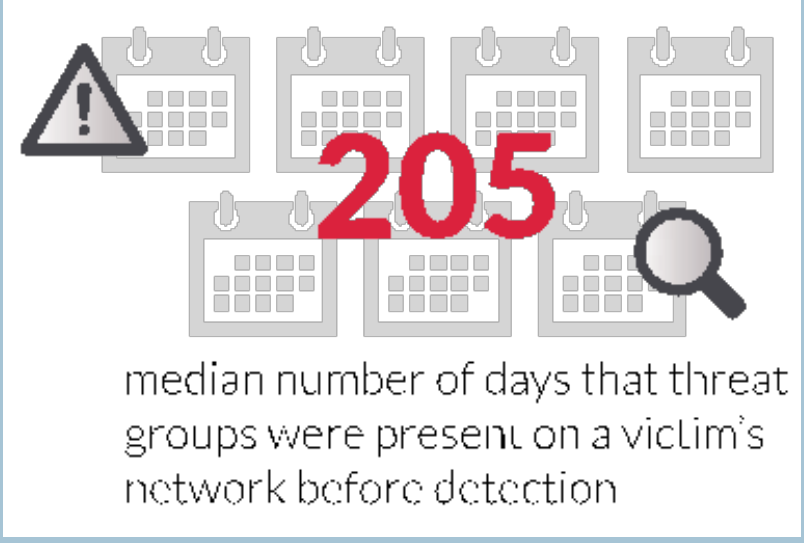
> "Novel malware can bypass detection, avoid run-time analysis and prevent post-incident traces in a number of ways undetectable to current defense-in-depth norms, [which are] as effective as trying to stop a laser pointer with a chain link fence.' Relying only on antiquated cyber defense systems, such as firewalls and antivirus programs, should be replaced by more innovative programs that can adapt and respond to the specific situation at hand. The brief recommended agency cyber

personnel institute a user behavioral analytics system, which creates a baseline profile of a user and detects and reports anomalous behavior."[21]

Simply put, it's better to know sooner rather than later if you've been hacked so corrective action can be taken. One expert notes, "Technology can help. [One intrusion detection system] uses complex algorithms and mathematical models to map what normal daily behavior on a network looks like and then flags up anomalies, such as a computer that suddenly starts downloading unusually large data files. The technology can also help spot hackers at work inside a system."[22]

This sort of signature-less intrusion detection technology is definitely needed and arguably required for a healthy network cybersecurity immune system. One very reputable computer networking and security firm, Cisco Systems, noted in its 2014 Annual Security Report "malicious traffic is visible on 100 percent of corporate networks." This means there is evidence that sophisticated criminals or other players have penetrated these networks and may be operating undetected over long periods of time. Another very reputable network security firm, FireEye, issued a report that the average time it takes for a company to detect it has been breached is 205 days.[24] And many firms (over 2/3) don't even detect breaches themselves. They unfortunately get a phone call from the FBI or Secret Service informing them of the breach. This is definitely not how you want to find out you've been hacked. Sometimes it may take even longer to know.[24]

The truth of the matter is that, many times, once an APT breaches the perimeter, the exfiltration of data and the intrusion occurs for months undetected. This aspect is clearly seen in past reports, such as "Operation Shady RAT." In this APT campaign, research indicated that many government entities and Fortune 100 companies had data exfiltrated by illegal perpetrators for as long as 28 months undetected.[25]



Source: FireEye

ACCESS SECURITY

Access security controls prevent unauthorized users from retrieving, using or altering information. These controls are composed of four basic elements: identification, authentication, authorization, and accounting. They are an additional part of the puzzle of good network security as they regulate who has access to the network, and what those users may or may not do with their level of access.

IDENTIFICATION AND AUTHENTICATION

As its core, identification means establishing a firm policy that every person allowed on the network has a user ID and that there is some method of authenticating such person as "actually" the person assigned to the user ID. Assigning a user ID is not hard. It is normally some combination of the person's first and last name.

Authentication is where the rubber meets the road. Authentication is the process of "proving" the user's identity before entering a system. Many authentication systems require the user to create and re-create complex passwords every 30 or 60 days. That unfortunately is easier said than done in reality. Where some users may be compliant, using non-specific combinations of letters, numbers, capitals and characters, others may stick to something they can readily remember, like foxhound2010, "Foxhound" (being the breed of your employee's beloved dog) and "2010," being the year his daughter was born, showing the employee's lack of ingenuity, along with the lack of proper password protection. The former password would be very hard to hack. The latter would take an experienced hacker a minute or two to figure out. That is the problem with passwords and password protection policies.

For those wedded to the password (at least for now), we recommend the following approaches to create a stronger password policy:

1. Companies should force employees to change their passwords regularly (preferably every 30 days), without exception;
2. Employee passwords cannot be common defaults such as "password," or "qwerty," or "12345";[26]
3. Employees should not store passwords on sticky notes placed on their computers or in a physical or digital file or folder called "password";
4. Employee passwords should be strong; rather than the first name of the employee's child, dog or cat, it should contain unique patterns of letters, numbers and other signs, like "I li6e cho$hlat@";
5. Employees should be required to install passwords on any device used to access company email or any company resources, including home laptops, so that they remain secure as well;
6. Companies should make sure that employees follow responsible "social media" practices with regard to company-specific information;
7. Companies should provide privacy screens to employees to prevent "shoulder surfing" (reading over an employee's shoulder); and
8. Employees should receive frequent training on spear phishing, so no employee inadvertently gives up his password to an unauthorized third party.

None of these policies alone is enough. A good, holistic cybersecurity password policy might include all of the above password strategies.[27]

Other and potentially better authentication systems exist. More advanced systems might use a token-based system assigned by a computer, iPad, iPhone or keychain token.[28] Others might require a retinal or fingerprint or thumbprint scan like that currently available on your iPhone.[29] Some organizations are even tinkering with voice recognition.

> "We've reached a point where usernames and passwords alone are no longer good enough. We've long had single sign-on technologies to remove the complexity of remembering multiple passwords, but what if someone else gets a hold of that single username and password? Now multi-factor authentication- which requires two or more factors to verify legitimacy of the user - has taken off and evolved pretty substantially in the past decade and we're now seeing authentication methods becoming as personalized and specific to the individual as the experiences they're trying to access."[30]

It is up to the CISO, CIO or security consultant to recommend what method of authentication works best for the particular business or enterprise involved - both its customers, and its employees. The fact remains, however, that a simple password alone is outmoded and outdated. The method, mode and means of identification and authentication will even become more important as the world transitions to a cloud-based information management network accessed by millions of endpoints. Next generation methods of securing these endpoints are already in process, and may dominate the cybersecurity industry down the road.

AUTHORIZATION AND ACCOUNTING

These are simpler concepts to understand. Authorization means creating a security policy that limits access to the computer network by a set of user rights or privileges. A mere employee might have one basic level of access to his own work product and nothing else. Accounting or finance personnel might have a different level of access to the company's financial statements or general ledger. A CFO or CEO might have even more access. Access should generally be limited on a "need to know" basis. Less access is obviously better than more.

Accounting is synonymous with "logging" what each individual user is doing on the network. Logs should be reviewed for unauthorized access to systems or areas theoretically unavailable based upon that user's set of network privileges. The log of a normal day's activity for any particular employee is a good comparison point when the next day his log shows that he has downloaded an unusually large amount of data.

INFORMATION SECURITY - ENCRYPTION

The final concept we will touch upon here is the concept of information security, i.e., keeping the confidentiality of data stored on the network. Confidentiality in the network security world is normally synonymous with "data encryption," the dictionary definition of which is the transformation of plain text into an unreadable cipher text. It is not necessary for a director or officer to know the basic types of encryption and decryption methods for transforming text into a cipher and back again into text. But it is important to know that encryption helps to better protect the data stored on the company's network, and is in fact sometimes required depending upon the business you are in, or the information you store (for instance, healthcare records kept by hospital systems or credit card data stored by a retailer.[31]

At its basic form, the most secure techniques of encryption

> "use a mathematical algorithm and a variable value known as a 'key'. The selected key (often any random character string) is input on encryption and is integral to the changing of the data. The EXACT same key MUST be input to enable decryption of the data. This is the basis of the protection... if the key (sometimes called a password) is only known by authorized individual(s), the data cannot be exposed to other parties. Only those who know the key can decrypt it. This is known as 'private key' cryptography, which is the most well-known form."[32]

THE END GAME

There is an awful lot of material in this chapter for a reason. Not because there will be a test at the end of the book. Because if you are a director of a US company your job is not to set up your company's cybersecurity architecture, but to ask the right questions of your CISO or CIO about what the company is doing, or not doing, and what hardware and software it is employing or not employing with regard to best cybersecurity practices. As we emphasize in the governance chapter, the goal for any director is to make reasonably well-informed and documented decisions regarding their company's cybersecurity policies, practices and procedures and to know how company resources and its budget are allocated to such protections.

ENDNOTES

[1] Please note that this chapter contains a lot of very technical terms. We mention them only to identify their importance in the cybersecurity ecosystem at any company and to enable you to understand how these technical terms and devices fit into a cybersecurity "best practices" scheme.

[2] See "Outsourcing: How Cyber Resilient Are You?" available at http://corpgov.law.harvard.edu/2015/07/26/outsourcing-how-cyber-resilient-are-you/ (noting that "Regulators are particularly concerned that the industry's third-party service providers are a weak link that cyber attackers can exploit. Financial institutions have become increasingly reliant on the information technology (IT) services these providers offer, either directly through the outsourcing of IT or indirectly through outsourced business processes that heavily rely on IT (e.g., loan servicing, collections, and payments). Regardless, banks remain ultimately responsible—they own their service providers' cyber risks.").

[3] See "CIOs and CISOs Can Learn From the Massive Sony Data Breach," found at http://mobile.blogs.wsj.com/cio/2014/12/05/cios-and-cisos-can-learn-from-the-massive-sony-data-breach/.

[4] See "Defense in Depth: An Impractical Strategy for a Cyber World," available at http://www.sans.org/reading-room/whitepapers/assurance/defense-depth-impractical-strategy-cyber-world-33896 (noting that "Defense in Depth was developed to defend a kinetic or real world military or strategic assets by creating layers of defense that compel the attacker to expend a large amount of resources, while straining supply lines. The tactical goal is to delay and render the enemy attack unsustainable."

[5] See "Defense in Depth has Always Been a Valid Concept," available at http://www.securityweek.com/defense-depth-has-always-been-valid-concept/ ("The concepts of defense in depth have been with us for years -- hundreds of years, if not thousands. Medieval castles embodied the very concept in their construction. Land was cleared so you could see the attacker coming up the glacis around the castle. The ground was made irregular to make a charge difficult. The castle was surrounded by pits and lined with spikes to make their traverse hazardous, or surrounded by moats if there was a water supply. Walls were tall and steep so they could not be climbed.")

[6] See "What is Firewall Security?" found at http://www.secureworks.com/resources/articles/other_articles/firewall-security/.

[7] See e.g., "Understanding Firewalls," available on the US-CERT ("Computer Emergency Readiness Team) website at https://www.us-cert.gov/ncas/tips/ST04-004.

[8] See "What is Firewall Security," available at http://www.secureworks.com/resources/articles/other_articles/firewall-security/.

[9] Id.

[10] Id.

[11] Id.

[12] See"Stealthy Regin malware is a 'top-tier espionage tool," found at http://www.cnet.com/news/stealth-malware-found-spying-on-telecoms-energy-sectors/.

[13] See "Cybersecurity Expert Puts Focus on Training People, Not Developing Technology," found at http://www.govtech.com/security/Cyber-security-Expert-Puts-Focus-on-Training-People-Not-Developing-Technology.html.

[14] See NIST Publication 800-83, "Guide to Malware Incident Prevention and Handling," found at http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf.

[15] Indeed there is some commentary that anti-virus technology may generally be outmoded or outdated at best. See "Antivirus is Dead: Long Live Antivirus!" available at http://krebsonsecurity.com/2014/05/antivirus-is-dead-long-live-antivirus/comment-page-1/.

[16] See "Antivirus software powerless against Sony hackers," available at http://www.usatoday.com/story/tech/2014/12/06/sony-attack-new-era-nuclear-option/19963063/. In this article, the FBI report on the data breach noted, ""This incident appears to have been conducted using techniques that went undetected by industry standard antivirus software…."

[17] See e.g., "Heartbleed security patches coming fast and furious," found at http://www.zdnet.com/article/heartbleed-security-patches-coming-fast-and-furious/.

[18] See "Cybersecurity requires more than 'patch and pray,' found at http://www.sfchronicle.com/business/article/Cybersecurity-requires-more-than-patch-and-5938625.php.

[19] See NIST Publication 800-94, "Guide to Intrusion Detection and Prevention Systems," found at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=50951.

[20] See "Theft of F-35 design data is helping U.S. adversaries -Pentagon," found at http://www.reuters.com/article/2013/06/19/usa-fighter-hacking-idUSL2N0EV0T320130619; "Chinese Hacked U.S. Military Contractors, Senate Panel Says," available at http://www.wsj.com/articles/chinese-hacked-u-s-military-contractors-senate-panel-says-1410968094.

[21] See Security Experts Point to OPM's Biggest Cybersecurity Failure," available at http://www.nextgov.com/cybersecurity/2015/07/security-experts-point-opms-biggest-cybersecurity-failure/118274/.

[22] See "Digital Disease Control," available at http://ww2.cfo.com/applications/2014/07/digital-disease-control/. Some advanced network security devices can help correlate large amounts of network events in order to allow companies to better identify which security alerts which are generated should be prioritized and investigated further, and which events potentially can be ignored as false positives. See also "The SIEM Who Cried Wolf: Focusing Your Cybersecurity Efforts on Alerts That Matter," available at https://www2.fireeye.com/rs/fireye/images/fireeye-alerts-that-matter.pdf?mkt_tok=3RkMMJWWfF9wsRolu6%2FLcu%2FhmjTEU5z17%2B0tWaC0hYkz2EFye%2BLIHETpodcMT8JiNb%2FYDBceEJhqyQJxPr3NKNgN3tx5RhPmCg%3D%3D.

[23] See M-Trends 2015: A View from the Front Lines," available at https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf.

[24] Id.

[25] See "Know your traffic: The case for egress monitoring and filtering," available at http://www.scmagazine.com/know-your-traffic-the-case-for-egress-monitoring-and-filtering/article/370851/.

[26] See "As hacking grows, biometric security gains momentum," available at http://phys.org/news/2015-03-hacking-biometric-gains-momentum.html.

[27] For other password and cyber employee awareness strategies, see "Is Employee Awareness and Training the Holy Grail of Cybersecurity?" available at http://www.weil.com/~/media/files/pdfs/httpsinteractweilcomreactionmailings150309cybersecurityalert.pdf.

[28] Id.

[29] Some term this "multi-factor authentication." See e.g., "What is Azure Multi-Factor Authentication?" available at https://azure.microsoft.com/en-us/documentation/articles/multi-factor-authentication/.

[30] See "Barclays to roll out biometric voice authentication," available at http://www.itsecurityguru.org/2014/06/23/barclays-roll-biometric-voice-authentication/. Others have talked more recently about biometric tattoos. See also "Hidden Risks of Biometric Identifiers and How to Avoid Them," available at https://www.blackhat.com/docs/us-15/materials/us-15-Keenan-Hidden-Risks-Of-Biometric-Identifiers-And-How-To-Avoid-Them-wp.pdf.

[31] See e.g., "Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals," found at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.

[32] See "Why Have Cryptography," available at http://www.cryptographyworld.com/what.htm.

CHAPTER 3:
CLOUD BASED CYBERSECURITY CONCERNS

PURPOSE OF THIS CHAPTER:

1. Identify the various cloud-based platforms that are available in the marketplace for an end-user.
2. Identify the various cloud-based models that cloud service providers are offering.
3. Identify the cybersecurity concerns that a Director should investigate if their CISO or CFO is pressing a move towards the cloud.
4. Identify the importance of user identification and authentication in a cloud environment.

Over the last few years, there has been a tremendous amount of literature published on moving data storage of companies to a "cloud environment." What exactly is the cloud? According to our son, the cloud is that white puffy thing in the sky that periodically floats over our house, and sometimes brings rain to our garden. To some of my clients after explaining to me their corporate governance and risk management structures, I am sometimes referred to as the "black cloud," as I tell the clients, albeit gently, "we are going to have to change things around *just* a little bit."

These simple examples are really the point of this chapter. The cloud means different things to different users. On one hand, cloud based network computing is considered to be one of the most important business innovations of the last decade[1], allowing companies, and even many federal and state government agencies, to store and access large amounts of data (even highly confidential "state secrets") without the need to buy hundreds of thousands (or even millions) of dollars of state of the art computer servers and the continuing cost of having to physically secure, manage them, patch them, and otherwise maintain them.

The move to the cloud has been rapid and is expected to accelerate. According to one study, "More than two-thirds (69%) of companies have already made cloud investments. The rest [of these companies] plan to do so within the next three years. Overall, companies appear to be moving steadily: respondents anticipate their cloud usage will expand, on average, by 38% in the next 18 months. At the end of 2015, companies expect to be operating an average 53% of their IT environments in the cloud."[2] In one recent report it was noted that the adoption of the cloud continues to grow rapidly, with Gartner forecasting $282 billion in spending by 2018.[3] The push to adopt cloud technology is not only in "brick and mortar" businesses, but in the financial sector as well.

"As financial services adopt the cloud, strict compliance regulations and corporate policies push them to be early adopters of security technologies," said Pravin Kothari, founder and CEO, CipherCloud. "At the same time, the influence of cloud has upped the ante for financial services firm CISOs and their teams. As these companies increase their cloud adoption, they are building data protection in the cloud with the help of innovative encryption and tokenization technologies. Both regulatory scrutiny and the pace of data breaches compel the increased protection of their sensitive information."[4]

However, the inherent flexibility and variety of cloud-based services a user can buy creates different levels of security concerns and compliance issues that must be understood well before the customer decides to sign a contract with a cloud service provider to store the specific type of data he or she wishes to move to the cloud.[5] One recent survey issued by Symantec notes that: "Among non-users of the cloud, about seven in 10 (68%) cite concerns over data security as the number one roadblock to cloud implementation of any kind within their organization. These concerns are more likely to be echoed by C-level executives than IT management (74% vs. 61%)."[6] These security concerns may further sensitize companies to the need to buy cyber insurance as well. "Breaches will continue to occur on a regular basis, forcing organizations to look toward adopting cyber insurance… [T]aking advantage of all applicable security measures to mitigate against cyber risk will become the enterprise battle cry."[7]

This chapter deals with the topic of cloud-computing and the security concerns that are associated with the various platforms and levels of service a company can purchase if it makes the decision to move its data operations to a cloud-based environment hosted by a "cloud service provider" or "CSP." As some of the associated terms related to cloud computing are difficult to understand, we are going to try and boil down cloud computing to the more relevant concepts a business person must understand in order to make a business judgment as to whether to abandon their servers for the cloud, or keep their data storage "ground based" and 100% exclusively within their custody and control.

CLOUD BASED MODELS

Like the various clouds one might find in the sky, there are many different types of cloud-based models that a customer can contract for:

Private Clouds

"A private cloud is a particular model of cloud computing that involves a distinct and secure cloud based environment in which only the specified client can operate. As with other cloud models, private clouds will provide computing power as a service within a virtualized environment using an underlying pool of physical computing resource. However, under the private cloud model, the cloud (the pool of resource) is only accessible by a single organization providing that organization with greater control and privacy."[8] (emphasis added). Think of the private cloud as the "single family housing" of cloud environments. The owner controls the security. The front door, the back door and the side door. The owner is the only one who has access to his or her own information. Obviously, the more sensitive the information the more likely one is to opt for the private cloud solution.[9]

Public Clouds

"The most recognizable model of cloud computing to many consumers is the public cloud model, under which cloud services are provided in a virtualized environment, constructed using pooled shared physical resources, and accessible over a public network such as the internet."[10] Think of the public cloud as the "multi-family condominium" of cloud environments. Users of a public cloud have an infinite amount of computer power to power their operations, but at economic prices far less than if they were to secure dedicated resources for themselves. "Public cloud services often employ a pay-as-you-go charging model whereby the consumer will be able to access the resource they need, when they need it, and then only pay for what they use; therefore avoiding wasted capacity."[11] A public cloud could have hundreds, if not thousands, of individual users. Some of the largest public cloud providers today include Amazon Web Services and Microsoft Windows Azure.

Hybrid Clouds

A hybrid cloud is an integrated cloud service utilizing both private and public clouds to perform distinct functions within the same organization. An organization can maximize their efficiencies by employing public cloud services for all non-sensitive operations, only relying on a private cloud where they require it and ensuring that all of their platforms are seamlessly integrated.[12]

THE DIFFERENCE BETWEEN IAAS, PAAS, AND SAAS

There are generally thought to be three different cloud based service provider models currently.[13]

- **INFRASTRUCTURE AS A SERVICE (IAAS):** Think of IaaS as if you decided to rent a fully networked and wired one-room school house and start teaching classes in cybersecurity. To do this you sign a lease renting the building. That lease allowed you to not only have access to the building, and its desks and chairs (e.g. the servers), the computers, and the servers supporting them. IaaS is the first floor of your cybersecurity school.[14] If you choose this route, it's up to you to supply the lesson plans (i.e. the operating systems), the school books (the applications) and the security guards (the cybersecurity process, software and procedures) to protect your students. In reality, if you choose Iaas, your cybersecurity concerns are no different than if you had a row of servers in your data center on premises.

- **PLATFORM AS A SERVICE (PAAS):** So your Cybersecurity school becomes popular, and you decide that you need to have more functionality and flexibility in your class offerings. You then start to think that you may need to switch to a PaaS architecture (which will necessitate adding a second floor to your school house). Building the second floor will allow your students to build and test applications, build specialized databases for their projects, and other tools to support your school.[15] The trade-off here is that cybersecurity functions will likely be more evenly allocated between you and the lessor since the responsibility for developing and securing your applications falls upon you.

- **SOFTWARE AS A SERVICE (SAAS):** So your Cybersecurity school is really successful and your students are demanding more functionality and off-the-shelf applications that will allow you to ramp up your teaching experience. A third floor for your school house thus needed above IaaS and PaaS. SaaS provides the total user experience for your students, and provides all the additional applications and tools your students need to succeed. Saas is the real deal: it provides the most functionality and the highest level of security offered to a customer.[16]

Dealing with Security Realities of Cloud Computing and Assessing the Risk

Here is really where, again, the rubber meets the road. As you go up the stairs in your school house from Iaas to SaaS to focus on different activities (and depending upon the public/private nature of the cloud service you contract for), your overall security concerns generally lessen. On the first floor (IaaS), the cloud provider is only responsible for physical and environmental security. The customer is responsible for security that relates to the IT system, the operating system, the applications and the data. Should you add on a third floor to your school house to reach a SaaS environment, the cloud provider is responsible for not only the physical and environmental controls, but also the security controls for the infrastructure, the applications and the data.[17]

The variability in security responsibilities as between the customer and cloud provider supplies the framework for necessary discussions internally between the various business constituencies involved in the decision regarding potential migration to the cloud. These discussions will end with a contract between the user and CSP, which hopefully will reflect which bells and whistles the user wishes to have.

The discussion is generally one of cost-benefit and risk-reward: knowing that it is likely cheaper to migrate many operations to the cloud to avoid infrastructure costs and create a flexible, expandable data storage structure, the customer then needs to have a fulsome discussion internally as to where it wishes the cybersecurity risk over its most sensitive business information to reside, i.e., either in its own server room down the hall, or if it is comfortable with the security requirements that are set forth under the respective SLA (and the company has sufficient transparency into those requirements and compliance measures to be comfortable with them), with the cloud service provider. Another alternative might be to have the security risk split between the customer and the client in a hybrid cloud environment. This is especially true when thinking about storing either personally identifiable information ("PII") or financial information in a cloud environment. For instance, many companies opt only to store email data, or sales and marketing data in the cloud, leaving financial data and health data "on the ground" behind lock and key or in a private cloud only accessible by the customer.[18] Again, these are not easy decisions to make. They should be discussed with your information management consultants, and especially your data protection lawyers if you are a multinational company that stores data overseas.

Prior to engaging with a cloud service provider, we would recommend a thorough investigation to make sure both the CSP and the security being offered is right for your organization. That investigation should include:

1. A review of the provider's incident response and disaster/data recovery policies. This is no different than with ground based server technology, yet sometimes infinitely more complicated with a cloud-based environment since the cloud may not be under your control. Indeed, "Companies are forced to fight attackers on multiple geographic fronts, but the complexities of the internet cloud and a patchwork quilt of data privacy laws means a prompt response is often difficult."[19] Transparency and visibility into the incident response plan is key and may be one of the deciding factors as to how, and by which method, companies should proceed to a cloud-based environment.

2. Transparency and visibility into the cloud providers own employee training and screening processes, like:

    - Lack of employee screening and poor hiring practices - some cloud providers may not

perform background screening of their employees or providers. Privileged users such as cloud administrators usually have unlimited access to the cloud data.

- Lack of customer background checks - most cloud providers do not check their customer's background, and almost anyone can open an account with a valid credit card and email.
- Lack of security education - people continue to be a weak point in information security. This is true in any type of organization; however, in the cloud, it has a bigger impact because there are more people that interact with the cloud: cloud providers, third-party providers, suppliers, organizational customers, and end-users. [20]

3. A review of the provider's own security policies and procedures, and documentation supporting such. A recent study by the Ponemon Institute, entitled "Data Breach: The Cloud Multiplier Effect," (hereinafter, the Ponemon Cloud Report") 62 percent of the respondents surveyed were unsure that cloud services are thoroughly vetted before deployment, and 63 percent believed there is a lack of vigilance in conducting audits or assessments of cloud-based services." [21]
4. A review of the provider's accreditation with certain well-known security umbrella organizations such as FedRamp, ISO 27018, or the National Institute of Standards and Technology Special Publication 800-171, which may give the Organization a greater sense of comfort that the CSP's own internal security procedures have been vetted by a third party (here the US government or the International Organization for Standardization); [22]
5. A review of what international or federal regulations a customer may be required to comply with if it chooses to move its data to the cloud (i.e. Gramm Leach Biley Act (GLBA), HIPAA or standards such as PCI DSS 3.1). These regulations may influence what level of cloud service is practical given the security regulations which already may apply to you, and how you document compliance with such regulations. "The architecture of your cloud environment is key and you must understand the respective data storage regulations in the countries you operate in. In general, you must look for cloud security solutions that are compliant with regulations like HIPAA, PCI DSS ver. 3.1, EU data protection laws, or whichever laws apply to you."[23] You should not have to guess about compliance. The CSP you choose is either complaint or not. Demand proof that the cloud you choose is complaint pursuant to the regulations or laws you are governed by.
6. A review of the customer's ability to periodically review or audit the security environment during the length of the contract to assure not only the continuing state of the cybersecurity environment, but its compliance with internal security policies, procedures and other federal and state regulations that may govern it; additionally, the organization needs to have visibility into the CSP's operational, outage and performance records so that there is some way to measure the quality and quantity of service being provided; [24]
7. A review of the provider's physical and back up storage and locations (just in case a malicious hacker tries to wipe out your database), and
8. A review and thorough discussion of the level of communications to be provided to the customer if there is a breach of their CSP. Indeed, in the Ponemon Cloud Report, 72% of the respondents were unsure that their CSP would notify them immediately if they had a data breach involving the loss or theft of their intellectual property or business confidential information. [25]

PROTECTING DATA SENT TO (AND FROM) THE CLOUD

As with cybersecurity precautions that need to be taken with customer-owned servers, cloud based data storage solutions also require data protection when information is moving to, from and within the cloud.

Though explaining the details of data protection within the cloud is beyond the scope of this book, three basic areas should be discussed by directors and officers when considering moving to a cloud-based environment: encryption, database monitoring, and authentication requirements for authorized users.

Encryption means what it says. It is the process of encoding messages or information in such a way that only authorized parties can read it. There are too many different methods of encryption to describe. The point here is that data should be encrypted by the customer before it is sent over an unsecured network to the cloud.

Once at the cloud-based destination, the data needs to monitored, in real time, for suspicious activity and for potential violations of access policies set by the customer. Real-time monitoring is critical in the present threat environment so that the customer's or provider's incident response plan can be initiated if necessary. This is not very different from the type of monitoring that is ideal for ground-based network servers. The more visibility into the cloud service provider and how your data is being stored the better.[26] One cloud expert recently noted, "IT leaders need insight into the entire data-hosting network system - locally, regionally and globally - to ensure that compliance standards are met and that the provider is operating transparently." [27]

Finally, companies considering a move to one form or another of a cloud environment need to re-double their efforts to make sure that only authorized users can access the cloud in an authorized manner pursuant to a written cloud cybersecurity policy. Here again is where the rubber meets the road as the biggest risk to a cloud environment is not generally the cloud architecture, but the individual cloud user.[28] It only takes one unauthorized action to wreak havoc on your cloud network. For instance, "[u]sing unauthorized cloud or mobile applications can compromise confidential corporate assets and lead to data leaks largely because these applications are unmonitored—that is, the company and IT department lose visibility and control of the information…."[29]

Strong passwords and multi-factor authentication should be the rule, not the exception. As recently noted for users thinking about moving to the cloud:

> "You'll have a rash of things to consider, ranging from what types of identities (log-on names, biometric tokens, smartcards, etc.) are allowable, to what authentication mechanisms are required to access a cloud service. You'll need to know what processes the CSP uses for provisioning and deprovisioning users, and what level of assurance the CSP's authentication provider's offer. The size of passwords or PINs, the frequency with which they're updated, how log-on credentials are stored and protected are all vital parts of the puzzle."[30]

In sum, cloud computing is one of the most exciting areas in the whole area of network computing and data storage solutions. It is scalable, efficient, and certainly less costly than ground based solutions. But it is certainly not without its security concerns. Here, there is no question that cloud data management and security consultants should be consulted well before a cloud based deployment decision, in order to vet the types of cloud environments an organization should consider as well as the level of security that is provided.[31]

ENDNOTES

[1] See "Top ten ways cloud computing drives innovation," found at http://thoughtsoncloud.com/2014/04/top-ten-ways-cloud-computing-drives-innovation/.

[2] See "Cloud Computing Continues to Make Inroads," found at http://core0.staticworld.net/assets/2014/11/03/2014-cloud-computing-idge-survey.pdf.

[3] See "Cloud encryption and tokenization trends in financial services," available at http://www.net-security.org/secworld.php?id=18688.

[4] Id.

[5] See e.g., "9 Worst Cloud Security Threats," available at http://www.informationweek.com/cloud/infrastructure-as-a-service/9-worst-cloud-security-threats/d/d-id/1114085.

[6] See "Protecting Corporate Information in the Cloud," available at http://www.databreachtoday.com/func_whitepapers_count.php?wp_id=1856.

[7] See 2015's top cloud security trends," available at http://blog.trendmicro.com/2015s-top-cloud-security-trends/.

[8] See "What is a Private Cloud?" available at http://www.interoute.com/cloud-article/what-private-cloud.

[9] See e.g., "Six cloud security predictions for 2015," available at http://www.scmagazine.com/six-cloud-security-predictions-for-2015/article/388926/ ("The private cloud has been a popular choice in recent years as enterprises looked to take advantage of the control, customization and other benefits offered by the cloud while simultaneously ensuring their security requirements were met").

[10] See "What is a Public Cloud?" found at http://www.interoute.com/cloud-article/what-public-cloud.

[11] Id.

[12] See "What is a Hybrid Cloud," found at http://www.interoute.com/cloud-article/what-hybrid-cloud.

[13] Cloud picture, available at https://www.porticor.com/2013/02/cloud-compliance-responsibility/.

[14] See "Cloud Computing Service Models," found at http://cloud.cio.gov/topics/cloud-computing-service-models. The Federal Risk and Authorization Management Program (affectionately known as "FedRamp"), is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services provided to the Federal Government. Since there are no generally accepted standards for judging the cloud-based cyber-security for private industry, many look to FedRamp as "a" standard to compare civilian-based cloud solutions.

[15] Said a little differently, in a PaaS environment, your students will use the "CSP's computing environments, tools, and libraries to create, test, manage, and host software applications." Id.

[16] Since CSP's are third parties, contracts are normally entered into between the customer and the CSP, called a service level agreement, or "SLA." Normally SLA's are negotiable as between the consumer and provider as to the services and security levels between provided by the cloud provider. It is very important to vet SLA's with not only your lawyers but your system administrator so that each party knows their respective legal and actual responsibilities when it comes to all cybersecurity related concepts and objectives (especially incident response). For a more exhaustive list of critical SLA provisions that companies should consider, see "One 'Giant Leap' to a Secure Cloud Platform for U.S. Corporations," available at http://www.dandodiary.com/2015/05/articles/cyber-liability/guest-post-one-giant-leap-to-a-secure-cloud-platform-for-u-s-corporations/.

[17] See e.g., "An analysis of security issues for cloud computing," available at http://www.jisajournal.com/content/4/1/5 ("With SaaS, the burden of security lies with the cloud provider. In part, this is because of the degree of abstraction; the SaaS model is based on a high degree of integrated functionality with minimal customer control or extensibility.")

[18] See"Cloud Security Spotlight Report," available at http://media.scmagazine.com/documents/114/cloud-security-spotlight-repor_28381.pdf.

[19] See "Cloud service providers often not set up for incident response," http://www.computerweekly.com/news/2240203007/Cloud-service-providers-often-not-set-up-for-incident-response.

[20] See "An analysis of security issues for cloud computing," found at http://www.jisajournal.com/content/4/1/5.

[21] See "Data Breach: The Cloud Multiplier Effect," found at http://go.netskope.com/rs/netskope/images/Ponemon-DataBreach-CloudMultiplierEffect-June2014.pdf.

[22] See list of FedRamp Cloud Service Providers, found at http://cloud.cio.gov/fedramp/cloud-systems; see also "Microsoft Azure is first major cloud provider to adopt ISO 27018 privacy standard," available at http://www.networkworld.com/article/2884641/microsoft-subnet/microsoft-azure-is-first-major-cloud-provider-to-adopt-iso-27018-privacy-standard.html (noting that Microsoft Azure in February 2015 became "the first major cloud provider to adopt the world's first international standard for cloud privacy."); "Need NIST Compliance in the AWS Cloud? AWS Compliance Has You Covered: NIST 800-171," available at http://blogs.aws.amazon.com/security/post/Tx115XWF9J5G4MM/Need-NIST-Compliance-in-the-AWS-Cloud-AWS-Compliance-Has-You-Covered-NIST-800-17.

[23] Top Cloud Computing Security Issues and Solutions, available at http://www.cloudave.com/34670/top-cloud-computing-security-issues-solutions/; "2015 AWS PCI Compliance Package Now Available," available at http://blogs.aws.amazon.com/security/post/Tx1GWQCS34C0A2B/2015-AWS-PCI-Compliance-Package-Now-Available (noting that AWS has been successfully validated against standards applicable to a Level 1 service provider under PCI DSS Version 3.1).

[24] See "NIST puts a sharper point on Cloud Computing," found at http://www.zdnet.com/nist-puts-a-sharper-point-on-cloud-computing-7000034990/.

[25] We will discuss incident response and recovery plans in Chapter 8. As we note later, just like in ground-based servers, incident response and disaster/data recovery plans are likely the most important part of any cloud data storage solution. These plans should be exhaustively set forth in the SLA. Incident response plans will vary significantly depending upon which cloud based model is used.

[26] See "5 Ways to Make Public Cloud More Secure," available at http://www.esecurityplanet.com/network-security/5-ways-to-make-public-cloud-more-secure.html ("[S]ecurity is needed in three places: entering or exiting the corporate network, entering or exiting the cloud provider and within the cloud itself.").

[27] See "Visibility, agility key for successful cloud security," available at https://www.datapipe.com/blog/2015/08/18/visibility-agility-key-for-successful-cloud-security/.

[28] See "Survey Roundup: Cloud Security Risks of the Highly Privileged," available at http://blogs.wsj.com/riskandcompliance/2015/08/28/survey-roundup-cloud-security-risks-of-the-highly-privileged/.

[29] See "Protecting Corporate Information in the Cloud," available at http://www.databreachtoday.com/func_whitepapers_count.php?wp_id=1856.

[30] See "Cloud Security: A New Security Model for The Cloud Era," available at http://core0.staticworld.net/assets/media-resource/15675/ast-0082898_cloud_security_v2.pdf. See our discussion of Access and Authentication Issues in Chapter 2 above.

[31] Certainly one of the most comprehensive cloud based data storage/management consultants is IBM. See http://www.ibm.com/cloud-computing/us/en/. Other well-known providers are Amazon Web Services (which is a major provider of cloud services to the United States government, see http://aws.amazon.com/govcloud-us/, as well as Microsoft Azure, see https://azure.microsoft.com/en-us/.

CHAPTER 4:

THE NEW AGE OF CYBER ENTERPRISE RISK MANAGEMENT FOR DIRECTORS

PURPOSE OF THIS CHAPTER:

1. Identify the role of the Board of Directors in cybersecurity oversight.
2. Identify relevant standards of liability in Delaware for breach of fiduciary duty.
3. Identify a "checklist" of cyber governance related questions Boards must be asking their executives (and themselves) on a regular basis regarding the cybersecurity posture of their company to help protect their company and potentially themselves personally from exposure due to a data breach.
4. Identify the potential importance of the NIST cybersecurity framework as it pertains to a Director's fiduciary duties.

While the Caremark case may not have had the wide-ranging impact envisioned by some, and may actually have been overtaken by rules and regulations imposed by Congress, the SEC and self-regulatory organizations, it still has served as a wake-up call to corporate America…emphasizing the need for increased monitoring of corporate affairs before they get out of hand.[1]

> For those worried that what happened to Sony could happen to you, I have several pieces of advice. The first is for organizations: take this stuff seriously. Security is a combination of protection, detection and response. You need prevention to defend against low-focus attacks and to make targeted attacks harder. You need detection to spot the attackers who inevitably get through. And you need response to minimize the damage, restore security and manage the fallout. [2]

Among the most notable cybersecurity breaches in the public company sector in 2013 was that which hit Target Corporation. This attack involved the alleged loss of approximately 40 million credit and debit cards, 70 million or more pieces of personal data, and a total estimated cost of the attack to date of approximately $300 million.[3] It was remarkable on several levels, not just on the enormity of the breach and its aftermath, but because it focused attention on public company directors with respect to their duties to oversee the enterprise risk management of their organization. Justified or not, ISS issued a voting recommendation against the election of all members of Target's audit and corporate responsibility committees - seven of its ten directors - at its then upcoming annual meeting. ISS's reasoning is that, in light of the importance to Target of customer credit cards and online retailing,

> "[the] failure of the committees to ensure appropriate management of these [cyber] risks set the stage for the data breach, which has resulted in significant losses to the company and its shareholders.[4] Though the ISS bid was unsuccessful, the ISS report "puts corporate board members on notice to treat the risks associated with cyberattacks more seriously, particularly directors at retailers which store vast amounts of data like credit card numbers and personal information that cybercriminals seek. Other retailers … have fallen victim to cyberattacks where credit-card information was compromised. The ISS move is raising a red flag about risk oversight that is a growing issue for boards…."[5]

If the reputational black eye apparently suffered by Target and its fellow retailers was not enough of a "red flag" to the US corporate community, then maybe the cyber breach lawsuits filed in 2014 were. Calendar year 2014 progressed with breach after breach, and lawsuits piled up against companies that suffered cyber-attacks. At least 140 customer lawsuits were brought against Target alone, which have recently been allowed to proceed past the motion to dismiss phase (these do not include suits brought by banking partners against Target relating to the breach, which have also been allowed to proceed).[6] At least 50 class actions have been filed against Anthem Healthcare relating to its data breach in 2015. At least 31 actions have been filed against Home Depot arising out of their breach.[7] And then there was Sony Pictures, in which at least 6 lawsuits have been filed by ex-employees relating to Sony's late November 2014 breach.

So clearly over the last eighteen months, the risk calculus for cybersecurity breaches has changed in many different ways:

1. Prior to 2014 the risk of customer class actions had been thought to be negligible. Not today. The Adobe, Target, Neiman Marcus and Schnuck Market's lawsuits have all survived motions to dismiss their consolidated complaints.
2. Prior to 2014, the risk of suits against directors and officers of public companies that have had cybersecurity attacks was also discounted severely. Not true today. And many of these actions are still being litigated.
3. The average cost of responding to a cyber-attack for U.S. companies has been increasing steadily.
4. The number of cyber-attacks has increased significantly year over year to the point where one cannot say these are random events.
5. The destructiveness of the cyber-attacks and rampant theft of customer, employee and patient data has now been evidenced with 18 months of hard data.

This path leads us to the Board of Directors. Charged with generally overseeing the affairs of the Company, a board now must factor in to its analysis not only the hazard risk that their company may face (i.e., property damage, flood damage or natural catastrophes, like hurricanes and earthquakes) but also the cyber risk its Company may face. Unlike many other aspects of directing the affairs of a public company (like overseeing its financial reporting function and obligations), "cybersecurity" is new for many directors, and is certainly far from intuitive. This chapter will focus specifically on the responsibilities of public company directors to oversee their company's cybersecurity program (within the framework of the company's enterprise risk management structure), the basic questions directors should be asking about

a company's cybersecurity program, incident response and crisis management program, and lastly, the potential value of a stand-alone cyber insurance policy to transfer some of the risk of a cyber-attack to a reputable insurance carrier.

Directors' Duty of Oversight with Respect to Cybersecurity/Other Duties and Regulations Lurking About for Directors

> [T]he board cannot and should not be involved in actual day-to-day risk management. Directors should instead, through their risk oversight role, satisfy themselves that the risk management policies and procedures designed and implemented by the company's senior executives and risk managers are consistent with the company's strategy and risk appetite, that these policies and procedures are functioning as directed, and that necessary steps are taken to foster a culture of risk-aware and risk-adjusted decision making throughout the organization. The board should establish that the CEO and the senior executives are fully engaged in risk management and should also be aware of the type and magnitude of the company's principal risks that underlie its risk oversight. Through its oversight role, the board can send a message to management and employees that comprehensive risk management is neither an impediment to the conduct of business nor a mere supplement to a firm's overall compliance program, but is instead an integral component of strategy, culture and business operations.[8]

Thus, as a general rule, "the business and affairs of every corporation…shall be managed by or under the direction of a board of directors…." See D.G.C.L. Section 141(a). A public company director's "duty of oversight" or "fiduciary duty to monitor" generally stems from the concept of good faith. As noted in the seminal Delaware Chancery Court case, In re Caremark Int'l, Inc. Derivative Litigation,[9] as a general matter "a director's obligation includes a duty to attempt in good faith and loyalty to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that the failure to do so in some circumstances, may, in theory, at least render a director liable for losses caused by non-compliance with applicable legal standards."

This simple statement, however, does not come without a high hurdle to meet.[10] To find liability under Chancellor William Allen's duty of oversight a plaintiff must either show that:

- The board must have failed to provide reasonable oversight in a "sustained or systemic" fashion, and
- The information reporting system on which the board must have relied must have been an "utter failure."[11]

Importantly, under Caremark, the actual failure to prevent wrongdoing does not in and of itself mean the information reporting system "is an utter failure." A court must also consider the design of the system, how it was tested and maintained by management, and how employees were trained under the provisions set forth in the system. Caremark thus sets forth a holistic approach to determining the level of board oversight. In sum, trying to set up a system of oversight and control over cybersecurity with appropriate supervision and control is much better than not trying at all and sticking one's head in the sand.[12]

In a later Delaware Supreme Court case, Stone v. Ritter, the Court refined the Caremark standard as a two part test, where liability stems from either:

- Utterly failing to implement any reporting or information system or controls, or
- Having implemented such system or controls, consciously failing to monitor or oversee its operations.[13]

Noting the liability for failure to monitor in terms of a "conscious failure," the Delaware Supreme Court placed an inherent scienter requirement for plaintiff's attempt to surmount. But the hope obviously is that such a suit never comes into fruition based upon a board's conscious attempt to stay reasonably informed about the enterprise risk management of their Company. Indeed, the business judgment rule generally protects a director's "informed" and "good faith" decisions unless the decision cannot be attributed to any rational business purpose, or the directors breached their duty of loyalty in making such decision.[14]

In today's world it would be hard to question that cybersecurity should not be part of any organization's enterprise risk management function, and thus, by inference, part of any director's duty of oversight. Indeed, the plaintiffs' securities class action bar has filed three shareholder derivative actions against the boards of directors of Target, Wyndham Worldwide Hotels, and The Home Depot[15] as a result of their publicly reported cyber breaches. In these complaints, the plaintiffs alleged, among other things, that the directors "failed to take reasonable steps to maintain their customers' personal and financial information in a secure manner" and/or "breached their fiduciary duties of loyalty, good faith, and due care by knowingly and in conscious disregard of their duties.[16] Indeed, Securities and Exchange Commissioner Luis Aguilar confirmed this exact cyber governance point in his June 10, 2014 speech, entitled "Cyber Risks in the Boardroom," that:

> "[E]nsuring the adequacy of a company's cybersecurity measures needs to be a critical part of a board of director's risk oversight responsibilities. In addition to the threat of significant business disruptions, substantial response costs, negative publicity, and [the] lasting reputational harm [that could result from a cyber-attack], there is also the threat of litigation and potential liability for failing to implement adequate steps to protect the company from cyber-threats."[17]

As was made clear by the questioning of the panelists in the SEC Cyber Roundtable, on March 26, 2014 (see Webcast of SEC Cyber Roundtable, dated March 26, 2014),[18] there are other reasons for directors to be intimately involved with decisions concerning a company's cybersecurity, i.e. "the regulators." Over the last several months, not only has the SEC been more involved generally with cyber "thinking," and security issues, but also the Office of Compliance, Inspections and Examinations of the SEC (governing investment advisors and asset managers), and the Financial Industry Regulatory Authority (FINRA), are all in the game.[19] So is the Federal Trade Commission, FDIC, Office of the Controller of the Currency[20] and FCC,[21] as well as state regulators, such as, e.g., the New York State Department of Financial Services. Each of these organizations has their own exhaustive list of factors or areas of examination/consideration. These lists are long and extensive. And we have yet to see whether the SEC will issue additional guidance to public companies concerning what information is required to be disclosed to investors concerning cybersecurity incidents.[21]

The failure to adhere to regulations or guidance concerning cybersecurity can be especially troublesome because of the concept of "red flags," i.e. danger signs that something is wrong within the organization. There are all sorts of red flags, and many do not rise to the level of trouble. For instance, the fact that a Company has thousands of potential cyber incident intrusion alerts every day might be viewed by an SEC OCIE examiner as a normal occurrence within any major financial organization. However, a

later revealed fact that the Company has no written cyber "incident" response plan and no information management business continuity plan might be viewed by a regulator as a very basic failure to appreciate potential cybersecurity risks and thus a huge "red flag" that might cause the Company to receive not only an unfavorable review, but a potential fine or penalty by the regulatory organization. If that red flag is not followed up upon by a board of directors or senior management, and something worse happens (i.e., a major breach), the red flag could serve as a very convenient basis upon which to file a "follow on" civil action litigation. "Red flags are … useful when they are either waived in one's face or displayed so that they are visible to the careful observer."[22] Given that many of the major cyber breaches are relatively new, we have yet to see how the regulators will respond to any particular fact pattern. But the fact that there will be more cyber-attacks will be no surprise to anyone.

Decision in the Wyndham Cyber Derivative Action

Though there have been several cases in the Financial Crisis context that have been decided based upon a Caremark/Stone v. Ritter analysis, there have been no decisions in the cybersecurity context other than the recent decision by Judge Stanley Chesler in the Wyndham Derivative Action. Though the facts of the commencement of the Wyndham Derivative Action were very different than these in similar actions commenced following the announcement of bad news (the Wyndham Derivative Action was filed 3 1/2 years after the original data breach - the Target derivative action was filed one month after Target's breach [23]), the Wyndham Derivative Action was dismissed by Judge Chesler on a factual record that not only had the board of directors met before the breach many times to discuss cybersecurity procedures and implement them, it held 14 quarterly meetings after the attack to discuss the company's cybersecurity procedures and proposed security enhancements, and the audit committee (which investigated the facts of the attacks) met at least 16 times to review cybersecurity. This record gave the Court ample opportunity to conclude that the board's decision to refuse the shareholder's demand that the Company investigate the breaches and sue the company's personnel involved was protected by the business judgment rule.

Judge Chesler's decision raises a lot more questions than it answers. What would have happened if there was not an extensive factual record of board involvement in the company's cybersecurity affairs, and had not taken both pre- and post-corrective action? Or worse, perhaps there existed only a very sketchy record of board involvement showing that the board was relatively uninterested in the cybersecurity procedures of the company, or did not receive regular reports on cybersecurity prevention and detection measures.[24] The recent 2015 US State of Cybercrime Survey issued by PwC revealed a startling fact. Despite 18 months of intense PR pressure around cybersecurity:

> "Our research shows that one in four (26%) respondents said their Chief Information Security Officer (CISO) or Chief Security Officer (CSO) makes a security presentation to the Board only once a year, while 30% of respondents said their senior security executive makes quarterly security presentations. But 28% of respondents said their security leaders make no presentations at all."[25]

What history teaches us today is that cybersecurity breaches have the potential to not only create regulatory risk for the Company involved, but in addition, the risk that directors and officers of the Company may be sued for breach of fiduciary duty for their alleged failure to oversee the cyber risks of the company.

Cyber Governance Checklist That Directors Must Consider

One of the key takeaways of the decision in the Wyndham Derivative Action is that board conduct matters, and will be reviewed, not only by the Court of public opinion, but also potentially by the Delaware Chancery Court, or other courts around the country, and most certainly the regulators. Wyndham teaches that having a factual record and documentation of board action and involvement is key to getting shareholder derivative actions either dismissed, or settled on a reasonable basis.

Here are some basic questions directors, especially those of public companies, must consider when reviewing their company's cybersecurity framework:

1. What part of the Board should handle examination of cybersecurity risks? Should it be the whole Board? Should this responsibility be assigned to the Audit Committee? To the Risk Committee (if there is one)? Should the Board create a "Cyber Committee" to exclusively deal with these issues? Should additional Board members be recruited who have specific cybersecurity experience?

2. How often should the Board (or Committee) be receiving cybersecurity briefings from management? In this world, which moves at light-speed and in which cyber-breaches are reported daily, are quarterly briefings enough? Should the Board be receiving monthly briefings? Or more (given the industry type of the Company on whose board they sit, e.g., a tech/IP company)?[26]

   A recent study noted that, " At the other end of the spectrum, only 25% of respondents said their full Board is involved in cyber-risks." [27] Is this a very low number because the full Board of Directors designated the oversight of cyber risk to another board committee, like the audit or risk committee? Or is it because companies and their boards are still not appreciating the cyber risk their companies face. The same PwC report also noted, "It's also essential that Boards treat cybersecurity as an overarching corporate risk issue rather than simply an IT risk. Many have yet to adopt this approach, however. Almost half (49%) of Boards view cybersecurity as an IT risk, while 42% see cybersecurity through the lens of corporate governance."[28]

3. Given the sheer complexity and magnitude of many cybersecurity issues, should the Board hire its own "cyber advisers" to consult on cybersecurity issues, and to be available to ask questions of the Company's senior management, CISO and CIO?

4. What are the Company's highest value cyber assets (e.g. credit card information, health care records), and where are they located (e.g. company servers, the cloud, a third party vendor)? And what is currently being done to protect those assets? If those highest value assets are not IP assets, but rather infrastructure assets, what is being done to protect those assets from a cyber attack? [29]

5. What are the greatest threats and risks to the Company's highest value cyber assets, and who are the potential threat actors (nation-states, cyber criminals)? Is the Company's human IT resources and financial capital adequate to protect those high value assets?

6. What is the Company's volume of all cyber incidents on a weekly or monthly basis? What is the magnitude/severity of those incidents (meaning e.g., were attackers just "probing" the network

perimeter for entry points, but were blocked, or were attackers actually able to penetrate the perimeter and exfiltrate data? What is the time taken and cost to respond to those incidents?

7. What would the "worst case" cyber incident cost the company - in terms of both lost business (because of downtime of systems that were attacked and need to be brought back), and in terms of lost business because of the harm to the Company's reputation as a result of the attack?

8. What is the Company's specific cyber incident response plan, and how will it respond to a major cyber-attack? Does the incident response plan contain a "crisis management" plan to respond to all various constituencies, as well as the media (both print and electronic/high activity bloggers)? Has the cyber-incident plan been tested (or "table-topped") so that it is ready to be put into place on a moment's notice? Does the company have an information management business continuity plan in the event that critical data is lost or destroyed (e.g., like in a wiperware or ransomware attack)?

9. What cybersecurity training does the Company give its employees on social media, spearphishing scams, and email high-jacking?

10. What sort of program does the Company have in place to monitor the level and robustness and security of the "administrative privileges" that it gives to its employees and executives?

11. What sort of cyber due diligence does the Company perform with respect to its third-party service providers and vendors?[30]

12. In a mergers and acquisitions context, what is the level of "cyber due diligence" that is done as part of the consideration of any acquisition or financial transaction?

13. Has the Company performed an analysis of the "cyber-robustness" of the company's products and services to analyze potential vulnerabilities that could be exploited by hackers? What sort of software "patching" schedule does the IT Department follow when software makers or other third parties issue vulnerability alerts?

14. Should the Company consider adopting, in whole or in part, the NIST cybersecurity framework as a way or method of showing affirmative action and due care in protecting the Company's IP assets?[31]

15. Finally, does the Company purchase cyber-insurance? And if they don't, why not given the risks involved and the tremendous costs associated with remediating a sophisticated cyber breach?

This list could go on for pages. But it won't, since we believe it serves its purpose, i.e., there are plenty of tough questions that directors must ask of senior management and senior IT staff. Not just once a quarter, but as needed in order to meet the ever-changing threat and risk environment. None of these questions should be hard for the IT professionals to answer. If the IT professionals don't have the answers to many of the questions, then they should be told to report back to the Board as soon as possible when they have them. Many of them go directly towards whether the organization has a functioning, effective and up-to-date cybersecurity program to protect its most valuable data and IP assets. Directors may also need their own advisors and professionals to help them fulfill their oversight duties in assessing and asking the tough questions of management.

Before we conclude, an important word about question 14 - the National Institute of Standards cybersecurity framework: We hear too often that cybersecurity issues are too hard to figure out for the average layperson who is not totally immersed in the IT trade, and that directors too often feel that they do not know the "right questions" to ask. The NIST cybersecurity framework should be a great help in this regard, as it was written so that a director and a CISO could speak the same "common language" when reviewing the company's cybersecurity posture. The NIST cybersecurity framework is written in a way that even the director afraid of updating his or her iPad should understand the issues at hand. IN SUM: "what are my most important information and IP assets, where are they located, how are they being protected today, and what can we do tomorrow to protect them even better?" Adopting the NIST framework, in whole or in part, is a great way for a company and its board to get the informational ball rolling on critical discussions as they pertain to cybersecurity. And it is a great way to document them in board meeting minutes and then form a plan to implement agreed-upon improvements. As the Sony cyber-attack proved, cyber is not just an IT department's problem; it is everyone's problem, most especially the board of directors. Full engagement is critical, and is essential for the survival and growth prospects of the company.

ENDNOTES

[1] See "Revisiting Caremark and a Director's Duty to Monitor: The Chancery Court's wake-up Call to Directors," found at http://www.conference-board.org/retrievefile.cfm?filename=DN-004-10.pdf&type=subsite.

[2] See "Sony Made It Easy, but Any of Us Could Get Hacked," available at http://www.wsj.com/articles/sony-made-it-easy-but-any-of-us-could-get-hacked-1419002701.

[3] See "The Target Breach: By the Numbers" at http://krebsonsecurity.com.

[4] See "ISS's View on Target Directors Is a Signal on Cybersecurity," available at http://online.wsj.com/articles/iss-calls-for-an-overhaul-of-target-board-after-data-breach-1401285278?mod=_newsreel_4; Following Target's announcement that affected 40 million customers and 46 percent profit loss, CIO Beth Jacob, who oversaw Target's web site and internal computer systems since 2008 resigned in March 2014. Shortly thereafter, the board decided it was time for new leadership and CEO Gregg Steinhafel resigned in early May 2014. See also "9 data breaches that cost someone their job," available at http://www.csoonline.com/article/2859485/data-breach/9-data-breaches-that-cost-someone-their-job.html#slide2.

[5] Id.

[6] Note also that Target board of directors was sued in a shareholder derivative class action, and Target was itself named in a securities class action arising out of the breach. Just recently, District Court Judge Paul Magnuson in Minnesota certified a class action of the banks all of who were suing Target for the losses they allegedly suffered. See "St. Paul judge certifies class-action status to banks in Target breach suit," available at http://www.startribune.com/st-paul-judge-certifies-class-action-status-to-banks-in-target-breach-suit/327772621/.

[7] We note that there is also currently pending a Delaware Section 220 "books and records" demand made against Home Depot arising out of the cybersecurity breach. See "Next Up: A Home Depot Data Breach-Related D&O Lawsuit?" available at http://www.dandodiary.com/2015/06/articles/cyber-liability/next-up-a-home-depot-data-breach-related-do-lawsuit/. Just recently, a shareholder derivative action was filed against the board of Home Depot. See "Data Breach-Related Derivative Lawsuit Filed against Home Depot Directors and Officers," available at http://www.dandodiary.com/2015/09/articles/cyber-liability/data-breach-related-derivative-lawsuit-filed-against-home-depot-directors-and-officers/.

[8] See "Risk Management and the Board of Directors," available at http://corpgov.law.harvard.edu/2015/07/28/risk-management-and-the-board-of-directors-3/.

[9] 698 A.2d 959 (Del.Ch. 1996

[10] See In Re Citigroup Inc. Shareholder Derivative Litigation, 698 A.2d 959, 971 (Del. Ch. 1996).

[11] Caremark, 698 A.2d at 970-971.

[12] See "Cybersecurity and the board of directors: avoiding personal liability," found at http://blogs.reuters.com/financial-regulatory-forum/2013/07/25/cybersecurity-and-the-board-of-directors-avoiding-personal-liability-part-i-of-iii/

[13] See Stone v. Ritter, 911 A.2d at 362, 370 (2006) (emphasis added).

[14] See generally Holland, "Delaware Director's Fiduciary Duties: The Focus on Loyalty," available at http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1334&context=jbl.

[15] See "Data Breach-Related Derivative Lawsuit Filed against Home Depot Directors and Officers," available at http://www.dandodiary.com/2015/09/articles/cyber-liability/data-breach-related-derivative-lawsuit-filed-against-home-depot-directors-and-officers/#more-11012.

[16] Id. See also "Wyndham Worldwide Board Hit with Cyber Breach-Related Derivative Lawsuit," at http://www.dandodiary.com/2014/05/articles/cyber-liability/wyndham-worldwide-board-hit-with-cyber-breach-related-derivative-lawsuit/ ("the Wyndham Derivative Action").

[17] See Commissioner Aguilar's speech at http://www.sec.gov/News/Speech/Detail/Speech/1370542057946.

[18] This webcast is available at http://www.sec.gov/news/otherwebcasts/2014/cybersecurity-roundtable-032614.shtml.

[19] See "Cybersecurity and Financial Firms: Bracing for the Regulatory Onslaught," at http://www.strozfriedberg.com/wp-content/uploads/2014/04/Cybersecurity-and-Financial-Firms-Bracing-for-the-Regulatory-Onslaught_BloombergBNA_Stark_April2014.pdf.

[20] See Regulation S-P, available at http://www.sec.gov/rules/final/34-42974.htm#P41_3349. Regulation S-P also applies to investment advisers registered with the SEC ("registered advisers"), brokers, dealers (collectively, "broker-dealers"), and investment companies ("funds") and requires them to adopt appropriate policies and procedures that address safeguards to protect this information. Id.

[21] 5 U.S.C. § 6827(4)(a); 15 U.S.C. § 6801(b)(1)-(3).

[22] See In re Citigroup Shareholder's Litigation, 2003 WL 21384599 (Del.Ch.June 5, 2003).

[23] See "Target Directors and Officers Hit with Derivative Suits Based on Data Breach," found at http://www.dandodiary.com/2014/02/articles/cyber-liability/target-directors-and-officers-hit-with-derivative-suits-based-on-data-breach/.

[24] We note that on August 24, 2015 the Third Circuit Court of Appeals affirmed a decision of the District Court finding that the FTC has authority to regulate the cybersecurity of U.S. companies. This ruling will send the case back to the United States District Court for future factual determinations which may bring to light additional purported allegations against the Wyndham board of directors as it pertains to their cybersecurity oversight role.

[25] See "PwC 2015 US State of Cybercrime Survey," available at http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf.

[26] See "4 Ways to Engage Executives in Cyber Risk," available at http://deloitte.wsj.com/cio/2015/07/20/4-ways-to-engage-executives-in-cyber-risk/ (noting, in a survey of retail executives in 2014 that "just 37 percent of survey respondents [retail CIO's] say their organizations report to the board on a quarterly basis regarding their cyber risk posture, while 44 percent say their organizations never report on cyber risk to any business stakeholders.").

[27] See "US cybersecurity: Progress stalled: Key findings from the 2015 US State of Cybercrime Survey," available at http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf.

[28] Id.

[29] See "NSA Director Warns of 'Dramatic' Cyberattack in Next Decade," available http://www.wsj.com/articles/nsa-director-warns-of-dramatic-cyberattack-in-next-decade-1416506197.

[30] See "Trustwave 2013 Global Security Report," noting that 63% of all investigations showed that a cyber breach emanated from a third-party vendor or IT administrator, found at http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf.

[31] See "Why You Should Adopt the NIST Cybersecurity Framework," available at http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/adopt-the-nist.pdf ("If, for instance, the security practices of a critical infrastructure company are questions in a legal proceeding, the Court could identify the Framework as a baseline for "reasonable" cybersecurity standards"); See also, "Understanding and Implementing the NIST Cybersecurity Framework," available at http://corpgov.law.harvard.edu/2014/08/25/understanding-and-implementing-the-nist-cybersecurity-framework/ ("By choosing to implement the Framework (or some part of it) sooner rather than later, organizations can potentially avoid the inevitable conclusion (or parallel accusation by a plaintiff's attorney) that they were "negligent" or "inattentive" to cybersecurity best practices following disclosure of a cyber-breach. Organizations using the Framework should be more easily able to demonstrate their due care in the event of a cyber-attack by providing key stakeholders with information regarding their cybersecurity program via their Framework profile."). We note here that there exists another cybersecurity risk framework that was issued by Committee of Sponsoring Organizations of the Treadway Commission (COSO) in 2013. We don't want to go into too much discussion of the COSO framework here as it contains many of the same principles of the NIST cybersecurity framework, which we discuss at length in this book. For more on the COSO framework, see "COSO-Guided Cybersecurity: Risk Assessment," available at http://deloitte.wsj.com/riskandcompliance/2015/09/08/coso-guided-cybersecurity-risk-assessment/.

CHAPTER 5:
FEDERAL REGULATION AND OVERSIGHT - TODAY AND TOMORROW

PURPOSE OF THIS CHAPTER:

1. Identify the various Federal regulatory agencies that have cybersecurity oversight and/or regulatory authority over companies.
2. Identify, in particular, the regulatory role of the Federal Trade Commission over cybersecurity.
3. Identify, in particular, the regulatory role of the SEC and FINRA over cybersecurity for registered investment advisers, funds and broker dealers.

The regulatory drumbeats out of Washington D.C. continue despite the dysfunction of Congress in actually doing anything to foster or strengthen cybersecurity procedures in the private industry sector:

> *"The consequences of cyber incidents are serious. When credit card data is stolen, it disturbs lives and damages consumer confidence. When trade secrets are robbed, it undercuts America's businesses and undermines U.S. competitiveness. And successful attacks on our financial system would compromise market confidence, jeopardize the integrity of data, and pose a threat to financial stability. As it stands, our laws do not do enough to foster information sharing and defend the public from digital threats. We need legislation with clear rules to encourage collaboration and provide important liability protection. It must be safe for companies to collaborate responsibly, without providing immunity for reckless, negligent or harmful behavior. And we need legislation that protects individual privacy and civil liberties, which are so essential to making the United States a free and open society. We appreciate the bipartisan interest in addressing this important issue, and the Administration will continue to work with key stakeholders on the various bills that are developing in Congress."*
>
> — US Treasury Secretary Jacob J. Lew, July 16, 2014[1]

In the absence of comprehensive cyber legislation, the responsibility for the consequences of a cyber-attack to a U.S. public company clearly lies with its board of directors. Luis Aguilar, a Commissioner of the SEC, stated very clearly in a speech entitled "Cyber Risks in the Boardroom,"[2] that,

> [B]oards must take seriously their responsibility to ensure that management has implemented effective risk management protocols. Boards of directors are already responsible for overseeing the management of all types of risk, including credit risk, liquidity risk, and operational risk **and there can be little doubt that cyber-risk also must be considered as part of board's overall risk oversight**. The recent announcement that a prominent proxy advisory firm [Institutional Shareholders Services (ISS)] is urging the ouster of most of the Target Corporation directors because of the perceived "failure…to ensure appropriate management of [the] risks" as to Target's December 2013 cyber-attack is another driver that should put directors on notice to proactively address the risks associated with cyber-attacks.

Id. (alteration in original) (emphasis added) (footnotes omitted).

Without equivocation, Commissioner Aguilar stated that cybersecurity was a Board responsibility. Likewise, ISS signaled after the Target breach that directors could or should be held personally accountable for cybersecurity breaches if they fail to keep their eye on the ball.[3] And the plaintiffs' bar has recognized that cybersecurity breaches may become a lucrative addition to their class action litigation practices.[4]

As previously noted, in the absence of some broad Congressional mandate regarding the imposition of a unified cybersecurity standard, we have instead a veritable panoply of federal and state regulators who have all issued some sort of "cyber guidance" to regulated entities to help focus them on cybersecurity governance. In response to this quickly evolving area of regulation and oversight of cybersecurity, and the ever-increasing scrutiny by multiple constituencies of the boards of directors, we provide here this short, non-exclusive list of how the U.S. government and its agencies are dealing with companies under their specific regulatory authority related to cybersecurity.[5] In a later chapter, we will discuss how many of these same agencies are dealing with consumer privacy issues that result from data collection, data storage and data breach issues.

The United States Department of Justice

The newest entrant into the field of regulatory "guidance" is the United States Department of Justice, who on April 29, 2015 issued a memo entitled "Best Practices for Victim Response and Reporting of Cyber Incidents."[6] Though not necessarily "regulatory" in nature, it certainly contains important suggestions from the Department of Justice for companies dealing with cyberattacks. It sets forth guiding principles for pre-breach conduct and post-breach conduct by companies. These principles include both reaching out to local enforcement before a breach to establish a working relationship with their local FBI or Secret Service Field office, as well as notifying local law enforcement of the breach early in the process if criminality is suspected. That cooperation may likely garner the full support of the Department of Justice, FBI and Secret Service, as it helps the victim company investigate the breach and perhaps attribute it to a definite source, and may also engender favorable treatment of the breached company by the Federal Trade Commission. The April 29th Department of Justice Memo is new, and we will watch closely to see how its principles play out in practice.

The SEC

Certainly most of the Federal activity on cybersecurity issues has come from the SEC. The genesis of its involvement began on or about October 12, 2011, when the SEC issued guidance regarding the disclosure obligations of public companies relating to cybersecurity risks and cyber incidents. The focus of this guidance was on whether information concerning cybersecurity and cyber incidents rose to the level of a disclosure obligation either as a risk factor under Regulation S-K Item 503(c) or in the MD&A Section of a Company's mandatory SEC disclosure. One of the critical determining factors for the SEC was whether:

> "[T]he costs or other consequences associated with one or more known incidents or the risk of potential incidents represent a material event, trend, or uncertainty that is reasonably likely to have a material effect on the registrant's results of operations, liquidity, or financial condition or would cause reported financial information not to be necessarily indicative of future operating results or financial condition.[7]
>
> If the registrant does determine its cybersecurity risk or previous cyber incidents rise to the level of a disclosable event, the SEC guidance notes that such disclosure might contain information reflecting:
>
> - Discussion of aspects of the registrant's business or operations that give rise to material cybersecurity risks and the potential costs and consequences;
> - To the extent the registrant outsources functions that have material cybersecurity risks, description of those functions and how the registrant addresses those risks;
> - Description of cyber incidents experienced by the registrant that are individually, or in the aggregate, material, including a description of the costs and other consequences;
> - Risks related to cyber incidents that may remain undetected for an extended period; and
> - Description of relevant insurance coverage."

Id.

The SEC's October 2011 cyber guidance was just that - guidance. The question of "materiality" is and was left within the discretion of the company. There was no discussion about when the risk of "potential incidents" rose to the level of disclosure. Fueled by continuing major cyber breaches, on March 26, 2014 the SEC organized a "cyber roundtable" among industry groups and public and private sector participants in order to consider, among other things, whether or not additional SEC guidance related to the level of disclosure in a company's public filings was necessary. It will be interesting to see how events develop at the SEC, particularly as cyber breaches continue to increase in number and scope.

We see already today that SEC Division of Corporate Finance comments letters are pointing registrants towards more cybersecurity disclosure rather than less regarding past cyber incidents and information security measures. We do not see that trend changing. In fact, at a conference in February 2015, David Glockner, the Director of the SEC's Chicago Regional Office, said that cybersecurity was effectively "high on [the SEC's] radar."[8] Note that some also theorize that the failure to safeguard assets may or could under some cases be a violation of Section 404 of the Sarbanes-Oxley Act of 2002.[9]

SEC Office of Compliance, Inspections and Examinations (OCIE)

On April 15, 2014, the OCIE issued a National Exam Program Risk Alert, entitled "OCIE Cybersecurity Initiative," announcing it would conduct examinations of more than 50 registered broker-dealers and investment advisors "designed to assess cybersecurity preparedness in the securities industry and to obtain information about the industry's recent experiences with certain types of cyber threats."[10] Importantly, this alert came with an extensive list of questions requiring registrants to respond to various areas of their cybersecurity preparedness. Some of the questions are as follows:

- Please identify any published cybersecurity risk management process standards, such as those issued by the National Institute of Standards and Technology (NIST) or the International Organization for Standardization (ISO), the Firm has used to model its information security architecture and processes.
- Please indicate which of the following practices and controls regarding the protection of its networks and information are utilized by the Firm, and provide any relevant policies and procedures for each item.
- Confirm that the Firm provides written guidance and periodic training to employees concerning information security risks and responsibilities. If the Firm provides such guidance and/or training, please provide a copy of any related written materials (e.g., presentations) and identify the dates, topics, and which groups of employees participated in each training event conducted since January 1, 2013.
- Confirm that the Firm maintains controls to prevent unauthorized escalation of user privileges and lateral movement among network resources. If so, please describe the controls, unless fully described within policies and procedures.
- Confirm that the Firm restricts users to those network resources necessary for their business functions. If so, please describe those controls, unless fully described within policies and procedures.
- Confirm that the Firm maintains a baseline configuration of hardware and software, and users are prevented from altering that environment without authorization and an assessment of security implications.
- Confirm that the Firm has a process for ensuring regular system maintenance, including timely installation of software patches that address security vulnerabilities.
- Does The Firm maintain protection against Distributed Denial of Service (DDoS) attacks for critical internet-facing IP addresses? If so, please describe the internet functions protected and who provides this protection.
- Confirm that the Firm maintains a written cybersecurity incident response policy. If so, please provide a copy of the policy and indicate the year in which it was most recently updated. Please also indicate whether the Firm conducts tests or exercises to assess its incident response policy, and if so, when and by whom the last such test or assessment was conducted.

The OCIE list also requires information on employee training, vendor management, the firm's practices to detect "unauthorized activity on its networks and devices," and specific information, if applicable, concerning any cyber breaches which the registrant experienced since January 1, 2013.[11]

On February 3, 2015, the SEC published a summary of the initial 100 examinations.[12] The results were both good and not so good. In most cases, firms admirably performed comprehensive risk assessments and had written information security policies. Note that in some cases however, the regulated entities examined did not have risk assessments of vendors that they dealt with. Very few of the entities examined maintained cyber insurance to transfer any risk of an attack to a third party. Clearly, the story of cybersecurity examinations of regulated investment advisers and funds will be continued, and it will be interesting to see if more and more firms adopt best practice guidance set forth by SEC OCIE. And if the regulated entities and advisers do not take the implicit "hint" of the SEC it will be interesting to see if penalties will result.

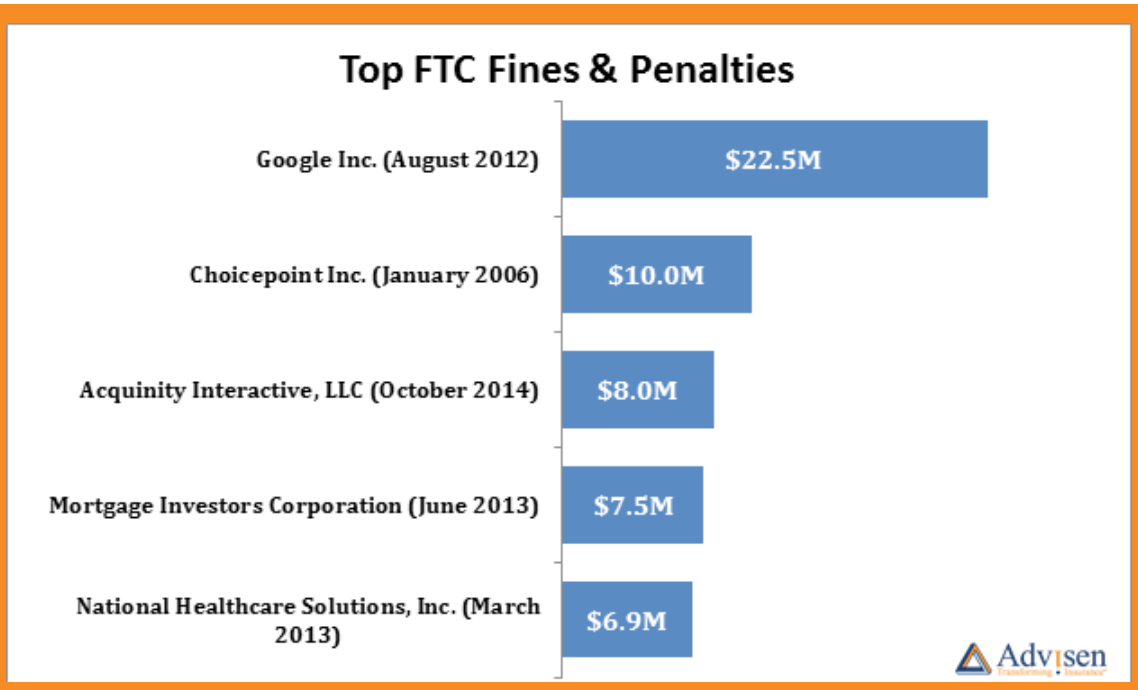
On September 15, 2015, OCIE put out a second cybersecurity risk alert, entitled "OCIE's 2015 Cybersecurity Examination Initiative."[13] Though this Risk Alert is somewhat repetitive of the April 2014 Alert, OCIE set forth an additional area of emphasis: "Access Rights and Controls," which deals in general with how users access network servers, and, in particular, how firms "prevent unauthorized access to systems or information, such as multifactor authentication or updating access rights based upon personnel or system changes."[14] We assume that with respect to access rights, OCIE is indicating that it will review how firms monitor access privileges given to authorized users in order to assess whether firms are over-privileging certain employees or groups of employees. Access and privilege rights have both emerged as pressing problems during 2014 and 2015 among many companies that have suffered significant breaches. In sum, this is important new information for registered funds and advisers to consider as they prepare for their second round of cybersecurity examinations. What we don't know (yet) is with so much guidance now in existence, if examiners find funds or firms deficient in their compliance, will that result in fines, penalties or, at the least, unnecessary adverse publicity.

Financial Industry Regulatory Authority (FINRA)

In January 2014, FINRA announced a "sweep" program, which in effect is very similar to OCIE's, whereby firms under FINRA's authority would be receiving targeted examination letters requiring them to respond to questions relating in general to their cyber preparedness.[15] FINRA's targeted examination letters seek information very similar to the OCIE cybersecurity initiative. Following its own targeted examinations in 2014, FINRA issued its own "Report on Cybersecurity Practices" which detailed its findings. The FINRA report focused on the need for strong cyber governance within the regulated entity, strong employee awareness and vendor management practices, and the need for a strong, tested incident response plan.

Section 5 of the Federal Trade Commission Act

To be fair and impartial, the winner in the US cybersecurity regulatory enforcement space has clearly been the US Federal Trade Commission ("FTC") which to date has brought over 50 enforcement actions against US companies related to cybersecurity. "Since 2002, the FTC has pursued numerous investigations under Section 5 of the FTC Act against companies for failures to abide by stated privacy policies or engage in reasonable data security practices. It has monitored compliance with consent orders issued to companies for such failures."[16] One recent report noted that:



> The FTC is gaining ground in the national cybersecurity debate due to an aggressive attempt to expand its authorities under Section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive acts or practices. The agency's push for greater authority to regulate cybersecurity practices in the private sector won a major victory recently when a federal judge denied a motion to dismiss the FTC's case against Wyndham Worldwide Corp. for failing to protect consumer information. According to a Sept. 11 report by the Congressional Research Service, the judge's ruling effectively lends support to the FTC's position that it possesses jurisdiction to regulate data security under its unfair or deceptive practices authority. And as new massive data breaches make the news, experts warn of additional FTC enforcement actions on the horizon."[17]

Following the disclosure of a cybersecurity breach, the FTC may charge the Company with a Section 5 violation, as it did in Wyndham Worldwide, alleging that the failure of the Company to safeguard it's customers' data was an unfair practice.[18] To our knowledge, the majority of these cases have settled prior to a full hearing or trial. AND NOTE - Now that the FTC's power to regulate cybersecurity was recently upheld by the Third Circuit Court of Appeals in August 2015, we expect that the FTC will be even more aggressive in filing enforcement actions arising out of cybersecurity breaches.

Other Federal Regulations Related to Cybersecurity

GRAMM-LEACH BLILEY ACT (GLBA)

Perhaps most famous for repealing part of the Glass-Steagall Act of 1933, the GLBA, also known as the Financial Services Modernization Act of 1999, has a cyber-data component and applies to "financial institutions," i.e., "any institution engaged in the business of providing financial services to customers who maintain a credit, deposit, trust, or other financial account or relationship with the institution." This

regulation is called Regulation S-P.[19] Under the Regulation S-P, financial institutions are required to "establish appropriate standards" to safeguard a customer's personal financial information, in order: "(1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[20]

Under Regulation S-P, financial institutions, in actions brought by the Department of Justice only (there is no private right of action), can be fined up to $100,000 for each violation, AND directors and officers of financial institutions could be held personally liable for civil penalties of up to $10,000 for each violation.

In April 2013, the SEC and CFTC jointly adopted a rule for the prevention of identity theft, called Regulation S-ID ("Reg S-ID" or "Rule"). "The Rule requires SEC or CFTC registrants (e.g., investment advisers, investment companies, broker-dealers, commodity pool advisors, futures commission merchants, retail foreign exchange dealers, commodity trading advisers, introducing brokers, swap dealers, and major swap participants) to establish and maintain programs that detect, prevent, and mitigate identity theft, if they maintain certain types of accounts for clients. These organizations must implement Reg S-ID policies and procedures by November 20, 2013."[21]

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)[22]

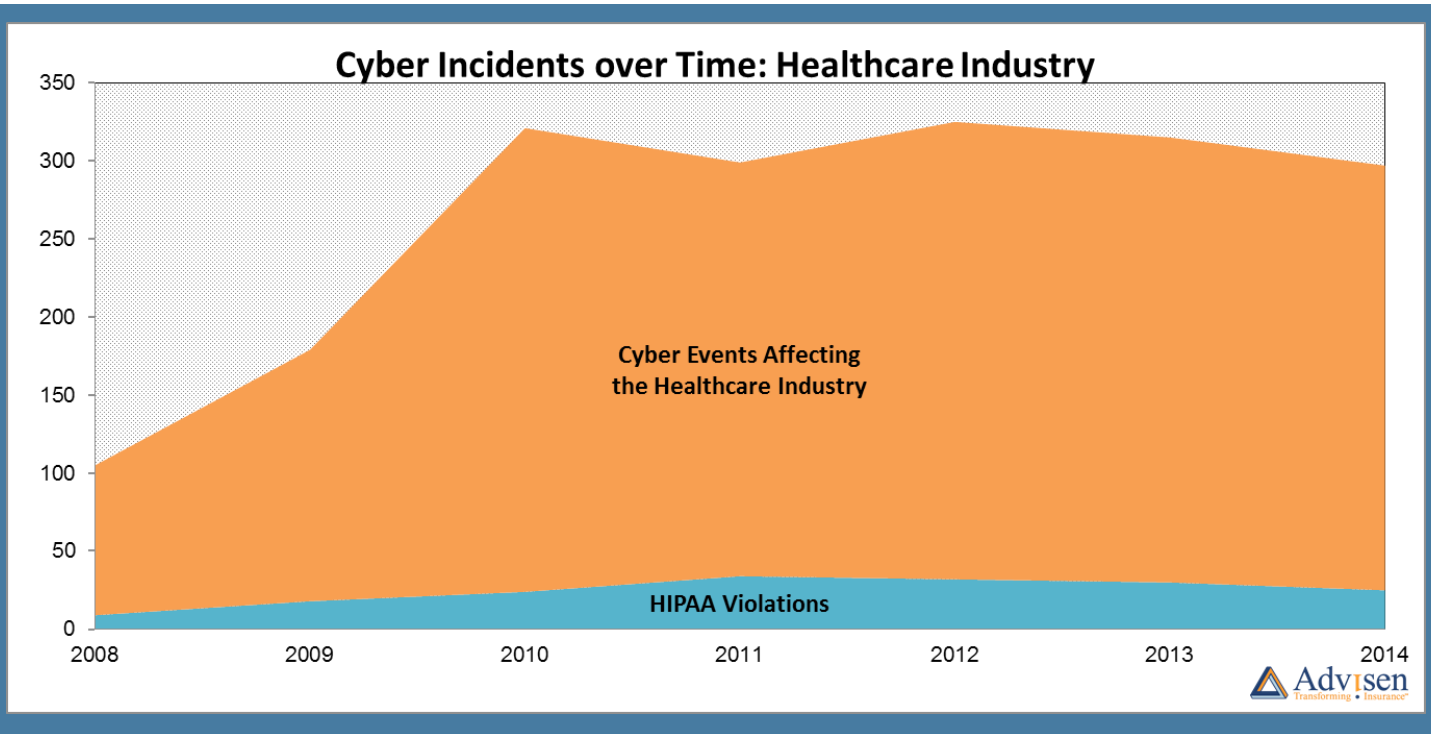
The PCI DSS is not a "law" but a list of cybersecurity standards developed by the payment card industry and applied to any U.S. company that processes credit cards, such as retailers, resort and destination companies, or financial institutions. The list focuses on, among other general requirements, the need to "develop and maintain secure systems and applications," and the need to "track and monitor all access to network resources and cardholder data." These standards provide an "actionable framework for developing a robust payment card data security process - including prevention, detection and appropriate reaction to security incidents."[23] PCI DSS 3.1, adopted in November 2013, enlarges the scope of data security requirements upon retailers and financial institutions.[24] It will be interesting to see whether "3.1," which was to be implemented by retailers on or about January 1, 2015, will have any material effect on an industry sector that continues to experience major cybersecurity breaches.[25]

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

Among many other things, 2014 was also a year when the US saw a staggering number of cybersecurity breaches in the healthcare, managed healthcare and hospital sectors. For instance, in August 2014, Community Health Systems - with 206 hospitals in 29 states - reported that it had been hacked, with protected health information covering 4.5 million patients compromised as a result.[26] In February 2015, Anthem Healthcare suffered a tremendous cybersecurity breach which resulted in the loss of personal information on over 80 million of its customers. Indeed, one recent KPMG survey noted that, "[i]n the past two years, 81 percent of hospitals and health insurance companies have had a data breach."[27]

Here is the basic problem for the healthcare industry when it comes to cyber - the information it stores on patients is a "gravy train" for cyber criminals:

- Medical identity theft is more lucrative than credit card theft. According to PhishLabs, a provider of cybercrime protection and intelligence services, stolen health credentials are worth about 10 to 20 times that of a U.S. credit card number.



- Forty-three percent of all identity theft is caused by medical records theft.
- The cost of a health care data breach averages $316 per record, well above the $201 per record for all industry segments combined, according to the Ponemon Institute's 2014 Cost of Data Breach Study.[28]

These facts show the lucrative target the healthcare industry provides to cyber thieves. Indeed, one senior healthcare cyber analyst at the Sans Institute noted:

> This level of compromise and control could easily lead to a wide range of criminal activities that are currently not being detected. For example, hackers can engage in widespread theft of patient information that includes everything from medical conditions to social security numbers to home addresses, and they can even manipulate medical devices used to administer critical care.[29]

HIPAA requires, in general, the protection and confidentiality of all electronically protected healthcare information that is created, received, maintained or transmitted. Under HIPAA, a healthcare facility must protect against any reasonably anticipated threat, or hazard, to the security or integrity of such healthcare information. Under HIPAA, fines can range from $50,000 to $250,000. There also can be civil litigation exposure as well, as demonstrated by the Anthem breach.

HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT (THE HITECH ACT)

The HITECH Act expands the scope of the institutions covered under HIPAA to now include any organization or individual who handles protected healthcare information, which could now include banks, businesses, schools and other organizations.[30] The HITECH Act also increased the potential fine or penalty for a health-care information cyber breach up to $1.5 million per violation.

THE REGULATORY ENVIRONMENT: TODAY AND TOMORROW

Cybersecurity is the buzzword of the day, year, and maybe the decade. Well-publicized cyber breaches at major U.S. companies are now becoming the norm and have caused not only tremendous anxiety for executives, but reputational damage and material revenue loss for many companies.[31] These breaches have not only caused both consumer and securities class and derivative actions, but have caught the eye of both federal and state regulators of many industries. Even for brick and mortar companies without any express regulator other than the SEC (retailers, for example, who are only subject to the retail industry-based PCI DSS standard), cybersecurity issues must continue to be omnipresent on the minds of corporate executives because any industry is at risk of having their IP destroyed or stolen by hackers.

In response to this ever-changing landscape of increasingly complex threat vectors, plus increasing regulation, directors and officers, and their companies' CISOs and CIOs, must adapt daily and continue daily discussions about how to improve their company's cybersecurity procedures and intrusion detection/incident response plans of action. Adaptation means not just "checking the box" on some measure of an industry standard (like OCIE Guidance or PCI DSS) but having real discussions about allocating real physical, human and financial resources of the company to protect its most valuable IP and customer information. Adaptation means that companies and firms need to continue to adopt demonstrable processes and procedures which provide evidence to all constituencies (including their auditors) that they are paying attention and responding to the cybersecurity threat with actionable measures, and not just talking points. As we note above, one of the most important constituencies is "the regulators," where a fine or penalty could lead to further civil or reputational consequences. Whether that means adopting the NIST cybersecurity framework or continuing to improve upon their own cybersecurity procedures in a demonstrable fashion, directors and officers must consider the consequences of failing to act. Even in the face of seemingly unimaginable technological threats to US businesses, directors and officers will likely be looked at with ever increasing scrutiny by regulators, customers, and investors in years to come.

ENDNOTES

[1] See "In Call to Action, Treasury Secretary Lew Urges US Financial Sector to Redouble Efforts Against Cyber Threats," found at http://www.treasury.gov/press-center/press-releases/Pages/jl2571.aspx.

[2] Available at http://www.sec.gov/News/Speech/Detail/Speech/1370542057946.

[3] See Paul Ziobro & Joann S. Lublin, ISS's View on Target Directors Is a Signal on Cybersecurity, Wall St. J., May 28, 2014, available at http://www.wsj.com/articles/iss-calls-for-an-overhaul-of-target-board-after-data-breach-1401285278.

[4] See Jeffrey Roman, Supervalu Hit With Lawsuit After Breach, Bank Info Security (Aug. 20, 2014), available http://www.bankinfosecurity.com/supervalu-hit-lawsuit-after-breach-a-7214; see also the following recently filed complaints in Davis v. Steinhafel, Case Nos. 14-cv-00203-PAM-JJK et seq., 2014 WL 3853976 (D. Minn. July 18, 2014) ; Diana v. Horizon Healthcare Servs., Inc., Case Nos. 2:13-CV-07418-CCC-MF, 2:14-cv-00584-CCC-MF, 2014 WL 3351730 (D.N.J. June 27, 2014).

[5] We leave for another day how various state agencies and authorities (e.g., the New York State Department of Financial Services) are simultaneously dealing with cybersecurity related issues. See e.g., New York State Department of Financial Services' Report on Cybersecurity in the Banking Sector (2014), available at http://www.dfs.ny.gov/about/press2014/pr140505_cyber_security.pdf.

[6] The Memo can be found at http://www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents2.pdf.

[7] WSecurities and Exchange Commission, CF Disclosure Guidance: Topic No. 2 (Oct. 13, 2011), available at http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[8] See "U.S. SEC on the prowl for cybersecurity cases -official," available at http://www.reuters.com/article/2015/02/20/sec-cyber-idUSL1N-0VU2AV20150220.

[9] See "Cybersecurity and Financial Reporting," available at http://www.mindthegaap.com/webarticle/In_Brief_Vol_12_Cybersecurity.pdf. ("According to the SEC's adopting release on ICFR…the safeguarding of assets is one of the elements of internal control over financial reporting. Because customer data is an asset, a company's failure to have sufficient controls to prevent the unauthorized acquisition, use, and/or disposition of customer data may constitute a weakness in ICFR.").

[10] Office of Compliance Inspections and Examinations, 4 National Exam Program Risk Alert, no. 2, Apr. 15, 2014," available here.

[11] In large part, these questions mimic guidance issued by the SEC's Division of Investment Management in April 2015. See "Cybersecurity Guidance," available at http://www.sec.gov/investment/im-guidance-2015-02.pdf.

[12] See Cybersecurity Examination Sweep Summary," available at https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.

[13] This Risk Alert can be found at http://www.sec.gov/ocie/announcement/ocie-2015-cybersecurity-examination-initiative.pdf.

[14] Id.

[15] See FINRA, Target Examination Letters re: Cybersecurity (Jan. 2014), available at http://www.finra.org/industry/cybersecurity-targeted-exam-letter.

[16] See "The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority," found at http://fas.org/sgp/crs/misc/R43723.pdf.

[17] See "The FTC's expanding cybersecurity influence," found at http://fedscoop.com/ftcs-expanding-cybersecurity-influence/#sthash.HY-QJfdC6.dpuf .

[18] See e.g., FTC v. Wyndham Worldwide Corp., Civil Action Number: 212-cv-01365-SPL (June 25, 2012), found at http://www.ftc.gov/enforcement/cases-proceedings/1023142/wyndham-worldwide-corporation.

[19] See e.g., "Cybersecurity Assessment General Observations and Statement," available at http://www.occ.gov/news-issuances/bulletins/2014/bulletin-2014-53.html.

[20] See e.g., "Cybersecurity and Communications Reliability Division, Public Safety and Homeland Security Bureau," available at http://www.fcc.gov/encyclopedia/cybersecurity-and-communications-reliability-division-public-safety-and-homeland-securi.

[21] See generally "Identity Theft Regulation: Are you under the SEC/CFTC microscope?" available at http://www.pwc.com/us/en/financial-services/regulatory-services/publications/identity-theft-regulation.jhtml.

[22] The PCI Security Standards Council is an open global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection. The PCI Security Standards Council's mission is to enhance payment account data security by driving education and awareness of the PCI Security Standards. See https://www.pcisecuritystandards.org/.

[23] PCI Security Standards Council, Navigating PCI DSS, Understanding the Intent of the Requirements, version 2.0 (Oct. 2010), available at https://www.pcisecuritystandards.org/documents/navigating_dss_v20.pdf; PCI Security Standards Council, PCI SSC Data Security Standards Overview, available here.

[24] Available at https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf.

[25] For more specific information on the attributes of PCI DSS 3.0, see "How PCI DSS 3.0 Can Help Stop Data Breaches," available at http://www.darkreading.com/risk/compliance/how-pci-dss-30-can-help-stop-data-breaches/a/d-id/1318306.

[26] See generally, "Health care data breaches have hit 30M patients and counting," available at http://www.washingtonpost.com/blogs/wonkblog/wp/2014/08/19/health-care-data-breaches-have-hit-30m-patients-and-counting/ ("Since federal reporting requirements kicked in, the U.S. Department of Health and Human Services' database of major breach reports (those affecting 500 people or more) has tracked 944 incidents affecting personal information from about 30.1 million people).

[27] See "81 percent of hospitals and health insurance companies have had a data breach," available at http://www.csoonline.com/article/2978911/data-breach/study-81-of-large-health-care-organizations-breached.html.

[28] See "Why cyber thieves love health care--and what you can do about it," available at http://www.propertycasualty360.com/2014/12/01/why-cyber-thieves-love-health-care--and-what-you-c.

[29] Two excellent articles, "The Top U.S. Healthcare Story For 2014: Cybersecurity," and "New Cyberthreat Report By SANS Institute Delivers Chilling Warning To Healthcare Industry," which summarize the details of the Sans Institute Health Cyber Threat report are available here at http://www.forbes.com/sites/danmunro/2014/12/21/the-top-u-s-healthcare-story-for-2014-cybersecurity/ and here at http://www.forbes.com/sites/danmunro/2014/02/20/new-cyberthreat-report-by-sans-institute-delivers-chilling-warning-to-healthcare-industry/.

[30] It should also be noted that federal legislation concerning cybersecurity has been promulgated to protect government data. The Federal Information Security Management Act was enacted in 2002 namely to "enhance the management and promotion of electronic Government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services." E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899.

[31] For example, Brian Yarbrough, a research analyst with Edward Jones, predicted that after Target's cyber breach, "Probably 5% to 10% of customers will never shop there again." Hadley Malcolm, Target sees drop in customer visits after breach, USA Today, Mar. 11, 2014, available at http://www.usatoday.com/story/money/business/2014/03/11/target-customer-traffic/6262059/.

CHAPTER 6:

UNDERSTANDING AND IMPLEMENTING THE NIST CYBERSECURITY FRAMEWORK

PURPOSE OF THIS CHAPTER:

1. Identify the purpose of the National Institute of Standards and Technology Cybersecurity Framework.
2. Identify the components of the NIST Cybersecurity Framework and its "Core Components."
3. Identify the reasons why adopting the NIST Cybersecurity Framework may be beneficial to any Company and its board of directors.

> *"The NIST Cybersecurity Framework represents a tipping point in the evolution of cybersecurity, one that emphasizes and encourages a proactive risk-management approach that builds on standards and compliance,… "While the framework is voluntary, we believe that organizations—across industries—should adopt the guidelines as a key tool to manage and mitigate cyber risk to their business, in combination with other risk-management tools and processes such as cyber insurance."*[1]

Despite the fact that companies are continuing to increase spending on cybersecurity initiatives data breachs continue to occur. According to the public reports, "global IT security spending will reach $71.1 billion [in 2014], which represents an increase of 7.9% compared to 2013. Next year, spending will grow even more, reaching $76.9 billion."[2] Despite the boost in security spending, vulnerabilties, threats against these vulnerabilities, data breaches and destruction persist.[3] The number of U.S. data breaches tracked in 2014 hit a record high of 783 in 2014, according to a recent report released by the Identity Theft Resource Center (ITRC) and sponsored by IDT911™. This represents a substantial hike of 27.5 percent over the number of breaches reported in 2013 and a significant increase of 18.3 percent over the previous high of 662 breaches tracked in 2010. The number of U.S. data breach incidents tracked since 2005 also hit a milestone of 5,029 reported data breach incidents, involving more than 675 million estimated records.[4] Hardly a day goes by when there is not another media report of a major cybersecurity breach.[5] Hardly a day goes by without another serious cyber attack being reported resulting in the loss of personally identifiable information of customers and employees.[6]

To combat these issues, the President on February 12, 2013 issued Executive Order (EO)

13636, "Improving Critical Infrastructure Cybersecurity."[7] The EO directed NIST, in cooperation with the private sector, to develop and issue a voluntary, risk-based Cybersecurity Framework that would provide U.S. critical infrastructure organizations with a set of industry standards and best practices to help manage cybersecurity risks.

In February 2014, through a series of workshops held throughout the country and with industry input, NIST released the "Framework for Improving Critical Infrastructure Cybersecurity" ("the Framework").[8] For the first time, the Framework provides industry with a risk-based approach for developing and improving cybersecurity programs. It also provides a common language regarding cybersecurity issues to allow for important discussions to take place between an organization's "IT" people, and an organization's "business" people, some of whom may cringe when hearing complicated terms like "APT" (Advanced Persistent Threat). Its common sense, "English language" approach allows an organization and its directors to both identify and improve upon its current cybersecurity procedures. Though the Framework was developed for the 16 critical infrastructure sectors, it is applicable to all companies - albeit at least today - on a voluntary basis.[9]

The Framework is not the only "standard" that exists right now for "best practices" in data security. ISO 27001 (ISO) is an international standard that describes a "best practices" approach for information security management. Like the Framework, ISO 27001 provides a holistic, system-wide approach to information security that encompasses people, processes and technology. And since it has been in the public domain for a longer period of time, many organizations have already adopted ISO 27001. For ease of reference, as the Framework incorporates by reference many of the ISO standards, we are going to refer mostly to the Framework in this section so there is no duplication of effort. The point of this chapter is not to discourage an organization from adopting either the Framework or ISO 27001. The point of this Chapter is the importance that one organization adopted some recognized standard for information management security so that the organization can point to such adoption, along with accompanying written policies and procedures implementing such adoption, as evidence not only for compliance or regulatory purposes,[10] but to demonstrate to regulators, the plaintiffs' class action bar, customers and other third parties that it is paying attention to "best practices" in cybersecurity.

WHAT IS THE CYBERSECURITY FRAMEWORK

The Framework contains three primary components: The Core, Implementation Tiers, and Framework Profiles.

The Framework Core

The Framework Core ("Core") is a set of cybersecurity activities and applicable references established through five concurrent and continuous functions - Identify, Protect, Detect, Respond and Recover - that provide a strategic view of the lifecycle of an organization's management of cybersecurity risk. Each of the Core Functions is further divided into Categories tied to programmatic needs and particular activities. The outcomes of activities point to informative references, which are specific sections of standards, guidelines, and practices that illustrate a method to achieve the outcomes associated with each subcategory. The Core principles can be thought of as the Framework's fundamental "cornerstone" for how an organization should be viewing its cybersecurity practices:

(1) identifying its most critical intellectual property and assets;

(2) developing and implementing procedures to protect them;

(3) having resources in place to timely identify a cybersecurity breach, and

(4) having procedures in place to both respond to and

(5) recover from a breach, if and when one occurs.

Now, the knee-jerk response to our explanation of the Core may be, "oh, well, we do this already," or "we had this discussion last year." Our response very simply is the following: Cybersecurity is a living, breathing holistic concept. Good cybersecurity must be instilled into a corporate culture by awareness, compliance, employee training. What was ok last year, or even six months ago, might not be ok today. New business lines, methods and processes may have incepted in the interim and created more data issues to be dealt with. Hackers have gotten more advanced in their threat vectors. Similarly each year firewalls, data intrusion and incident response hardware has gotten more advanced. Good data security is not merely taken in snapshots every year. It is like one continuous movie stream, where every frame shows a different picture at any given point in time. At least at the CIO or CISO level, data and information security discussions must happen frequently and be documented so as to be true to the principles contained in the Framework's Core, so that relevant information can be transmitted upstream to senior management and the Board of Directors.

KEY:

ASSET IDENTIFICATION: At "the core" of the Framework's Core are discussions concerning what are the organization's most important IP assets. This is really one area that does not get enough attention in our view because not all information has the same significance to a corporation. To some companies, customer and credit card information is the key. For others, personally identifiable healthcare information is critical. And to others, it might be the plans to a new fighter plane or nuclear battleship. Without identifying these critical assets it would be difficult if not impossible to determine what level of security to apply to each category of informational assets, and how and where to store back up copies of such data if you need to immediately invoke your business continuity plan. For the most critical of data, other strategies of information might need to be invoked to make security for such data the equivalent of Fort Knox. Without identifying your critical information data sets, the allocation of assets and resources to protect such assets will potentially turn into a fruitless exercise without any residual benefits to the organization.

PROTECTION: Now for a few words about the "protection" aspect of the Framework's Core. Above, we mentioned this concept in connection with explaining the various pieces of a network server cybersecurity system, including hardware, software and the new, next "best black box" that vendors urge upon organizations on every sales call. The point here, in today's cybersecurity ecosystem, is that cybersecurity "defensive" hardware is constantly changing to adapt to the hackers' next best threat vector. Though a CISO may say that "oh, everything is just fine," boards of directors must be asking in return, "is there anything new out there we need to have?" or more simply put, "what can we be doing better?" For instance, many companies, including some portions of the US government today, rely on signature-based

instrusion detection systems, meaning they only attempt to block "known threat signatures." Additionally, every company should at least consider running "red team - blue team" tests once a quarter. With full knowledge of the Company, its IT department, and "the lawyers," the "red team" attempts to hack into the network and steal a defined data set (e.g. Human resources data). The "blue team" tries to repel, stop or locate the intrusion as soon as possible. The key here is to determine in a "war games" scenario whether the network cybersecurity defenses have any holes. At the same time, such testing trains the company's incident response teams to better hunt down intrustions. Its obviously better for the Company itself to find a problem itself, rather than a malicious hacker. Also, compromise testing can also be run at any point to determine whether the company's network has actually been compromised. Same rule applies: find out sooner rather than later if you could potentially be breached, or already have been breached. This is called "adaptive defense" cybersecurity. [11] Thus boards must ask the hard questions in order to answer the simpler one, to wit, "are we ok with what we have, or should we attempt to step up our game to be better than the average company?" The answer [hopefully] should be the latter.

RECOVERY/BUSINESS CONTINUITY PLANNING: Finally, the recovery aspect of the Framework's core has been mentioned a few times already above (and there will be more below). Aside from the importance of an incident response plan, it is critical that companies have an information management business continuity plan (or "BCP"). Not unlike the plan a major corporation might have bordering the Gulf of Mexico in the event of a hurricane, a BCP is designed so that a corporation can recover from a major loss of data. Think Saudi Aramco. Think Sony Pictures. Think "the dark ages" where business was done with typewriters and fax machines. The Corporation should have a regular back up plan for data that it creates daily and weekly, and keep that data ideally off premises (or even in the cloud). For many cloud service providers or data centers, they too have their own backup plans if for some reason access to their services is denied or unavailable. Unlike the 1930's, data is the lifeblood of most corporations. It needs to be ready to be restored or recovered to the mainframe instantaneously in the event network servers suffer catastrophic damage. Along with incident response plans, information management business continuity plans should be practiced quarterly, with a full "cut-over" to the backup material done in order to evidence the resiliency of an organization to withstand even the worst cyber breach.

The Framework Implementation Tiers

The Framework Implementation Tiers ("Tiers") describe the level of sophistication and rigor an organization employs in applying its cybersecurity practices, and provide a context for applying the core functions. Consisting of four levels from "Partial" (Tier 1) to "Adaptive" (Tier 4), the tiers describe approaches to cybersecurity risk management that range from "informal, reactive responses to agile and risk-informed." Think of the Tiers as a "self-assessment" that take place at the time the NIST framework is adopted. Though you might be a Tier 1 or Tier 2 at the beginning, the goal obviously is not to remain static in your cybersecurity practices, because (simply put) as the hackers get progressively better in their intrusion methods, the organization can simply fall even further behind the cybersecurity eightball. A Tier 1 should strive to be a Tier 2. A Tier 2 should strive to be a Tier 3, and so on. Showing progression through the Tiers, even in small bites, arguably shows contining attention to cybersecurity principles in general, and more specifically and arguably a desire to attain "best practices."

FRAMEWORK IMPLEMENTATION TIERS EXPLAINED

TIER 1 (PARTIAL): Here, the Organization's cyber risk management profiles are not formalized, and are managed on an ad hoc basis. There is a limited awareness of the Organization's cybersecurity risk at the Organization level, and an Organization-wide approach to managing cybersecurity risk has not been established.

TIER 2 (RISK INFORMED): Unlike Tier 1, Tier 2 Organizations establish a cyber risk management policy that is directly approved by senior management (though not yet on an Organization wide basis). There is some effort by senior management to establish risk management objectives related to cybersecurity, to understand the Organization's threat environment, and to implement cybersecurity procedures with adequate resources.

TIER 3 (REPEATABLE): Here, the organization is running with formal cybersecurity procedures, which are regularly updated based upon changes in risk management processes, business requirements, and a changing and technology landscape. Cyber-related personnel are well-trained threat and can adequately perform their duties. The Organization also understands its dependencies and business partners, and receives information from them which allows for collaboration and risk-based management decisions.

TIER 4 (ADAPTIVE): Here, the Organization adapts its cybersecurity practices "in real time" based upon lessons learned and predicative indicators derived from previous and current cybersecurity activities. Through a process of continuous improvement incorporating advanced cybersecurity technologies, real time collaboration with partners, and "continuous monitoring" of activities on their systems, the Organization's cybersecurity practices can rapidly respond to sophisticated threats.

The Framework Profile

The Framework Profile ("Profile") is a tool that provides organizations a method for storing information regarding their cybersecurity program. A profile allows organizations to clearly articulate the goals of their cybersecurity program. The Framework is risk-based; therefore the controls and the process for their implementation change as the organization's risk changes. Building upon the Core and the Tiers, a comparison of the Profiles (i.e., Current Profile versus Target Profile), allows for the identification of desired cybersecurity outcomes, and gaps in existing cybersecurity procedures. Attention then can be focused on allocating time, resources and people to close the gaps.

WHY DIRECTORS SHOULD CARE ABOUT THE FRAMEWORK

"Our critical infrastructure networks are extremely vulnerable to such a damaging attack, and we can't count on deterrence if we're already in a shooting war with a nation like China or Russia…. It's not hard to understand how difficult it would be if the power or water was shut off, but imagine if one of our adversaries were able to shutdown key American financial transactions. Our economy would grind to a halt." Rep. Mike Rogers, (R.-Mich.), chairman of House Intelligence Committee.[12]

When the Framework was originally announced, Tom Wheeler, Chariman of the Federal Communications Council (FCC), stated that an industry-driven cybersecurity model is preferred over prescriptive regulatory approaches from the federal government.[13] Nonetheless, we continues to see, almost daily, successful attacks on critical infrastructure organizations, like financial institutions, major corporations and the healthcare sector.

At some point, if critical infrastructure organizations do not demonstrate that a voluntary program can provide cybersecurity standards that are the same as, if not better than, federal regulations, regulators will likely step in with new laws. In fact, according to SEC Commissioner Luis Aguilar, the Framework has already been suggested as a potential "baseline for best practices by companies, including in assessing legal or regulatory exposure to these issues or for insurance purposes. At a minimum, boards should work with management to assess their corporate policies to ensure how they match-up to the Framework's guidelines — and whether more may be needed."[14] If the SEC OCIE guidance, or other proposed federal regulation of cybersecurity becomes a reality, implementing the Framework could be a mandatory exercise either in whole or in part.

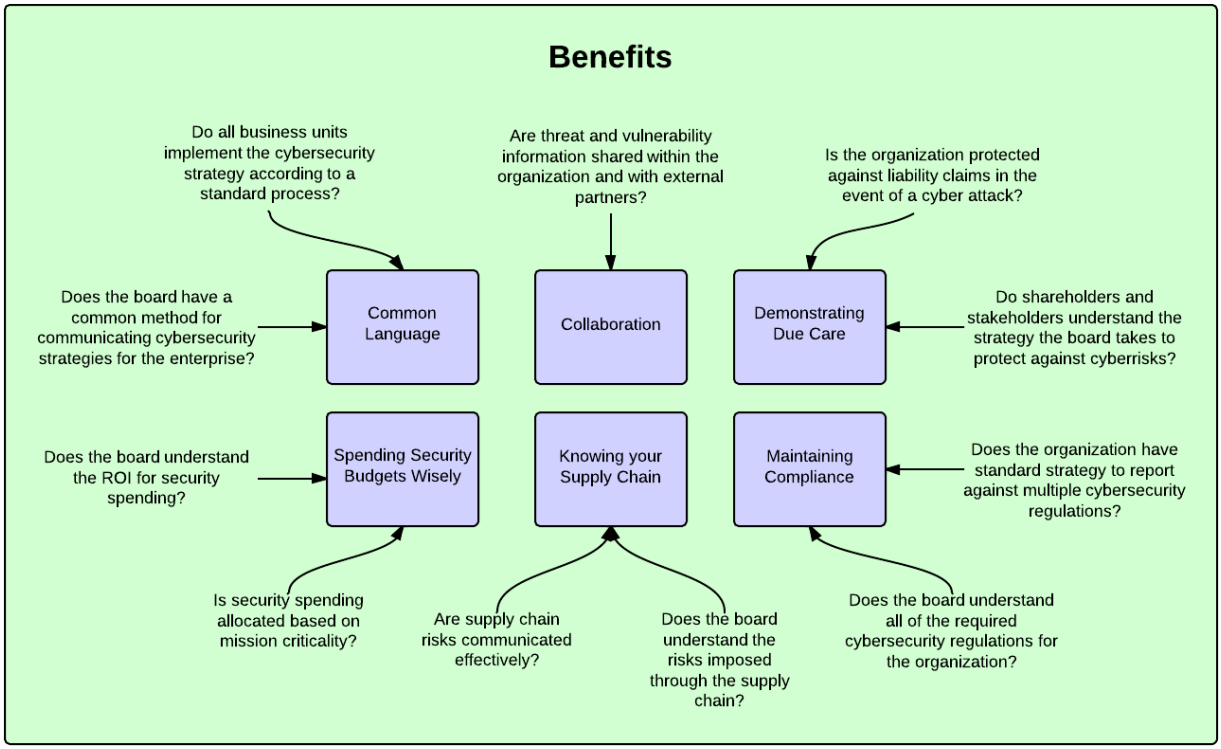
In addition to staying ahead of federal and state regulators and potential Congressional legislation, the Framework provides organizations with a number of other benefits, all of which support a stronger cybersecurity posture for the organization. These benefits include a common language, collaboration opportunities, the ability to verifiably demonstrate due care by adopting the Framework, ease in maintaining compliance, the ability to secure the supply chain, and improved cost efficiency in cybersecurity spending. Though it would be Herculean to accurately summarize all benefits of the Framework and how to implement them, we stress its key points below.

Common Language

The Framework, for the first time, provides a common language to standardize the approach for addressing cybersecurity concerns. As we have noted a few times in other chapters,many cybersecurity principles are not intuitive. They are not based upon well-established principles that Directors (especially audit committee members) are used to hearing, like "revenue recognition." The Framework allows for cybersecurity programs to be established and shared within an organization and with organizational partners using a common easy-to-understand language. For example, the Framework allows for the creation of several types of Profiles: Profiles that provide strategic enterprise views of a cybersecurity program, Profiles that are focused on a specific business unit and its security, or Profiles that describe technologies and processes used to protect a particular system. Despite the number of Profiles that may exist for an organization, directors can quickly and easily understand how corporate guidance is implemented in each Profile since they have a standard language and format for describing an organization's cybersecurity programs.

Collaboration

NIST and participants from industry that assisted in the Framework development envision the Framework Profiles as a way for organizations to share best practices and lessons learned. By leveraging the common language and increased community awareness established through the Framework, organizations can collaborate with others through programs such as the Cybersecurity Forum (CForum).[15] CForum provides an online forum for organizations to share lessons learned, post questions regarding their cybersecurity challenges, and maintain the conversation to continually improve cybersecurity capabilities and standards.



Demonstrating Due Care

By choosing to implement the Framework (or some part of it) sooner rather than later, organizations can potentially avoid the inevitable conclusion (or parallel accusation by a plaintiff's attorney) following disclosure of a cyber breach that they were "negligent" or "inattentive" to cybersecurity best practices.

Organizations using the Framework as a common language for board discussions should be more easily able to demonstrate their due care in the event of a cyber attack by providing key stakeholders with information regarding their cybersecurity program via their Framework profile and the active steps the company took to elevate that profile to a higher level. At the same time, Directors can point to their request that the organization consider implementing the Framework (or using it as guidance) in defense of any claim that they breached their fiduciary duties by failing to oversee the cybersecurity risk inherent in their Organization. New guidance has been issued that such discussions should be documented in corporate board minutes in order to evidence such discussions.

Maintaining Compliance

Many critical infrastructure organizations are required to meet multiple regulations with overlapping and conflicting requirements. In order to avoid fines and additional fees from regulatory bodies, many operators are forced to maintain multiple compliance documents describing how the organization is complying with each requirement. The standard developed by the Framework enables auditors and regulators to evaluate cybersecurity programs and controls in one standard format eliminating the need

for mulitple security compliance documents given the fact that many of the Framework's standards have already been incorporated into the regulatory guidance standards issued by both OCIE and FINRA.

Knowing your Supply Chain/Good Vendor Management Practices

The Framework also provides an opportunity for organizations to better understand the cybersecurity risks imposed through their supply chains. Chinks in the armor of vendors to major corporations have proved catastrophic to at least two major retailers this year alone. Organizations purchasing IT equipment or services can request a Framework profile, providing the buying organization an opportunity to determine whether or not the supplier has the proper security protections in place. Alternatively, the buying organization can provide a Framework profile to the supplier or vendor to define mandatory protections that must be implemented by the service provider's organization before it is granted access to the buying organization's systems.

Spending Security Budgets Wisely

In an environment where cyberthreat information is not readily available, organizations struggle with understanding how much security is enough security, leading to organizations implementing unnecessary cybersecurity protections. Through the use of the Framework, standards for care can be established for each critical infrastructure sector. Organizations can leverage these standards to determine the appropriate level of security protections required, ensuring efficient utilization of security budgets.

The diagram on page 65 provides questions to help determine if and how an organization can benefit from implementing the Framework. Discussing these questions and their responses will help organizations determine how well their current cybersecurity efforts are protecting them against cyber attacks. Based on the answers to these questions, they will better understand which of the benefits presented in this article will apply to their organization should they implement the Framework.

WHERE DO YOU START WITH IMPLEMENTING THE FRAMEWORK?

A major challenge in adopting the Framework is simply getting started. Some organizations, maybe those in Implementation Tier 1, may have limited resources and familiarity with the Framework (or the ISO 27001 standard) which could help them leverage their existing cybersecurity, compliance and audit programs, policies and processes. But coming to grips with the Framework is certainly worth the effort and expense for any organization, when considering on the otherhand that a major cybersecurity breach could conceivably wipe out the entire organization.

At a minimum, directors and their management should become familiar with the Framework. Additionally, directors (or some committee thereof) should have a deep discussion with management about the organization's Implementation Tiers. The Implementation Tiers allow an organization to both consider its current cyber risk management practices, the present threat environment, legal and regulatory requirements (e.g., those imposed by the SEC, FINRA, FTC, GLBA or HIPAA), business/mission objectives, and organizational constraints, and set a goal to ascend higher within the Implementation Tiers.

Educating managers and staff on the Framework to ensure all organizations are on the same page is also an important step toward the successful implementation of a robust cybersecurity program. The

previously mentioned CForum is a source for success stories, lessons learned, questions and information useful to organizations implementing the Framwork. This information about existing Framework Implementations may help organizations with their own approaches. Additionally, organizations can seek out cybersecurity service providers skilled in helping organizations with the education, awareness and planning required to implement the Framework across an entire enterprise.

Though "voluntary," it cannot be overstated that the Framework is "a National Standard" developed with input from industry experts, collaborators and businesses (and our own government) with years of cyber experience. As stated by the former Chairman of the House Intelligence Committee, Mike Rogers, "there are two kinds of companies. Those that have been hacked and those that have been hacked but don't know it yet."[16] Given that it is almost inevitable that an organization will be hacked, there will be a time and a place where it may need to demonstrate to customers, investors, regulators, and plaintiff's attorneys that it gave thought to, and implemented, cybersecurity measures in order to defend its most critical intellectual property assets, or its most critical business and customer information. Implementing the Framework will not only allow organizations to improve cybersecurity measures, but also to effectively demonstrate due care when it comes to protecting its most valuable data and IP assets.

ENDNOTES

[1] See "Getting Inside the Insider Threat," found at http://www.nxtbook.com/nxtbooks/kmd/hst_20141011/#/44.

[2] See "Global Cybersecurity Spending to Reach $76.9 Billion in 2015: Gartner," available at http://www.securityweek.com/global-cybersecurity-spending-reach-769-billion-2015-gartner.

[3] See e.g., "JPMorgan hack exposed data of 83 million, among biggest breaches in history, " available at http://www.reuters.com/article/2014/10/02/us-jpmorgan-cybersecurity-idUSKCN0HR23T20141002.

[4] See Identity Theft Resource Center Breach Report Hits Record High in 2014," available at http://www.idtheftcenter.org/ITRC-Surveys-Studies/2014databreaches.html.

[5] See e.g., "Sears says Kmart stores hit by data breach," found at http://www.reuters.com/article/2014/10/10/us-sears-holdings-cybersecurity-idUSKCN0HZ2BW20141010.

[6] See "Newly discovered Chinese hacking group hacked 100+ websites to use as "watering holes", available at http://arstechnica.com/security/2015/08/newly-discovered-chinese-hacking-group-hacked-100-websites-to-use-as-watering-holes/; "Victims of June OPM Hack Still Haven't Been Notified," available at https://threatpost.com/victims-of-june-opm-hack-still-havent-been-notified/114512#sthash.Ee77EfP0.dpuf.

[7] Executive Order 13636 of February 12, 2013, *Improving critical Infrastructure Cybersecurity*, available at http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.

[8] The National Institute of Standards and Technology (NIST) "Framework for Improving Critical Infrastructure Cybersecurity version 1.0", February 12, 2014,available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[9] G2, Inc. was engaged by the National Institute of Standards and Technology (NIST) as the prime contractor to assist in the development of the Framework for Improving Critical Infrastructure Cybersecurity. We thank Tom Conkle, Commercial Cybersecurity Lead at G2, Inc. for his assistance with this Chapter.

[10] Indeed, regulatory guidance issued by the SEC's Office of Compliance, Inspections and Examination requests information from regulated entities as to whether they have adopted "any published cybersecurity risk management process standards, such as those issued by the National Institute of Standards and Technology (NIST) or the International Organization for Standardization (ISO)." See also, "3 ways healthcare CIOs can avoid an FTC lawsuit over security," available at http://www.fiercehealthit.com/story/3-ways-healthcare-cios-can-avoid-ftc-lawsuit-over-security/2015-09-01 (noting that "Having [NIST cybersecurity framework] in place is one way a CIO can show the FTC that the company took serious steps to keep data safe.").

[11] See e.g., "FireEye Adaptive Defense," available at https://www.fireeye.com/products/fireeye-adaptive-defense-cyber-security.html.

[12] See "US Cybersecurity Practices Fail to Keep Pace with Cyber Adversaries," found at http://www.hstoday.us/channels/dhs/single-article-page/us-cybersecurity-practices-fail-to-keep-pace-with-cyber-adversaries.html.

[13] (Sarkar, 2014), available at http://www.fiercegovernmentit.com/story/fcc-chairman-pitches-new-industry-driven-regulatory-model-enhance-cybersecu/2014-06-13.

[14] See "Boards of Directors, Corporate Governance and Cyber-Risks: Sharpening the Focus," available at http://www.sec.gov/News/Speech/Detail/Speech/1370542057946.

[15] The Cybersecurity Forum (CForum) is a not-for-profit, publically available site dedicated to the evolution and implementation of the Cybersecurity Framework, available at http://Cyber.securityFramework.org.

[16] Graham, Scott, Interview: Greg Toughill, DHS, USA on Cybersecurity, July 28, 2014, available at http://www.globalgovernmentforum.com/brigadier-general-greg-touhill-cybersecurity-department-of-homeland-security-interview/.

CHAPTER 7:

SPEARPHISHING - WHAM, BAM, THANK YOU SPAM! DON'T CLICK ON THE LINK!

PURPOSE OF THIS CHAPTER:

1. Identify the nature and identity of social media scams.
2. Identify the nature and identity of various spearphishing and related email scams.
3. Identify pro-active steps that a company may take to attempt to defeat spearphishing and email-related scams through employee awareness and automated training.

It seems that just like in old times (in cyberspace that means last year), the existence of "snake-oil" salesmen[1] on the Internet is getting worse, not better. Rather than selling something medicinal or at the very least useful, these snake-oil salesmen of today have only the following intent: to steal your personal information or worse, to distribute malware to your computer.[2] One recent report issued by Symantec in April 2015[3] details literally scores of scams all designed to steal information and potentially ruin your computer (and others' as well) and steal your personal information.

We detail them not out of morbid curiosity about the utter gall of these modern day snake-oil salesmen, but to hopefully inform and prevent the inadvertent "click on the link" circumstances which you and your company would rather avoid. We also point to recently issued reports noting that other scams like phishing and spear phishing continue to be a bothersome and dangerous component not only of company emails, but emails sent to US government agencies, officials and employees.[4] And spear phishing attempts by nation-states, cyber criminals and others will likely continue, and worsen, given the large amount of personal information already stolen by other cyber-attacks. This information will no doubt be used for malicious purposes.[5] At the end of the day, continuous and thorough employee training and awareness programs outlining these sorts of scams must be considered an essential part of the "Holy Grail" of cybersecurity, along with certain network hardware components that can help stop bad emails before they get to your employees' desktops.

Social Media Scams

"Where attacks of yesteryear might have involved a foreign prince and promises of riches through shady exchanges of currency,…today's phishers scan social media for birthdays, job titles and anything else that can be used to create the appearance that an email request is coming from a legitimate source."[6] As the Symantec Report points out, a lot of these email scams and offers are now generated through the explosive growth of social media sites such as Facebook, Twitter, and Pinterest. Here are some of them:

- **MANUAL SHARING** - These rely on victims to actually do the work of sharing the scam by presenting them with intriguing videos, fake offers, or messages that they can then share with their friends;[7]
- **FAKE OFFERINGS** - These scams invite social network users to join fake events or groups with incentives such as free gift cards. Joining often requires the users to share credentials with the attacker or to send a text message to a premium rate number;[8]
- **LIKEJACKING** - Using fake "Like" buttons, attackers trick users into clicking website buttons that install malware and may post updates on a user's newsfeed, thereby spreading the attack;
- **FAKE APPLICATIONS** - Users are invited to subscribe to an application that appears to be integrated for use with a social network, but is not as described and may be used to steal credentials or harvest other personal data; and
- **AFFILIATE PROGRAMS** - When you click on the link, these might allow you to get a free smartphone, airline ticket, or gift card. Caveat emptor: Nothing in life is free, especially when malware is attached thereto.

Phishing Attacks - Email Scams - Email Hijacking

We have previously pointed out the prevalence of phishing or spear phishing attacks against U.S. public companies. As noted in the recently issued 2015 Verizon Data Breach Investigation Report,[9]

> Social engineering has a long and rich tradition outside of computer/network security, and the act of tricking an end user via e-mail has been around since AOL installation CDs were in vogue.
>
> Phishing campaigns have evolved in recent years to incorporate installation of malware as the second stage of the attack. Lessons not learned from the silly pranks of yesteryear and the all-but-mandatory requirement to have e-mail services open for all users has made phishing a favorite tactic of state-sponsored threat actors and criminal organizations, all with the intent to gain an initial foothold into a network.

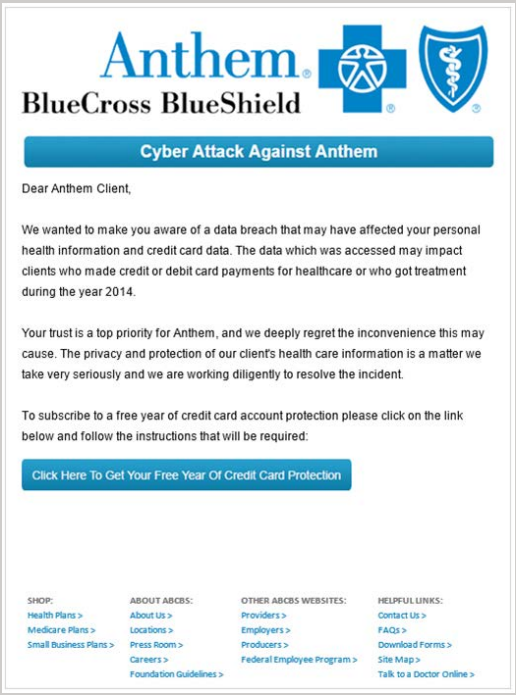
Some of the statistics set forth in the Verizon Report are cause for concern:

- 23% of recipients now open phishing messages and 11% click on the links;
- 50% of the recipients open emails and click on the links within the first hour;
- The median time to first click on the link: one minute, 22 seconds!![10]

HERE ARE SOME PUBLICLY AVAILABLE EXAMPLES OF SPEAR PHISHING EMAILS THAT UNFORTUNATELY HAD SOME SUCCESS IN TRICKING EMPLOYEES AND CUSTOMERS TO CLICK ON THE LINK:

If you had a HSBC account, this would certainly look like a link that you should click on to keep your banking services?

If you had your healthcare insurance provided for by Anthem Healthcare, this link looks like "you have to" click on it to get free credit monitoring. But many probably did not know that Anthem notified its customers in writing by mail of this free credit protection offer. That is the problem with socially-engineered spearphishing. By some business, personal or emotional connection, they force you to want to click on the link to investigate further. But we urge you not to! [11]



How Do You Stop Malicious Social Media/Spear Phishing/Email Campaigns

Obviously there are no good answers to these questions - especially in an era when the bad guys are sending such realistic socially engineered emails that they look like they could come from your husband, wife, son, or daughter, or your company, school or church. They are that good.

A recent, very well written Harvard Business Review article, entitled "Cybersecurity's Human Factor: Lessons from the Pentagon",[12] accurately summarizes the problem and a potential solution:

> Companies need to address the risk of human error too.... The exfiltration of 80 million personal records from the health insurer Anthem, in December 2014, was almost certainly the result of a "spear phishing" e-mail that compromised the credentials of a number of system administrators. These incidents underscore the fact that errors occur among both IT professionals and the broader workforce."

Clearly, the human element of cybersecurity is one of the most important elements (if not the most important element) of the cybersecurity ecosystem. But what do we do with us humans to help us navigate such a very difficult cybersecurity environment highly charged with socially engineered spear phishing emails? Here are some points to consider:

1. **ANTI-PHISHING TRAINING:** Many argue that the weakest link in cybersecurity is the person who is sitting in the chair in front of his or her computer. As such, we strongly advocate a consistent training program, with tailored solutions to your employee base, or specific sections of your employee base (like your IT department or your finance department), to help them change their behavior and discern between "good" emails and potentially "really, really bad" emails, that may contain malware packages just waiting to go off when someone opens the email or clicks on the link. Choose a program which can provide metrics and reports to either your compliance or IT security department, which might point out areas of risk such as divisions, departments, or employees who need further training. A recent report noted:

   > "The infamous Sony hack, the systematic attacks of Heartbleed and Shellshock targeting core internet services and technologies, and the new wave of mass mobile threats have placed the topic of security center stage. Companies are dramatically increasing their IT budgets to ward off attack but will continue to be vulnerable if they over-invest in technology while failing to engage their workforce as part of their overarching security solution. If we change this paradigm and make our workforce an accountable part of the security solution, we will dramatically improve the defensibility of our organizations."[13]

2. **INCREASE USER TRAINING AND ADVISE WORKERS ON SAFE PRACTICES WHEN USING SOCIAL MEDIA:** Simply put, there are bad actors out there who will attempt to lure your employees into doing things or sharing information which may, at its core, contain or share malicious code with others. Adopt policies and procedures to educate your employees on social media website scams, which may include limiting use of such sites to their own devices. "It is key that all staff receive security awareness training covering your acceptable usage policy for social networking. Promoting good practice and improving user behavior are the best methods of reducing the risks from this form of communication."[14]

3. **EMPLOY DMARC BASED TECHNOLOGY:** Many companies have chosen to employ a technology-based solution founded on DMarc, or "Domain-based Message Authentication, Reporting & Conformance."[15] "DMarc is an Internet protocol specification that… provides visibility into email flows, and can tell receiving servers to delete spoofed messages from spooked addresses immediately upon receipt, thus ensuring that only legitimate emails are delivered to inboxes."[16] DMarc allows companies to "pre-qualify" email providers who are "approved" to

send your employees emails from those who may be attempting to spoof or clone domain names to send your employees malicious emails. Other vendors provide email spear phishing protection as well.

4. **SANDBOXING:** Deploy a solution that checks the safety of an emailed link when a user clicks on it. The hardware solution that is employed examines the link-driven email and analyzes it against known malicious email threats and URLs and then quarantines them using anti-spam and anti-virus threat engines to see if those emails exhibit "bad" characteristics. These solutions can be used both on premises and, if your email is handled by cloud mailboxes, off premises. It is better to check and stop the email before it gets to an employee's desk where it could be inadvertently opened and spread malware to your network. Beware that not all sandboxing technology works the same way, and it may not be 100% effective against all threat vectors, especially as bad actors get more and more sophisticated in masking their attacks.

5. **CHECK BEFORE YOU WIRE:** Given the vast increase in business email compromise scams, there should be checks and balances in place before large, unexpected wire transfers take place, including secondary sign-offs within the company if the amount to be wired is over a pre-set threshold.

Virtually all high profile attacks in 2014 and 2015 all have seemed to contain one common element: some employee, either high-level, low-level, or one targeted specifically for his or her password and administrative privileges information, opened a malicious email which set off a catastrophic set of consequences for a company. Though there are many solutions that can be potentially employed to stop this pattern of doom and gloom, not one can be said to be entirely effective. Instead, the set of proactive approaches described above, when used jointly, may help companies reduce the risk of potentially being spear phished to death by bad actors.

ENDNOTES

The author thanks Randi Singer, for co-authoring a related article with him on cybersecurity employee training in a Weil Gotshal & Manges LLP Client alert.

[1] The existence of the first "snake-oil salesmen" date back at least to the time of the First Intercontinental Railroad in 1863.

[2] See "Symantec Internet Threat Report 2015," available at http://www.symantec.com/index.jsp (hereinafter, the "Symantec Report").

[3] See e.g., "Phishing Email Baits Indiana Medical Center, Health Data Exposed," available at http://www.nextgov.com/cybersecurity/threatwatch/2015/04/breach/2233/; "SendGrid: Employee Account Hacked, Used to Steal Customer Credentials," available at https://krebsonsecurity.com/2015/04/sendgrid-employee-account-hacked-used-to-steal-customer-credentials/.

[4] See "China and Russia are using hacked data to target U.S. spies, officials say," available at http://www.latimes.com/nation/la-na-cyber-spy-20150831-story.html.

[5] See "Data Breach Methods Getting More Sophisticated, Report Says," available at http://www.govtech.com/data/Data-Breach-Methods-Getting-More-Sophisticated.html.

[6] See "Beware of Nepal charity scams," available at http://www.usatoday.com/story/money/personalfinance/2015/05/03/weisman-nepal-charity-scams/26755507/ (highlighting that "Email and text message solicitations for charities as well as solicitations you find on social media are also not to be trusted. Once again, you cannot be sure as to who is actually contacting you and these solicitations carry the additional danger of having links or attachments that, if clicked on or downloaded, will install malware on your computer or smartphone that will steal the personal information from your device and use it to make you a victim of identity theft.").

[7] See "5 Scams to Watch for in 2015," available at https://www.allclearid.com/blog/5-scams-to-watch-for-in-2015.

[8] See 2015 Verizon Data Breach Investigations Report," available at http://www.verizonenterprise.com/DBIR/2015/ (hereinafter, the "Verizon Report").

[9] See Verizon Report.

[10] There are scores of other scams too. Most recently, a network technology manufacturer overseas was caught in a "CEO email hijacking" scam in which an overseas subsidiary was tricked through employee impersonation into sending money to several offshore accounts. Very little of that money was recovered. See "Networking Manufacturer Ubiquiti Lost $46.7M after Falling for Elaborate Impersonation Scam," available at http://www.nextgov.com/cybersecurity/threatwatch/2015/08/breach/2438/. Another term for this scam is a "business email compromise," where the attacker impersonates a legitimate person or vendor and requests money be wired to another location (likely outside of the US). This scam has resulted in the loss of approximately $750 million in the past two years. See FBI: Social Engineering, Hacks Lead to Millions Lost to Wire Fraud - available at https://threatpost.com/fbi-social-engineering-hacks-lead-to-millions-lost-to-wire-fraud/114453#sthash.lmnaJHc7.dpuf.

[11] This article is available at https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-the-pentagon.

[12] See "The Weakest Link Is Your Strongest Security Asset," http://blogs.wsj.com/cio/2015/02/26/the-weakest-link-is-your-strongest-security-asset/.

[13] See "Social networking best practices for preventing social network malware," available at http://searchsecurity.techtarget.com/answer/Social-networking-best-practices-for-preventing-social-network-malware.

[14] See "DMARC - What is it?" available at http://dmarc.org/.

[15] See "How To Reduce Spam & Phishing With DMARC," available at http://www.darkreading.com/application-security/how-to-reduce-spam-and-phishing-with-dmarc/a/d-id/1319243.

CHAPTER 8:

THE IMPORTANCE OF A BATTLE-TESTED INCIDENT RESPONSE PLAN

"The days of the IT guy sitting alone in a dark corner are long gone. Cybersecurity has become an obvious priority for C-Suites and boardrooms, as reputations, intellectual property and ultimately lots of money are on the line."

- Priya Ananda, "One Year after Target's Breach: What have we learned?" November 1, 2014.[1]

"Resiliency is the ability to sustain damage but ultimately succeed. Resiliency is all about accepting that I will sustain a certain amount of damage."

- NSA Director and Commander of US Cyber Command Mike Rogers, September 16, 2014.[2]

PURPOSE OF THIS CHAPTER:

1. **Identify the Most Important Elements of a Cyber Incident Response Plan.**
2. **Identify the Importance of Compliance with the Department of Justice's April 29, 2015 Memo on Incident Response Practices.**
3. **Identify the Importance of Proactive Press and Investor Relations Practices as they relate to Responding to a Cyber Incident to preserve the company's reputation in the event of attack.[3]**

Well, for one thing, the last few months of catastrophic cybersecurity breaches have taught us definitively that throwing tens of millions of dollars at "prevention" measures is not enough. The bad guys are smart, very nimble and can adapt their strategies to exploit network weaknesses and software vulnerabilities far quicker than companies have been able to eliminate them.[4] We have also learned that there are no quick fixes in the cybersecurity world. They don't work. The best approach is the holistic approach: basic blocking and tackling like password protection, encryption, "ASAP" patching, employee training, and strong, multi-faceted intrusion detection and prevention systems[5] really trump reliance on the "50 foot high firewall" alone. But there are also two more things that are critical to a holistic cybersecurity approach:

a strong, well-practiced incident response, and as Admiral Rogers noted, the concept of cyber-resiliency, e.g., the ability to "take your cyber lumps," but continue your business operations as soon as possible after the breach is remediated. In fact, a very recent September 2015 Ponemon study of more than 600 IT and security executives stated that "75 percent of U.S. organizations are not prepared to respond to cyberattacks, leaving them more vulnerable than ever against increasing intensity and volume of security breaches. Improving Cyber Resilience is found to be the most potent weapon organizations have in prevailing against the mounting threats they face."[6]

The questions we ask, and hopefully answer in this article are (1) What are the essential elements of a Cyber Incident Response Plan ("IRP")? And (2) Why Incident Response Plans are so important to your organization?

Indeed, the NIST has its own booklet, the "Incident Handling Guide,"[7] which notes:

> Computer security incident response has become an important component of information technology (IT) programs. Cybersecurity-related attacks have become not only more numerous and diverse but also more damaging and disruptive. New types of security-related incidents emerge frequently. Preventive activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services. [Emphasis Supplied].

Note that each element of an effective incident response plan has multiple sub-elements, and multiple levels of complexity. We also note that for effective incident response plans, "one size does not fit all." Plans will likely be different based upon organization size, complexity and industry sector, and on the types of personally identifiable information stored by the organization (and where that data is stored). But we write here to "ground" directors, officers, managing directors, partners and other senior executives on a topic that cannot be ignored -- what questions do they ask about their company's incident response plan prior to finding out that inevitable has become reality: that "we've been hacked." The name of the game is "cyber resiliency": to "get back in the game (quickly and safely)" as soon as possible in order to keep your customers and investors happy and your corporate reputation intact. And to show any regulators and federal law enforcement agencies in the mix (e.g. SEC, OCIE, FINRA, FTC) that you have paid attention and planned for the worst.

"By failing to prepare, you are preparing to fail."
"Never leave that till tomorrow which you can do today."
- Benjamin Franklin

A cyber "event," according to NIST is "an observable occurrence in an information system or network." A cyber "incident" is something more. A cyber "incident" is "a violation of computer security policies, acceptable use procedures, or standard security practices."[8] In a recent book, co-authored by Kevin Mandia, the founder of security consulting firm, Mandiant (now FireEye/Mandiant), entitled "Incident Response and Computer Forensics," he simplifies this definition for today's cyber environment:

> An incident is "any unlawful, unauthorized, or unacceptable action that involves a computer system, cell phone, tablet, and any other electronic device with an operating system or that operates on a computer network."

In sum, cyber "events" may ultimately be "non-events" from a business perspective if it is determined either by intrusion detection systems, along with trained cyber-technicians reviewing the logs that the event is something akin to "normal." Cyber "incidents" need to be investigated, because if they are "bad," they could be very bad, and result in catastrophic results to an organization if not promptly addressed, properly and fully identified (network-wide) and remediated as quickly as humanly possible so the organization may continue its operations relatively un-hindered.

Distinguishing between potentially harmless cyber events and potentially serious cyber events is not an easy task, as many companies get thousands, if not tens of thousands of cyber alerts a day from their intrusion detection systems. Skill, experience and hardware that can distinguish "noisy" or "abnormal"[9] events from potentially serious events are required for this task. It is a daunting task for many major companies.

The best answer to the "we've been hacked" is not "now what?" The best answer is "let's invoke our incident response plan immediately." Though there are literally hundreds of cybersecurity consultants in the marketplace today that could provide a very complex version of an incident response plan, here are the basics (as least as we see them):

1. *Preparation, Ownership and Testing of the Incident Response Plan*

Just as many high-rise buildings in New York City have their own emergency evacuation plan in the event of a fire or other catastrophic event, and practice them with their tenants several times a year, all companies should have a table-top tested, written incident response plan ("IRP") ready to go in the event of a cyber-attack. Directors and officers should consider the following elements essential to a good IRP:

a) The IRP needs to be in writing, fully documented and regularly updated in order that there are no surprises when it is invoked after an incident has been detected. The IRP needs to be in place before the breach. Putting one in place after you've been hacked is not the best time to try and figure out "on the fly" how to proceed.

b) The IRP should define the team of professionals (in-house and third-party vendors) that are part of the incident response team (IRT). The IRT needs to have clear delegation of authority (who does what), and clear lines of communication (who reports to who). The team should have a legal component (whether in-house, outside firm, or probably both most likely) that is skilled in forensic investigations, disclosure obligations, and the preservation of evidence since law enforcement may ultimately be involved depending upon the severity of the breach. The presence of an outside legal team can also help maintain privilege over certain communications. Also, companies should consider having both a Human Resources Person and a Finance Department designee on the IRT as well, since issues well beyond "just the hack" may suddenly surface (like the theft or loss of employee data). The IRP should have full sign-off by senior management so again, there are no surprises, and no excuses.

c) The IRT and IRP should be "owned" by one person in the organization ("the head" of the IRT). This is not the time for too many cooks in the kitchen. This is the time for action, and ultimately the responsibility to get the organization back on line. The head of the IRT

should have a deputy who is completely skilled on his own with strong incident response skills and experience, and who can, as an alternate, also serve as the owner of the incident response plan. Underneath the owner and the deputy are normally skilled incident response handlers who on their own have strong technical intrusion detection and forensic skills. The size and shape of internal IRT's vary from company to company, and are obviously budgetary dependent as 24/7 ready IRT's have a price.

If the organization is solely US-based, it is possible to have only one owner of the IRP and one head of the IRT. In a global organization, the "one owner" policy may not be possible or even practical. Global organizations need to "globalize" their IRP's so that a local "owner" is in place, a person who is closer to the action, and closer to his designated third party vendors. A local owner will likely also be more familiar with local laws relating to cyber and privacy related disclosures which may be implicated when a cyber-security breach is investigated.

d) Many companies rely, in part, upon cyber breach lawyers and third-party vendors to help work with them and guide them through a data breach. The lawyers and vendors should be pre-selected well in advance, and be on a retainer in the event of a breach.[10] The lawyers and vendors need to be available 24/7. There are no vacations in cybersecurity land. Firm evidence of a breach developed by the IRT and its vendors may ultimately be developed which will require a great deal of attention thereafter by all involved in the company, so outside counsel should be involved in retaining the vendors to preserve any applicable privileges.

e) The IRT should contain some element of "pre-planned" internal and external crisis communications that are kept up to date because, depending upon the severity of the breach and the potential for severe reputational damage, there will likely be disclosure obligations (both formal and informal) following the breach. Notification of a "material" breach to investors may be necessary under US Securities and Exchange Commission guidance, or in any event, may be necessary in order to reassure both customers and investors that the company is on top of the cyber breach and doing everything possible to protect investors as well as its consumers. Given that today's news cycle is 24/7, the company needs to be ready to act on a moment's notice if it discovers (or it is notified by a third party like the FBI or Secret Service) that it has been breached. Finally, some sort of formal notification may be required in various jurisdictions depending upon privacy concerns. Because of potential formal notification requirements, it is important to have inside or external lawyers involved with and overseeing breach notifications.[11] In major nation-state attacks, law enforcement may also play some role in the disclosure of the breach.

Thus a good crisis management/investor relations firm with experience in major corporate catastrophic events should be on retainer as well. A major hack and the associated costs may also mean losing the faith and trust of customers, clients or patients. These circumstances could cause a "death spiral" that may be unrecoverable.

f) Engagement with Law Enforcement Before A Breach Occurs

As we noted above in the federal regulation chapter, the April 29, 2015 DOJ Incident Response memo makes it very clear that the Department of Justice recommends/suggests that a company get to know its local federal law enforcement agents (the local Field Office of the FBI and US Secret Service) before a breach occurs. We considered this good advice even before the DOJ IR memo, and now we strongly recommend this to all our clients. It makes complete sense to build a one-on-one relationship with these offices in order to facilitate a working and cordial relationship just in case something happens and the company needs immediate help. Having such a relationship is a great way to understand (well in advance) how your cyber-attack case will be handled by law enforcement; what information they will want to know, who they will want to talk to, and what information the FBI or Secret Service will need to help them do their job, and help you. The FBI or Secret Service can be a "friend in need" if the company later discovers it has been breached.

g) Practice, Practice, Practice.

> "Practice does not make perfect. Only perfect practice makes perfect."
> -Vince Lombardi

IRP's and IRT's are no good if they are dusty, and unpracticed. Drills need to be conducted on a regular basis (we would recommend at least quarterly) so that all members of the IRT and 3rd party vendors (and the company's lawyers and PR team) know exactly what they are supposed to do, and say, in the event of a major cybersecurity incident. Rather than repeat the same "exercise" over and over, practice sessions should be pre-planned to simulate a wide variety of situations, from DDoS attacks to situations involving the destruction of data.

A good IRT is like a college rowing team rowing a scull down the Charles River. Everyone needs to row in cadence and in the same direction to immediately respond to a cyber-attack given both customer information and corporate reputations are at the heart of any breach. As noted in one recent report,

> "Failure to act decisively when customer, investor and staff interests are at the heart of the matter, can cost a business a fortune, and, for senior executives, their jobs. Companies under stress from a cyber-incident are like families under stress - the strong ones come together and those that aren't, can fall to pieces under the pressure."[12]

2. *Detection and Analysis of Threat Vectors, or "Houston, We have a Problem"*

No incident response plan will be effective without the ability to accurately detect and assess possible incidents. How exactly this is done today is a moving target of both software and hardware necessary to detect incidents from a variety of threat vectors. The technical side of this equation is too complicated for laymen to understand, but, in sum, organizations need to be able, through "continuous monitoring,"[13] to identify "indicators" or "evidence" of an attack through network monitoring systems such as "event-based alert monitoring" and "header and full packet logging." In sum, both are designed to collect data transferred but are also systems to help the

IRT generate digital signatures, network system activity logs, or identify data that might show evidence of compromise when looked at in the whole. Here a few of the potential indicators of compromise that may show up:

- A network intrusion detection sensor alerts when a buffer overflow attempt occurs against a database server.
- Antivirus software alerts when it detects that a host is infected with malware.
- A system administrator sees a filename with unusual characters.
- An application logs multiple failed login attempts from an unfamiliar remote system.
- An email administrator sees a large number of bounced emails with suspicious content.
- A network administrator notices an unusual deviation from typical network traffic flows.[14]

But today, since many cyber-attacks are found to flow from one-time only use of malware (thus have no recognized "signature" to identify it as a threat), many companies are now transitioning to a signature-less intrusion detection system. One long term industry expert noted in a recent interview, "We don't know what to look for when nobody else has seen it. The [signature] model breaks down…. How you protect yourself from a shotgun blast is very different than how you protect yourself from a sniper's bullet. Traditional protection mechanisms are geared toward those noisy mass attacks."[15] To combat this cyber-attack technique, "Rather than relying on detecting known signatures, [many] companies marry big-data techniques, such as machine learning, with deep cybersecurity expertise to profile and understand user and machine behavior patterns, enabling them to detect this new breed of attacks. And to avoid flooding security professionals in a sea of useless alerts, these companies try to minimize the number of alerts and provide rich user interfaces that enable interactive exploration and investigation."[16]

Whatever the monitoring system in place (which includes antivirus software alerts), incident response information may contain evidence of either network traffic anomalies, or evidence of actual data theft, which could lead to the conclusion that there has been a data breach. Today, many monitoring systems are automated (and even outsourced) because, quite simply, large organizations may have tens of thousands of incidents daily that need to be analyzed, correlated and investigated. Logs should be kept and retained for some defined period (e.g. 60 days) as a matter of good practice as they may be needed for a breach investigation.

3. *Containment*

Containment means, "how do we stop the bleeding" so that no further damage can be done. Again, this topic is complicated so that both in-house and outside legal experts and third-party vendors are needed. In sum, a containment program should generally involve:

1. Isolating a network segment of infected workstations and taking down production servers that were hacked;[17]
2. A plan to isolate infected systems, forensically copy them and transfer them to another off-grid environment for further analysis by either your forensic team or law enforcement;

3. Triaging and analyzing the infection or malware so that an eradication plan can be formulated;

4. Notifying law enforcement immediately if the Company suspects that the incident stemmed from criminal behavior. Note here that the April 29, 2015 DOJ Incident Response memo states that any subsequent law enforcement investigation will be done with as little disruption as possible, and with as much discretion as possible.[18] Indeed, as we now know, local law enforcement has information that companies may not be privy to, like digital signatures from breaches of other companies. They may have other indicators that could help the company both identify the nature of the threat vector involved, where to look on the server to find the evidence of compromise, or other helpful information.

Finally, assuming the Company has come to the conclusion that a breach has occurred, and personally identifiable information has been compromised, it is important to have the IR/PR/legal team available to advise the IRT on potential disclosure obligations under federal law (like HIPAA), the data breach laws of most states, or under the law of a foreign government (EU/UK directives) that may be applicable.

If the company's incident response plan was prepared well in advance, these disclosures should be in some shape of "ready to go" but for filling in the facts as the company then understands them to be at the moment the press release is issued. Though it is critical for a company to not be too quick to issue a press release if it does not understand all the facts at that time, it can be equally critical to show the public (consumers and investors) that the company took decisive action when it first discovered the breach. Here again, experienced counsel and an experienced cyber IR/PR advisor can help the company find a happy medium for both public and required disclosures to regulators.

Though there is no right or wrong answer as to when to issue a breach press release, and how much to say in the release, clearly the trend is towards more and quicker disclosure rather than less when a company is breached. Keeping customer confidence is critical if a company wants to jump right back to its feet after a cybersecurity breach. In fact, one customer study noted "Thirty-five percent of respondents said they would stop shopping at a company altogether if it lost their personal data, while an additional 23 percent said they would be "much less likely to shop there. With figures like this, it's clear that breaches do drive customers away. And while large firms with deep pockets may be better able than smaller ones to ride out the storm and wait for customers' memories of the breach to fade, many millions of dollars will be lost in the interim."[19]

Lastly, disclosure will be necessary to the Company's cyber insurance provider. Many cyber insurance policies provide coverage (under their terms and conditions, which should be reviewed well in advance of any breach) so as to allow the company to take advantage of forensic and remediation services and coverage, as well as a "breach coach" and suggested third party vendors if the Company does not have such vendors on retainer.

4. *Remediation and Eradication*

Remediation and Eradication means "fixing the problem," as rapidly as possible after the threat vector is fully identified, so that the attacker doesn't have time to change his method or mode of attack. Eradication efforts could involve:

- Blocking malicious IP addresses identified during the investigation;
- Changing all passwords;
- Patching holes in the network architecture that are identified during the investigation;
- Fixing all vulnerabilities identified during the investigation.

5. *"Lessons Learned" Post-Mortem*

Cyber post-mortems are like many post-event discussions. Lessons can always be learned as to what went right with your IRP (where did you excel), what went wrong (what didn't work so well), and thus what areas can be improved upon by the entire IRT so that it can perform better during the next incident investigation.

WHY IS AN EFFECTIVE INCIDENT RESPONSE PLAN SO IMPORTANT TO ANY ORGANIZATION?

> "We are in a world now where, despite your best efforts, you must prepare and assume that you will be penetrated," he told the group. "It is not about if you will be penetrated, but when…." Admiral Mike Rogers, head of the NSA and US Cyber Command [20]

We placed this section here at the end of the chapter because, frankly, we didn't want to give away the punchline too early.

But we kind of did already with Admiral Roger's quote above. An effective IRP is absolutely vital to your organization because: (1) it has already been hacked (or doesn't know it yet), and thus (2) your organization needs to be able to take a "cyber punch," and get off the canvas to fight another day. An effective, table-top practiced incident response plan is essential for a variety of other reasons:

1. If you are in a specific industry sector, most especially the regulated financial services sectors, your regulators will specifically ask whether your organization has, in fact, an incident response plan. If your answer is "no," that answer might not be well received;
2. A battle-tested incident response plan may be evidence of cybersecurity best practices if the Company is later the subject of a lawsuit or regulatory proceeding resulting from disclosure of the breach;
3. A battle-tested incident response plan will hopefully prevent an organization from having a cyber-incident develop into a catastrophic event, either financial, reputational, or both, which could cause the company's decline or death in some cases if there is a "crisis in confidence," among customers or investors or a "run on the bank" following disclosure of the cyber-incident.

ENDNOTES

[1] Found at http://www.marketwatch.com/story/one-year-after-targets-breach-what-have-we-learned-2014-10-31.

[2] Found at: http://threatpost.com/nsa-director-rogers-urges-cyber-resiliency/108292#sthash.V4bkayBQ.dpuf.

[3] The author thanks Austin Berglas, a Senior Managing Director at K2 Intelligence, for his critical review and comments to this section.

[4] See "Sony Films Are Pirated, and Hackers Leak Studio Salaries," found at http://www.nytimes.com/2014/12/03/business/media/sony-is-again-target-of-hackers.html?_r=0; "Hackers Using Lingo of Wall St. Breach Health Care Companies' Email," found at http://www.nytimes.com/2014/12/02/technology/hackers-target-biotech-companies.html; "Hacking the Street," a Fire Eye/Mandiant Special Report, found at https://www2.fireeye.com/rs/fireye/images/rpt-fin4.pdf.

[5] See "Intrusion Detection FAQ: Can you explain traffic analysis and anomaly detection?" found at http://www.sans.org/security-resources/idfaq/anomaly_detection.php.

[6] See "New Ponemon Institute Study Reveals That Improving Cyber Resilience is Critical for Prevailing Against Rising Cyber Threats," available at http://www.freshnews.com/news/1129839/new-ponemon-institute-study-reveals-that-improving-cyber-resilience-critical-prevailin.

[7] See NIST "Computer Security Incident Handling Guide," (hereinafter, the "NIST Incident Handling Guide," found at http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf.

[8] Id.

[9] Next generation intrusion prevention systems and next generation firewalls will generally have some element of "machine learning" about what network behavior is "normal" versus what can be considered "abnormal." See e.g. "Creating cybersecurity that thinks," available at http://www.computerworld.com/article/2881551/creating-cyber-security-that-thinks.html (discuss the transition from signature-based to non-signature based intrusion detection technology).

[10] Three of the larger companies that we and our multi-national clients regularly deal with from an incident response perspective are Fire Eye/Mandiant, Verizon, and IBM. See https://www.fireeye.com/, http://www.verizonenterprise.com/products/security/, and http://www-935.ibm.com/services/us/en/it-services/security-services/emergency-response-services/?S_TACT=R02102GW&S_PKG=-&cmp=R0210&ct=R02102GW&cr=google&cm=k&csr=IT+Emergency+Response+Services_UN&ccy=us&ck=security%20services&cs=b&mkwid=sk3dL6Acl-dc_49046510203_4326fb30773. There are certainly other companies in the incident response space that have the ability to fully respond to domestic breaches, see e.g. https://www.k2intelligence.com/.

[11] In some cases, and for some larger companies, it may even be important for companies to consider "off the grid" communications systems, like temporary cellphones and satellite phones so that key IRT members can communicate with each other in the event that the breach also affects a Company's corporate phone lines. See "Spike in Cyber Attacks Requires Specific Business Continuity Efforts," found at http://www.emergency-response-planning.com/blog/topic/cyber-security.

[12] See KPMG "Global CEO Outlook 2015," http://www.kpmginfo.com/ceo-outlook2015/documents/CEOSurvey_2015-US-Revise-07-22-FINAL-R.pdf.

[13] "Continuous Monitoring" is the hallmark of a Implementation Tier 4 organization in the NIST cybersecurity framework. See NIST Cybersecurity Framework, found at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[14] See "Cybersecurity and Privacy Diligence in a Post-Breach World," available at http://corpgov.law.harvard.edu/2015/02/15/cybersecurity-and-privacy-diligence-in-a-post-breach-world/.

[15] See "On prevention vs. detection, Gartner says to rebalance purchasing," available at http://searchsecurity.techtarget.com/news/2240223269/On-prevention-vs-detection-Gartner-says-to-rebalance-purchasing.

[16] See "Why Breach Detection Is Your New Must-Have, Cybersecurity Tool," available at http://techcrunch.com/2014/09/06/why-breach-detection-ss-your-new-must-have-cyber-security-tool/. A very good description of how big-data cyber analytical tools work is available in the following article, "Connecting the Cyber-Threat Dots Through Big Data," available at http://www.smartdatacollective.com/juliehunt/332900/connecting-cyber-threat-dots-through-big-data.

[17] For a very good summary of basic incident response plans and techniques, see Incident Handler's Handbook," SANS Institute: InfoSec Reading Room, available at http://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901.

[18] Cooperation with law enforcement may also garner a company "more favorable" treatment by the Federal Trade Commission in any subsequent breach investigation by that agency. See "If the FTC comes to call," available at https://www.ftc.gov/news-events/blogs/business-blog/2015/05/if-ftc-comes-call?utm_source=govdelivery ("We'll also consider the steps the company took to help affected consumers, and whether it cooperated with criminal and other law enforcement agencies in their efforts to apprehend the people responsible for the intrusion. In our eyes, a company that has reported a breach to the appropriate law enforcers and cooperated with them has taken an important step to reduce the harm from the breach. Therefore, in the course of conducting an investigation, it's likely we'd view that company more favorably than a company that hasn't cooperated.").

[19] See "Survey: Consumer Confidence in the Security-Breach Era," available at http://intelligent-defense.softwareadvice.com/consumer-confidence-security-breach-era-0614/.

[20] For the article containing the quote, see "NSA Chief Expects More Cyberattacks Like OPM Hack: Mike Rogers says, 'I don't expect this to be a one-off'" available at http://www.wsj.com/articles/nsa-chief-expects-more-cyberattacks-like-opm-hack-1436985600.

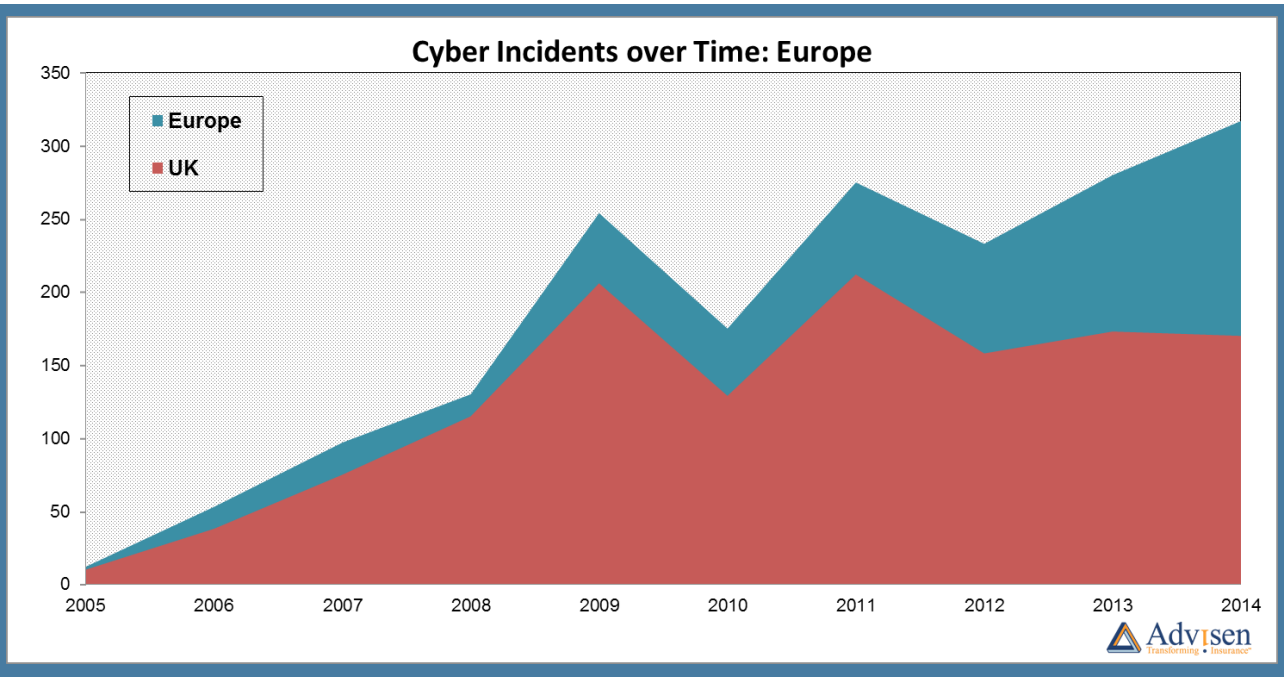
CHAPTER 9:

FACTORING UK/EU PRIVACY ISSUES INTO YOUR DATA COLLECTION AND CYBERSECURITY EQUATION

PURPOSE OF THIS CHAPTER:

1. Identify the Important Provisions of the EU Data Protection Directive of 1995.
2. Identify the Important Provisions of the UK Data Protection Act of 1998.
3. Identify Potential Changes Being Discussed for The New Network and Information Security ("NIS") Directive.

Unlike the United States where discussions concerning data privacy concerns have often, rightly or wrongly, taken a back seat to cybersecurity concerns (at least before the name Edward Snowden[1] was uttered in public), privacy concerns historically have been the most important issue in Europe since World War II.[2] These privacy concerns have been formally legislated in both the United Kingdom and in the European Union ("EU") at least since 1980, and have taken on different shapes and forms all centered upon the right of privacy in one's personal and family life. [3] A very good article in the Financial Times recently noted the following, "The key difference is a legal one: in Europe, data protection is a fundamental right and in the US it does not have the same status."[4]

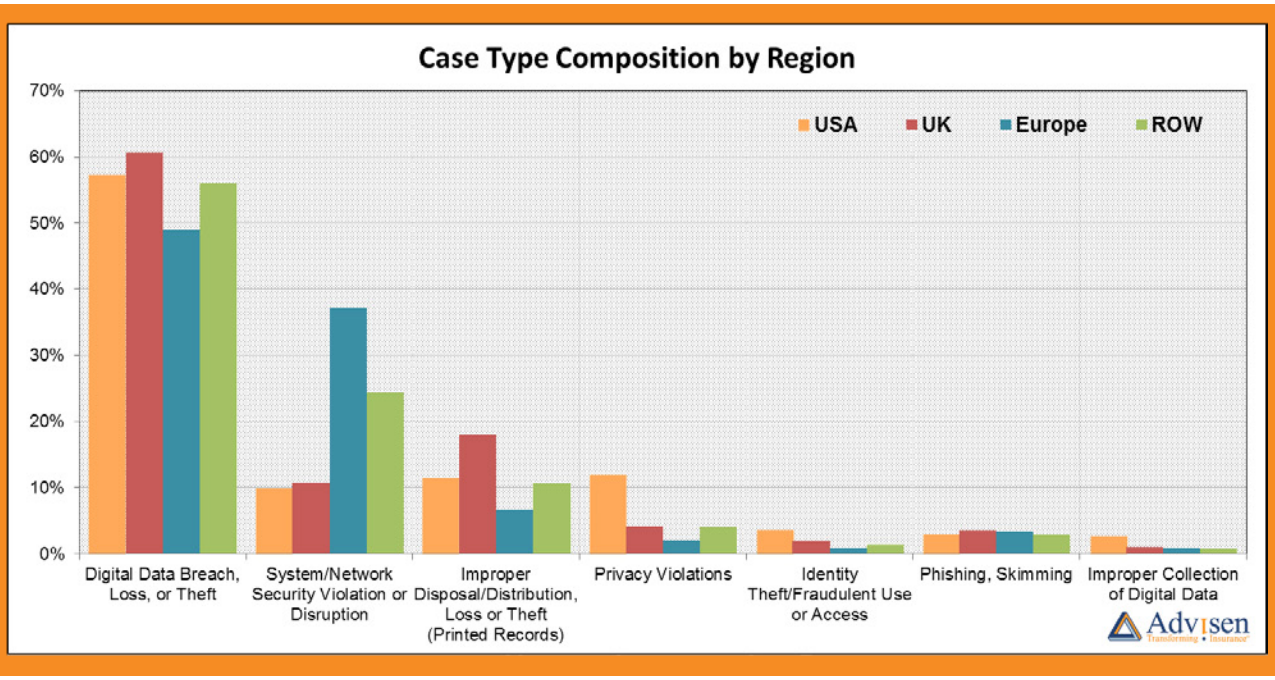


Though the exact legal requirements of both the UK and EU privacy laws are beyond the scope of this book (and of this NY-based lawyer), we mention them here briefly because they too present unique cybersecurity concerns and challenges to multi-national companies doing or conducting business in the UK and EU, or transferring personal data between the UK/EU and the United States. These concerns not only impact how data are collected and stored in the UK and EU, but also how companies can and should respond in the event there is a cybersecurity incident that needs to be investigated. Finally there are breach notification laws in the UK and EU that need to be complied with. These new requirements may in some cases require companies to hire Chief Privacy Officers or Chief Data Protection Officers. Of course, like additional cybersecurity regulation expected here in the United States as a result of the monster data breaches of 2013 and 2014, a new European Data Protection Regulation is also expected to be implemented sometime in 2016, which will likely carry with it even larger fines: up to five percent of global revenue for a serious breach. Since regulatory risk and red flags present unique problems to directors charged generally with Enterprise Risk Management, we lay them out here so that board members can proactively understand and deal with international data collection and data security issues as they arise during the business cycle.[5]

The EU Data Protection Directive of 1995 ("Directive 95/46")

Directive 95/46 was adopted by the European Union to, among other things, protect the privacy and protection of personal data collected for, or about the citizens of the European Union. Directive 95/46 is founded on seven essential principles:

- **NOTICE:** subjects whose data are being collected should be given notice of such collection.
- **PURPOSE:** data collected should be used only for stated purpose(s) and for no other purposes.
- **CONSENT:** personal data should not be disclosed or shared with third parties without consent from its subject(s).



- **SECURITY:** once collected, personal data should be kept safe and secure from potential abuse, theft, or loss.
- **DISCLOSURE:** subjects whose personal data are being collected should be informed as to the party or parties collecting such data.
- **ACCESS:** subjects should be granted access to their personal data and allowed to correct any inaccuracies.
- **ACCOUNTABILITY:** subjects should be able to hold personal data collectors accountable for adhering to all seven of these principles.[6]

Found in these seven principles are two fundamentals: (1) that data should not be disclosed or shared with third parties without the consent of its subjects, and (2) once collected, personal data should be kept safe and secure. There is no affiliated definition under Directive 95/46 as to what "safe and secure" means, though we would expect that basic and documented adherence to some recognized data security standard like ISO 27001, COBIT or the NIST cybersecurity framework would at the very least provide some evidence that information collected is being kept safe and secure.

Directive 95/46 applies to not only responsible parties (the term of art is "data controllers") that operate within the EU, but also when a responsible party (perhaps located in the US) uses servers set up in an EU jurisdiction to process personal data.

There is no express breach notification requirement under Directive 95/46, though under later EU privacy regulations, EU electronic communications service providers (such as phone companies and ISPs) have to notify their competent national authorities of any personal data breaches without undue delay, and may also be required to notify the potential victims themselves.[7]

The UK Data Protection Act of 1998

The UK Data Protection Act of 1998 ("the UK 1998 Act") was meant to bring the United Kingdom of Great Britain and Northern Ireland into line with Directive 95/46, and generally requires that personal data should only be processed fairly and lawfully. In order to be processed "fairly and lawfully," one of these six pre-conditions must be met:

1. The data subject (the person whose data is stored) has consented (given their permission) to the processing;
2. Processing is necessary for the performance of, or commencing, a contract;
3. Processing is required under a legal obligation (other than one stated in the contract);
4. Processing is necessary to protect the vital interests of the data subject;
5. Processing is necessary to carry out any public functions;
6. Processing is necessary in order to pursue the legitimate interests of the "data controller" or "third parties" (unless it could unjustifiably prejudice the interests of the data subject).

Exceptions to these pre-conditions include:

- Section 28 of the UK 1998 Act- National security. Any processing for the purpose of safeguarding national security is exempt from all the data protection principles, as well as Part II (subject access rights), Part III (notification), Part V (enforcement), and Section 55 (Unlawful obtaining of personal data).
- Section 29 of the UK 1998 Act - Crime and taxation. Data processed for the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of taxes are exempt from the first data protection principle.
- Section 36 of the UK 1998 Act - Domestic purposes. Processing by an individual only for the purposes of that individual's personal, family or household affairs is exempt from all the data protection principles, as well as Part II (subject access rights) and Part III (notification).

Data Transfer outside the UK/EU to and from the U.S., Pre-October 2015

As written initially, neither Directive 95-46 or the UK 1998 Provisions allow the transfer of personal data outside of the UK and the European Union countries to the United States, thus potentially making the data collection and transmission for multi-national US companies daunting, if not impossible to execute without irritating one regulator or another along the way. For this reason the EU and the US Department of Commerce developed the "US/EU Safe Harbor Framework," to provide "a streamlined and cost-effective means for U.S. organizations to satisfy the Directive's "adequacy of privacy" requirement…[8] The U.S.-EU Safe Harbor Framework… is an important way for U.S. organizations to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by EU member state authorities under EU member state privacy laws."[9] Under the provisions of the US/EU Safe Harbor, data can only be transferred outside borders if there are assurances that it will be accorded same legal protections.

Prior to October, 2015 more than 4,000 US companies self certified that they met the US/EU Safe Harbor Framework requirements. Some of the basic requirements included:

- **CONFIRMATION THAT ORGANIZATION IS SUBJECT TO THE JURISDICTION OF THE U.S. FEDERAL TRADE COMMISSION OR THE U.S. DEPARTMENT OF TRANSPORTATION:** Any U.S. organization that is subject to the jurisdiction of the Federal Trade Commission (FTC) or U.S. air carriers and ticket agents subject to the jurisdiction of the Department of Transportation (DoT) could participate in the Safe Harbor.
- **DEVELOP A SAFE HARBOR COMPLIANT PRIVACY POLICY STATEMENT:** A Safe Harbor compliant privacy policy was necessary for self-certification.
- **ENSURE THAT YOUR PRIVACY POLICY CONFORMS TO THE U.S.-EU SAFE HARBOR PRIVACY PRINCIPLES:** In order for a privacy policy to be compliant with the Framework, the privacy policy had to conform to the Safe Harbor Privacy Principles, as well as any relevant points covered in the Frequently Asked Questions (FAQs), which are located with the other Framework documents. In addition, the privacy policy had to reflect your organization's actual and anticipated information handling practices.
- **REFERENCES IN THE TEXT OF PRIVACY POLICY TO SAFE HARBOR COMPLIANCE:** FAQ 6 requires each organization that self-certifies to state in its applicable published privacy policy that

it complies with the U.S.-EU Safe Harbor Framework and that it has certified its adherence to the Safe Harbor Privacy Principles.

- **ENSURE THAT YOUR ORGANIZATION'S VERIFICATION MECHANISM WAS IN PLACE:** As discussed in FAQ 7, organizations self-certifying to the Framework were required to have procedures in place for verifying compliance. To meet this requirement, organizations generally used either a self-assessment or an outside/third-party assessment program.
- **DESIGNATE A CONTACT REGARDING SAFE HARBOR:** Each organization was required to provide a contact for the handling of questions, complaints, access requests, and any other issues arising under the Safe Harbor. This contact can be either the corporate officer certifying compliance, or another official, such as a Chief Privacy Officer.[10]

THE BENEFITS FOR A US ORGANIZATION TO BECOME CERTIFIED WERE IMMENSE:

- All 28 Member States of the European Union were be bound by the European Commission's finding of "adequacy";
- Participating organizations were deemed to provide "adequate" privacy protection;
- Member State requirements for prior approval of data transfers either was waived or approval was automatically granted;
- Claims brought by EU citizens against U.S. organizations were heard, subject to limited exceptions, in the U.S.; and
- Compliance requirements were streamlined and cost-effective, which particularly benefited small and medium enterprises.

With the use of Binding Corporate Rules approved by the particular nation-state data protection authority, all multi-national companies may also be able to transfer data within their own corporate network without signing something akin to a model contract when each such transfer is made. "Binding Corporate Rules ("BCR") are internal rules (such as a Code of Conduct) adopted by a multinational group of companies which define its global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection."[11] BCRs are normally made to the lead data protection authority (e.g., Germany), and then, if approved, they are co-recognized by the other EU jurisdictions. To date, 45 corporations have received individual BCR approval. This can be a time-consuming process as it requires application to, and often negotiation with, individual member-state data protection authorities.

EU/UK/US Data Transfer Post October 2015

On October 6th, 2015, the European Court of Justice (ECJ) issued a ruling in Schrems v. Data Protection Commissioner that has invalidated the European Commission's decision that the data privacy principles of U.S.-E.U. Safe Harbor - pursuant to which U.S. companies transfer personal information about E.U. citizens to the U.S. after agreeing to abide by these principles - provide an adequate level of protection for the data of E.U. citizens. As a result of this ECJ decision, the privacy supervisory authority in each E.U. Member State has the power to question whether transfers of personal data to the U.S. comply with E.U.

data protection law and to suspend such transfers if E.U. privacy obligations are not met. The impact is potentially enormous for the thousands of U.S. multinational companies that currently operate under the Safe Harbor (as well as for the thousands of European businesses that have their data hosted in the U.S. by these U.S. companies), but the European Commission has indicated that it is committed to finding a "safer" safe harbor so that the transfer of transatlantic data can continue. Regardless, companies that rely on the U.S.-E.U. Safe Harbor agreement must review their current practices and consider alternatives.

THE ECJ DECISION SUMMARY

On October 6th, 2015, the ECJ issued a non-appealable opinion that essentially invalidates reliance upon the U.S.-E.U. Safe Harbor. Adopting the reasoning of the Advocate General's Opinion, the ECJ found that Safe Harbor did not provide an adequate level of data protection given U.S. intelligence activities. The ECJ held that the European Commission's 2000 decision finding that the U.S. Safe Harbor provides an adequate level of protection is invalid and does not trump the powers available to E.U. national data supervisory authorities to question the lawfulness of transfers under the U.S. Safe Harbor regime.[12]

The Schrems case will resume in Ireland, with the specific merits of that case to be determined. As a result of the ruling, we are likely to see other data privacy complaints filed against DPAs in other Member States, with unpredictable and likely varying results. Thus, the privacy requirements in the E.U. have the potential to become disparate and unwieldy, and U.S. companies may find it necessary to adjust their data privacy policies on a country-by-country basis.

TAKEAWAYS FROM THE SCHREMS DECISION

We expect that E.U. national data supervisory authorities will be inundated with complaints from individuals and consumer groups. There are a number of existing alternatives to the Safe Harbor, which include:

- Restructuring data storage architecture to ensure that European data remains in Europe. Such a restructuring may add significant cost as well as impacting corporate structure.
- Adopting Binding Corporate Rules (BCRs), which are internal rules adopted by multinational groups of companies and approved by the E.U.[13] BCRs can be costly and time consuming to develop and implement, but would provide a U.S. company with essentially the same capacity to transfer data as it enjoyed under the Safe Harbor agreement.
- Adopting the pro forma model contractual clauses approved by the European Commission.
- Obtaining individual consent. For example, the addition of an extra consent form for European users to click, explicitly allowing a company to transfer their data to U.S. servers.

In the wake of the decision, the European Commission has said it would work with national supervisory authorities to issue further guidelines - including a "safer" safe harbor. European Commission and U.S. officials had already entered into negotiations in 2013 for creating a new Safe Harbor agreement. The ECJ ruling may also place more pressure on Congress to pass legislation currently under consideration that would allow E.U. citizens to bring privacy lawsuits in U.S. courts.

The New Network and Information Security ("NIS") Directive/ EU General Data Protection Regulation

The new NIS and EU General Data Protection regulations are potential game-changers for companies collecting and processing information in the EU and UK, as they will, when implemented (maybe the end of 2016) provide for one stop-shopping for data controller and processors[14] to understand the "rules of the road." "It will also provide citizens with a 'right to be forgotten' if they want old or inaccurate data deleted, a right to know what information is stored about them and whether it is correct - as well as a right for transparency in the way data is collected. There will be significant fines - in the current draft the suggested figure is 5% of global turnover or €100 million if greater - for companies that negligently breach regulations."[15]

The new NIS Directive, adopted by the EU Parliament in March 2014 is equally important, and will likely go into effect in or about 2016 when the new EU Directive comes on line. The exact timetable is uncertain however and the Directive continues to be negotiated.[16] Under the NIS Directive, "Member states are required to adopt a national strategy that sets out concrete policy and regulatory measures to maintain a level of network and information security. This includes designating a national competent authority for information security and setting up a computer emergency response team (CERT) that is responsible for handling incidents and risks."[17] Along with a national strategy setting forth measures to maintain a minimum level of cybersecurity, under the NIS Directive member states will be required to form a cooperation network to coordinate against risks and incidents. "The network will exchange information between authorities, provide early warnings on information security issues and agree on a coordinated response in accordance with an EU NIS co-operation plan."[18]

Asia Pacific Data Privacy Requirements

If dealing with UK and EU data collection and privacy requirements were not enough, let's add one more regulatory jurisdiction to the mix: The Asia-Pacific Economic Communities (APEC).

In November 2004, 21 countries endorsed the APEC Privacy Framework ("the APEC Framework"). The Framework is comprised of a set of nine principles and guidance on implementation to assist APEC Economies in developing consistent approaches to personal information privacy protections. It also forms the basis for the development of a regional approach to promote accountable and responsible transfers of personal information between APEC Economies. Like the rules of the EU and UK, the APEC Framework is very much grounded on privacy concerns:

- To develop appropriate privacy protections for personal information, particularly from the harmful consequences of unwanted intrusions and the misuse of personal information;
- To enable global organizations that collect, access, use or process data in APEC Economies to develop and implement uniform approaches within their organizations for global access to and use of personal information;
- To assist enforcement agencies in fulfilling their mandate to protect information privacy; and
- To advance international mechanisms to promote and enforce information privacy and to maintain the continuity of information flows among APEC economies and with their trading partners.[19]

Without getting into specific details of the APEC Framework, note that it is very similar in effect to both the EU-US Safe Harbor and the EU Binding Corporate Rules. It allows cross-border transfer of data in the APEC countries more easily. However there is an extensive certification process involved with getting APEC certification.[20] We will now have to see whether the APEC countries follow the ruling in Schrems and similarly invalidate the safe harbor governing data transfers to and from their region and the US.

IMPLICATION OF THE NEW EU DATA REGULATION, APEC FRAMEWORK AND INDIVIDUAL APEC DATA PRIVACY REQUIREMENTS

Though it is obviously hard to tell whether or not the new EU General Data Protection Directive and the new NIS Directive will result in positive benefits to the international cybersecurity and privacy community, we think it is important to note the potential implications of the new EU General Data Protection Directive.[21] We think those implications are different depending upon where each individual company is in its cyber-security lifecycle. For companies that have cyber-security DNA in their culture, it is likely the new EU General Data Protection Directive will have some, but not significant impact, as these companies by implication already are taking active measures to protect the personal information of their customers and investors.[22] Additional steps may be needed to incorporate new disclosure "timetable" requirements into their Incident Response Plan ("IRP") when dealing with both individuals and EU regulators.[23] But that should be it. Note: Timing is everything with a battle-tested IRP, and the timing of potential disclosures to EU and UK regulators will have to be figured in the mix when companies are in the middle of their IRP, hoping to contain and mitigate a cyber-security incident.

For companies that are well up/down the cybersecurity learning curve, the new EU General Data Protection Directive, the invalidation of the EU safe harbor, along with the APEC Framework and individual APEC data privacy requirement, spells an additional level of regulatory risk if they are found to be non-compliant. Companies with UK collection sites should be well-prepared with an Incident Response and disclosure plan which takes into account the new rules, or face historic fines and penalties for the failure to comply. The complexity of the international data protection regime may require some companies to hire a chief data protection officer ("DPO"), especially those companies that sell products and render services to Europeans.[24] Moreover, given the Schrems v. Data Protection Commissioner decision invalidating the Safe Harbor, now is the best time to go back through the Company's cybersecurity policies and procedures to make sure they are privacy-and-disclosure-ready as well as cybersecurity-ready. Given its similarity to the US/EU Safe Harbor (which has now been invalidated), we do not know at this time whether the APEC nations will follow the Schrems decision and prohibit data transfers from the APEC nations to the US.

ENDNOTES

[1] See biography of Edward Snowden, found at http://en.wikipedia.org/wiki/Edward_Snowden.

[2] There is no one document we are aware of that attributes the origin of EU privacy concerns. It is posited however that privacy concerns arise out of the Nazi's use of confidential names, addresses and personal information to commit horrible atrocities upon many European nations and communities. In the United States, concerns about freedom of speech under the First Amendment have always dominated society, and the advent of social media has only amplified American's concerns that they can both be seen and heard at any time. Notwithstanding, we note that several US laws (like e.g. HIPAA, GBLA and SEC Regulation S-ID) have express requirements that patient and depositor/customer information remain private and that appropriate precautions are taken to safeguard such information. See e.g., SEC Regulation S-ID, found at http://www.sec.gov/rules/final/2013/34-69359.pdf.

[3] See Gonzalez v. Google, E.C.J. (May 13, 2014). Articles 7 and 8 of the Charter of Fundamental Human Rights of the European Union state "everyone has the right to respect for his or her private and family life, home and communications." See also Article 29 "Working Party Issues Guidelines on the Implementation of the EU's Right To Be Forgotten", found at https://privacyassociation.org/news/a/article-29-working-party-issues-guidelines-on-the-implementation-of-the-eus-right-to-be-forgotten/.

[4] See "Concerns grow over EU digital rules targeting American companies", available at http://www.ft.com/cms/s/0/56e58018-3393-11e5-b05b-b01debd57852.html#ixzz3kfquV3EH.

[5] Please note that data collection issues are not only issues in the EU/UK and US. Companies doing business or collecting information in other parts of the world should similarly consult with experts to become aware of additional nation-state requirements.

[6] See EU Data Protection Directive (Directive 95/46/EC) found at http://searchsecurity.techtarget.co.uk/definition/EU-Data-Protection-Directive. For a more general discussion of the Directive, Wikipedia has a helpful link, which is available at https://en.wikipedia.org/wiki/Data_Protection_Directive.

[7] See Data Breach Notifications - New Rules, found at http://www.timelex.eu/en/blog/detail/data-breach-notifications-new-rules.

[8] The "adequacy of privacy" requirement means generally that the organization being certified under the Safe Harbor provides for adequate level of data protection.

[9] See "U.S.-EU Safe Harbor Overview," found at http://www.export.gov/safeharbor/eu/eg_main_018476.asp.

[10] See generally for a fuller description of these requirements http://www.export.gov/safeharbor/eu/eg_main_018495.asp.

[11] See "Overview on Binding Corporate Rules," found at http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm.

[12] European Court of Justice Press Release No 117/15, Judgment in Case C-362/14 Maximillian Schrems v. Data Protection Commissioner (Oct. 6, 2015).

[13] European Commission's Directorate General for Justice and Consumers, Overview on Binding Corporate Rules (Sept 2, 2015), available at http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm.

[14] It is important to note that in its present form the new EU Directive will apply not only to data collectors, but also data "processors" as well. This means that if you store information in the cloud, your cloud service provider must also comply with the new regulations. See "10 things you need to know about the new EU data protection regulation," available at http://www.computerworlduk.com/security/10-things-you-need-know-about-new-eu-data-protection-regulation-3610851/#.

[15] See "The enterprise guide to preparing for the EU's new data-protection legislation," found at http://www.information-age.com/technology/security/123458144/enterprise-guide-preparing-eus-new-data-protection-legislation#sthash.zpak2KZV.dpuf. The new EU Data Protection Regulation will also provide a 72 hour mandatory notification rule in the event an organization has suffered a breach.

[16] See "Three-way EU Big Data privacy wrestling match kicks off," available at http://www.theregister.co.uk/2015/06/24/big_data_protection_negotiations_commence_on_wednesday/.

[17] See "What to Expect from Europe's NIS Directive," found at http://www.computerweekly.com/opinion/What-to-expect-from-European-NIS-Directive.

[18] Id.

[19] See "APEC CROSS-BORDER PRIVACY RULES SYSTEM," found at http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.ashx.

[21] Id. Further note that many of the individual nations in the Asia Pacific economy also have their own individual data privacy rules. See e.g., http://lawbrain.com/wiki/Asia-Pacific_Privacy_Law .

[22] Indeed the new NIS Directive may be helpful in ultimately bring many European data protection standards together under one roof, which was the practical result of the US's adoption of the NIST cybersecurity framework.

[23] We do not want to present a picture that the UK doesn't care about cybersecurity concerns. That is not true. On June 5, 2014 the UK government rolled out its Cyber Essentials Scheme, which laid out a voluntary certification program for UK businesses to follow to evidence their compliance with certain cybersecurity essentials. See generally, "Cyber Essentials Scheme," ("the Scheme") available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317481/Cyber_Essentials_Requirements.pdf. The Scheme is based upon 5 prerequisites that, if satisfied, may prevent or mitigate a cyber attack. For a shortened version of the Scheme, see "Guide to the UK government cyber essentials scheme," available at https://www.titania.com/sites/default/files/articles/Guide%20to%20the%20UK%20government%20cyber%20essentials%20scheme.pdf.

[24] See "10 things you need to know about the new EU data protection regulation," available at http://www.computerworlduk.com/security/10-things-you-need-know-about-new-eu-data-protection-regulation-3610851/#.

CHAPTER 10:

PRIVACY AND DATA SECURITY[1]

PURPOSE OF THIS CHAPTER:

1. Provide an overview of U.S. Privacy Law.
2. Identify the key privacy risks that companies face.

What is privacy? Privacy generally means the right to be left alone, or to be free from interference or intrusion. When we talk about privacy in the information context, we generally mean a person's right to have some control over how his or her personal information is collected and used. Privacy and cybersecurity overlap in that one of the primary goals of cybersecurity is to protect personal information.

What is personal information (aka "personally identifiable information," "PII," and many others)? There's no single, accepted definition in the United States. Some people use the term to mean name and contact information, such as address, phone number and email address. Most people agree that it includes social security number, driver's license or other government identification number, and credit card information. At its broadest, it may include any "persistent identifier that can be used to recognize a user over time and across different Web sites or online services."[2]

Why should companies care about data privacy? Well, in addition to being good business, it's the law — or maybe we should say, it's the laws. Unlike certain foreign jurisdictions, no single comprehensive law governs privacy in the United States; U.S. privacy law is primarily derived from various federal and state laws and regulations. Federal laws range from various sector-specific laws and regulations that apply to specific industries or to specific types of information, to general consumer protection laws and regulations that broadly prohibit unfair or deceptive acts and practices. Additionally, most states have laws that apply to privacy, whether prescribing procedures in the event of a data breach, prohibiting employers from requesting social media passwords, or requiring operators of websites and online services to post a privacy policy that satisfies specific requirements. Entities doing business in the United States can also find themselves subject to regulations from other sources, including self-regulatory frameworks that have become the norm in certain areas.

It's a lot of laws. And they are enforced by a lot of different entities - various federal agencies, state attorneys general, and sometimes, "enforcement" comes in the form of consumer class action lawsuits. Indeed, it may be easier to talk about who doesn't claim some sort of jurisdiction over privacy (answer: almost no one). It is critical for businesses that collect personal information to ensure that they comply with any and all applicable privacy and data security laws or they may face government investigations, sanctions, and private lawsuits.

In this chapter we provide an overview of the U.S. privacy framework and offer insights and suggestions for how to mitigate certain key privacy risks that many companies face.

Privacy at the Federal Level

In the absence of a single federal statute specifically governing data privacy in the United States, the Federal Trade Commission ("FTC") has taken a leading role in regulating privacy. The FTC's authority is based on Section 5 of the Federal Trade Commission Act, which broadly prohibits "unfair or deceptive acts or practices in or affecting commerce."[3] In this context, deception is generally defined as a material representation or omission that is likely to mislead consumers acting reasonably under the circumstances.[4] Unfair practices are ones that cause or are likely to cause substantial injury to consumers and are not outweighed by countervailing benefits to consumers or competition and are not reasonably avoidable by consumers.[5] By alleging deception, unfairness, or both, the FTC can and has applied Section 5 to many different situations, entities, and technologies, including privacy, marketing, blogging and other social media activities.[6]

To protect privacy and personal information, the FTC may bring an enforcement action or commence an investigation under Section 5. With skillful and experienced counsel, many companies are able to negotiate settlements with the FTC before litigation ensues. For example, in 2014, the FTC entered into a consent decree with Snapchat to settle charges that Snapchat deceived consumers into believing that messages sent via the service would disappear when, in fact, there were numerous ways to capture and retain users' messages. The FTC also alleged that Snapchat mislead users regarding the amount of personal information it collected and the security measures it employed.[7] Consent decrees can create numerous on-going obligations for a company: they can require the comprehensive privacy and security programs, robust privacy notice mechanisms, third-party audits, monetary redress, disgorgement of profits, or deletion of personal information obtained via impermissible means. In its consent decree, Snapchat neither admitted nor denied the allegations, but it agreed to implement a comprehensive privacy program and agreed not to make any future misrepresentations about the extent to which a message is deleted after being viewed by the recipient, among other things.[8] Note that a company's subsequent failure to comply with the provisions of its consent decree can result in federal court proceedings and civil penalties.

The FTC doesn't just pursue enforcement actions and investigations; it also undertakes consumer education initiatives, conducts studies, issues reports, hosts workshops, and plays an active role in shaping legislative and regulatory proposals concerning privacy. For example, the FTC recently issued a report on privacy concerns relevant to the "The Internet of Things,"[9] that is meant to help provide businesses with concrete steps that they can take to enhance and protect customers' privacy and security in the context of Internet-connected devices, such as headphones, wearable devices, and even refrigerators — things we all use every day.[10]

The FTC isn't the only player when it comes to privacy enforcement. Other federal agencies with enforcement authority in the data privacy arena include:

- Consumer Financial Protection Bureau
- Federal Communications Commission
- Department of Commerce
- Department of Health & Human Services
- Federal Reserve
- Comptroller of the Currency
- Department of Labor
- Equal Employment Opportunity Commission
- National Labor Relations Board
- Securities and Exchange Commission

The White House has also been active in the privacy space. In February 2015, the White House released a discussion draft of the Consumer Privacy Bill of Rights Act of 2015.[11] According to a White House representative, the proposed bill, which would apply across industries, "seeks to provide consumers with more control over their data, companies with clearer ways to signal their responsible stewardship over data and strengthen relationships with customers, and everyone the flexibility to continue innovating in the digital age."[12] To accomplish this, the bill proposes that, among other things, covered entities be required to collect, use, and retain personal information in a manner that is reasonable in light of how it is collected, and provides additional consumer protections for any use of data out of context.[13]

There are also several sector-specific laws that have detailed requirements about the collection and use of certain types of personal information or use of personal information by certain entities. The discussion below is meant as a high-level summary of some of these laws; it is not a substitute for consulting experienced counsel to help understand and aid compliance with all of the requirements of applicable law.

Financial Sector

The Gramm-Leach-Bliley Act ("GLBA") applies to "financial institutions" or companies that offer financial products or services to individuals, and requires these companies to explain their information-collection and information-sharing practices to customers and to protect sensitive data.[14] Under a rule promulgated by the FTC, an entity must be "significantly engaged" in financial activities to be considered a "financial institution." Notably, this definition can apply to businesses that would not normally describe themselves as financial institutions, such as retailers that issue their own credit cards or providers of medical services that generate a significant number of long-term patient payment plans involving interest charges.

The Fair Credit Reporting Act ("FCRA") essentially allows consumers to access and correct information that consumer credit reporting agencies maintain, and limits the use of consumer credit reports to certain defined purposes. The FCRA also requires that consumers be given notice when third-party information

is used to make adverse decisions about them. Note that there are additional requirements when credit information is used to make employment decisions. The FCRA was amended by the Fair and Accurate Credit Transactions Act ("FACTA") in 2003 and now includes rules about properly disposing of credit information and procedures for detection, prevention and mitigation of identity theft.

Healthcare Sector

The Health Insurance Portability and Accountability Act ("HIPAA") protects the privacy of individually identifiable health information via its Privacy and Security Rules. The HIPAA Privacy Rule requires covered entities - healthcare providers, health insurers and healthcare clearinghouses - to provide consumers with a detailed privacy policy, to implement security safeguards for personal health information ("PHI"), and to make reasonable efforts to limit the use and disclosure of PHI.[15] The HIPAA Security Rule, in turn, requires covered entities to "[e]nsure the confidentiality, integrity, and availability" of electronic protected health information ("ePHI").[16] HIPAA also mandates that third-party vendors and service providers ("business associates") undertake particular obligations to protect PHI.

Students and Children

The Family Educational Rights and Privacy Act ("FERPA") applies to disclosure and access to student education records. Generally, FERPA prohibits educational institutions that received federal funding from disclosing education record information without the student's consent.

The Children's Online Privacy Protection Act ("COPPA") applies to companies that operate commercial websites that collect information from children under the age of 13. These website operators must post privacy notices and obtain verifiable parental consent before collecting information from children. It also requires that parents be given access and the ability to delete their children's information, and that children's information be kept confidential and secure.

Marketing and Communications

There are various laws and regulations that govern how marketers may contact individuals. The Telemarketing Sales Rule (TSR) established the "Do Not Call" registry, as well as various rules governing "robocalls." Among other provisions, telemarketers must scrub their calling lists against the Do Not Call Registry, make specific disclosures to consumers and must keep records regarding their activities. The Telephone Consumer Protection Act (TCPA) prohibits the use of autodialers to cell phones (including text messages) without prior consent. The CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing Act) applies to commercial email messages that advertise or promote a product, and prohibits misleading headers and subject lines, requires that the sender maintain a functional opt-out system, and prohibits certain automated practices. There are also rules about the use of fax machines for marketing messages.

In addition, the Video Privacy Protection Act (VPPA) prohibits "video tape service providers" from disclosing customer personal information other than for certain limited exceptions. It was passed after then-Supreme Court nominee Robert Bork's video rental records (nothing salacious in them) were disclosed during the confirmation hearings. The VPPA has gotten a lot of play recently in the context of social media integration as customers' playlists are posted and shared.

Privacy at the State Level

As privacy concerns continue to grow, states continue to enact and amend their various privacy and data security laws. As of the date of this publication, forty-seven states have enacted security breach notification laws, which typically require businesses to notify consumers about any security breaches involving personal information. For example, a September 2012 amendment to Texas's breach notification law requires businesses to provide breach notification to residents of all states, including the three states that have not enacted their own breach notification laws (i.e., Alabama, New Mexico, and South Dakota).[17]

Some states mandate certain security standards with respect to personal information. Under California law, any company that maintains personal information about a California resident must use reasonable security procedures.[18] Similarly, a recently passed Florida statute requires "reasonable measures to protect and secure" personal information.[19] Nevada mandates compliance with PCI DSS by law.[20] Massachusetts law, Mass. 201 CMR 17, is one of the most prescriptive, setting minimum security standards for certain types of sensitive information, including designation of an individual responsible for security, development of security program rules, imposition of penalties for violations of those rules, and contractual agreements with third parties to ensure similar security procedures.[21] Many states also have provisions concerning appropriate data disposal or destruction, and some states have laws relating to identity theft. Some states also have laws relating specifically to the treatment of social security numbers with which employers must ensure compliance.[22]

States have also taken a special interest in social media. Several states are developing laws and regulations specifically related to social media accounts, including legislation prohibiting employers from requesting or requiring current/prospective employees to disclose social media user name or passwords.

A few words of caution about state law: Some state laws are more prescriptive than others.[23] And the choice of law will often be determined by where the customer is located, not where the company is located.

Privacy Self-Regulation

Self-regulation also plays an important role in certain industries. One significant example is the PCI Data Security Standard (PCI DSS), which is an enforceable standard that includes 12 requirements for any business that stores, processes or transmits payment cardholder data.[24] It includes a comprehensive framework of specifications, tools and measurements that focus on preventing, detecting and reacting appropriately to security incidents involving payment cards and personal information. There are various levels of PCI DSS compliance, but it is a serious commitment at any level, and businesses that are not in a position to undertake such a commitment are well-advised to outsource this function to a company that specializes in doing so.

For marketing companies, another important source of self-regulation is provided by the Network Advertising Initiative (NAI), an association of digital advertising companies that maintains and enforces voluntary standards for data collection and use in online and mobile advertising.[25] The NAI has developed codes of conduct and guidance that apply to data collection and use generally, as well as in specific areas such as the mobile application environment and in connection with specific technologies, such as non-cookie technologies. The Digital Advertising Alliance (DAA), a consortium of media and marketing associations that includes the NAI, also establishes and enforces voluntary data collection and use principles across industries.[26]

TODAY'S BIGGEST PRIVACY RISKS

Given the number of cooks in the U.S. privacy-legislation kitchen and the fact that privacy law is constantly evolving - keeping up-to-date and in compliance with all applicable privacy laws can be a challenge. However, there are certain key risks and principles that cross the various industries and state lines. These are discussed below.

1. RISKS ASSOCIATED WITH UNDISCLOSED COLLECTION AND USE OF INFORMATION

When it comes to privacy, the most important rule for U.S. companies is complete and accurate disclosure. Many information collection and use practices may pass muster so long as they are accurately and adequately disclosed to consumers. California, for example, requires operators of commercial websites or online services that collect personally identifiable information through the Internet about individual California consumers who use or visit its site or services to conspicuously post on their website or make their privacy sufficiently available, and describes a number of disclosures that such a policy must contain.[27] Its Attorney General has specified that this requirement applies to providers of mobile applications as well.[28] Included within the information that must be provided are disclosures about how companies are handling "personally identifiable information."

The fact that "personally identifiable information" doesn't have a single, accepted definition complicates such disclosures. For example, the Children's Online Privacy Protection Act ("COPPA") Rule has a fairly broad definition of "personal information" that includes any "persistent identifier that can be used to recognize a user over time and across different Web sites or online services. Such persistent identifier includes, but is not limited to, a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier."[29] This is a change from the original COPPA rule, which only covered persistent identifiers when they were combined with individually identifiable information.[30] This trend seems to acknowledge that it can be possible to target an individual without his/her name, a concept that is rejected in some other definitions. What is clear is that the definition is constantly evolving, necessitating ongoing attention to ensure that disclosures and practices are aligned.

Companies should also give special consideration to tracking mechanisms and behavioral advertising. "Cookies" are small text files sent by a website's server and stored on a computer's Internet browser. Cookies can transmit information about the user's web surfing activities. Cookie practices should be clearly and accurately explained - in the EU there are special regulations concerning cookies.[31] In addition to cookies, companies use a number of ever-changing online tracking tools, including web beacons or web bugs, and best practices dictate the disclosure of all online tracking - even where the law has not explicitly caught up with the technology.[32]

TAKE AWAY: When it comes to collecting and using information, companies should be transparent about their practices; they should disclose all manners of data collection and tracking, even where the law has not yet caught up with the technology.

2. RISKS ASSOCIATED WITH HAVING PRACTICES THAT ARE INCONSISTENT WITH DISCLOSED POLICIES

Honesty is the best policy. Seems simple enough, right? But in practice it's an area where

companies often find themselves in trouble. Misrepresentations about privacy or data security practices could subject a company to charges of unfair and deceptive practices under section 5 of the FTC Act, as well as actions by state regulators and private class action litigants. For example, in 2014, the FTC brought an enforcement action against TRUSTe, Inc. for failure to act consistently with its own policies.[33] The FTC alleged that TRUSTe, a major provider of privacy certifications for websites, had represented that it recertified its website's privacy certifications on an annual basis, but had failed to do so for more than 1,000 websites.[34] TRUSTe settled these claims with the FTC and agreed, among other things, to pay $200,000 and to refrain from making false statements about its certification process and timeline.[35]

And it is critically important for companies to follow-through on representations made in their own policies. In November 2012, a federal judge approved a $22.5 million fine against Google as part of a settlement that Google reached with the FTC regarding charges that Google misrepresented to users of Apple Inc.'s Safari Internet browser that it would not place tracking cookies or serve targeted ads to those users in violation of a settlement between Google and the FTC.[36] The penalties for failing to comply with your own privacy policy can be harsh, so companies should consider internal policies that require the creation and maintenance of a list of all user tracking tools, and should not implement additional tracking tools without both IT and legal review.

TAKE AWAY: Companies should keep their privacy policies update-to-date and keep consumers informed of any changes. Companies should periodically evaluate what they do and how it does or doesn't match with the representations that they've made.

3. RISKS ASSOCIATED WITH NOT PROVIDING CHOICE OR RESPECTING USER CHOICES ONLINE

Is your inbox full of emails for sales and deals? As online marketing continues to grow, companies have moved away from traditional direct marketing and have dedicated more of their resources to online advertising and marketing via email and other electronic communications. While this form of marketing has many benefits for companies and for customers, companies that engage in online marketing must be aware that they are subject to specific laws and regulations. For example, if the business engages in email marketing, messages should include opt-out options as required by the CAN-SPAM Act.[37] A company's website should provide customers with the ability to change or discontinue email notification.[38] Additionally, the Telephone Consumer Protection Act ("TCPA") requires companies to receive consent prior to sending text messages to consumers.[39]

Many statutes have provisions related to respecting user choices. For example, the GLBA requires financial institutions to explain to customers that they have a right to opt out of having certain information shared with third parties, and to comply with users' choices with respect to this right.[40] In some instances, companies are not required to comply with users' choices, but they are required to disclose their failure to do so. The California Online Privacy Protection Act ("CalOPPA") requires businesses to disclose in their privacy policies how they respond to online users' Do Not Track signals.[41] Under this law, businesses are not required to comply with a user's Do Not Track signal, but they are required to provide users with transparency as to the practices in this regard.[42]

Also - a word of caution: We've seen a number of companies that put terms in their privacy policies saying that they can unilaterally change their policies at any time without notice. Courts, unsurprisingly, take a dim view of such provisions. Privacy policies would be meaningless if a company could collect personal information with guarantees of confidentiality and then change its policy the next day and disclose that information to the world. Companies can and should update their policies, but information collected prior to a change likely needs to be treated according to the previous policy unless and until there is some form of implied or explicit consent. If there is a material change in the way that information will be handled, consumers should be provided notice and an opportunity to opt-out. Thus, instead of stating in a privacy policy that it has a unilateral right to change its practices without any notice, a company may find itself better protected if it informs consumers that it may change its policies from time-to-time and provides information on how consumers will be notified of such changes.

TAKE AWAY: Give users choices when you should, and respect users' choices. Tell them when you are changing course.

4. FAILURE TO CONSIDER ISSUES RELATED TO TRANSFERS OF INFORMATION BETWEEN ENTITIES OR ACROSS BORDERS

Where is the information going? Where could it go in the future? Smart businesspeople should be asking these questions from the get-go. Because privacy law generally requires notice and consent prior to sharing of personal information, companies that don't obtain consent for certain future uses of data may find themselves limited in what they can do with data that they've already collected - or find that they need to go back to users in order to request additional permission. This can be a painful exercise, particularly in the context of a merger or acquisition.

Does that mean you should draft a privacy policy that disclaims every single potential future use you can think of? Not necessarily. There's a balance between disclosing your current practices and protecting yourself for the future and there are risks associated with drafting a privacy policy that discloses practices that go far beyond what a company actually does or may do. Users could be unwilling to share information with companies that they think do too much with their personal data, or the company could draw unwanted attention from regulators or the media based on disclosures of broad sharing practices that bear no relation to what the company actually does. But at an absolute minimum, companies should have a provision that would allow for the transfer of personal information in the event of a merger, asset sale, acquisition or bankruptcy.

Companies should also consider transfers of data across international borders. Companies interested in transferring data internationally (a likely possibility given the increasingly interconnected nature of businesses), should be sure to evaluate these issues and seek legal counsel especially in today's environment where the EU/US safe harbor has recently been invalidated under the Schrems v. Data Protection Commissioner decision.

TAKEAWAY: From the beginning, companies should plan for data transfers - whether between companies or cross borders.

5. FAILURE TO PROVIDE FOR A DATA SALE IN THE EVENT OF A BANKRUPTCY

As the old saying goes, when it comes to customer data, companies are wise to hope for the best and plan for the worst. Sadly, companies occasionally face the worst and must file for bankruptcy.

Dealing with customer data in a bankruptcy presents a unique set of challenges that are best addressed by planning ahead. In a bankruptcy situation, companies without comprehensive privacy policies have run into trouble when trying to sell off customer data in an asset sale.

In 2000, Toysmart, an online toy company, filed for bankruptcy and attempted to sell its customer data as part of its asset sale.[43] Unfortunately, Toysmart's privacy policy stated that it would "never" sell customer data to third parties.[44] As a result, the FTC objected to the sale on the grounds that Toysmart's sale of customer data constituted a deceptive trade practice under Section 5 of the FTC Act.[45] A proposed settlement between Toysmart and the FTC imposed certain conditions on the sale: (i) Toysmart was prohibited from selling the customer data as a standalone asset; (ii) the customer data could only go to a "qualified buyer"—a company in a substantially similar business; (iii) the buyer was required to abide by Toysmart's privacy policy; and (iv) the buyer was required to get affirmative consent from consumers prior to any material changes to its privacy policy regarding the use of customer information.[46] Even though the court rejected this proposed settlement and these issues became moot when the buyer paid Toysmart to destroy the data rather than selling it, Toysmart has served as important precedent for any company filing for bankruptcy and contemplating the sale of customer data.[47]

Following Toysmart's bankruptcy, The Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 ("BAPCPA") was introduced to address the consumer data issues highlighted in that case. Under the BAPCPA, if the sale of customer data is inconsistent with the debtor company's privacy policy, the bankruptcy court may appoint a consumer privacy ombudsman to assist the court by providing recommendations regarding the sale of that data.[48]

TAKEAWAY: To avoid the potential loss of a valuable asset at a crucial time, companies should draft comprehensive privacy policies, which include a provision contemplating the sale of customer data in the event of a change in business circumstances, such as a bankruptcy or asset purchase.

6. RISKS FROM FAILING TO USE ADEQUATE SECURITY MEASURES TO PROTECT INFORMATION

Consumers' personal information is a valuable asset - and companies should treat it that way. They must have adequate protections in place for the personal information and other sensitive data that they collect and maintain; companies cannot simply place disclosures in their privacy policies disclaiming any obligations. In general, it is advisable for companies to minimize the data that they collect and maintain. This will help to minimize the amount of harm caused if a breach occurs. However, certain data collection is unavoidable. Even companies that do not collect consumer data have a duty to protect sensitive employee data.

Depending on the industry, businesses may be required to follow particular data security requirements of various regulatory authorities, including the FTC and the U.S. Department of Health and Human Services. Various states also have specific requirements for securing, storing and disposing of sensitive data. Failure to comply with the required security standards can result in liability. In 2014, the Massachusetts attorney general announced a consent judgment with Rhode Island Hospital, resolving a lawsuit for violations of federal and state laws, including 201 CMR 17 and federal regulations under HIPAA, in connection with a 2011 data breach.[49] The agreement "requires the Hospital to pay $150,000 to the Commonwealth of Massachusetts and

to take steps to ensure compliance with state and federal security laws…," including hiring an outside firm to perform audits and maintain an updated inventory of all unencrypted electronic media and patient charts containing personal information.[50]

But the buck doesn't stop there. Companies should also ensure that their vendors and service providers protect any sensitive or confidential data that they access. Massachusetts law, for example, requires companies to take reasonable steps to select and retain third-party service providers that are capable of providing security measures that comply with applicable laws or regulations and expects companies to include contractual provisions that require those service providers to implement and maintain appropriate security measures for the handling of personal information. Best practices in this arena include regular audits of vendors, but the bare minimum is contractual provisions requiring that service providers maintain adequate security measures.

TAKEAWAY: Companies should make sure that they have a system in place for ensuring that information is adequately protected and that data security issues are considered when making significant changes. Be vigilant in updating your practices to conform to the law.

7. FAILURE TO ADEQUATELY NOTIFY FOLLOWING A BREACH

When a company experiences a data breach, things can go from bad to worse if the company does not notify affected individuals about the breach in a timely manner. Depending on the company, the severity of the breach, and the circumstances surrounding it, state and federal law may require the company to disclose the breach by notifying affected individuals as well as state and regulatory authorities. Reporting requirements can vary depending on the jurisdiction and industry, thus making compliance challenging. Although numerous proposals for a unitary federal notification system have been introduced in Congress, to date, these initiatives have not been successful.

While no two state breach notification laws are the same, these laws often relate to data breaches involving unencrypted data and specify when, how, and who to notify in the event of a data breach.[51] For example, New York's data breach notification law requires any person or business which conducts business in New York to notify affected New York residents, the state attorney general, and the state police whenever a breach occurs.[52] The law further requires notification to consumer reporting agencies when there is a data breach of certain unencrypted personal information involving 5,000 or more New York State residents. California law similarly requires notification in the event of a data breach involving certain unencrypted information, but unlike New York law, notification to the state attorney general is only required when 500 or more California residents are affected by a single breach, and notification to consumer reporting agencies is never required.[53] Given the variations in state law with respect to notification, it is important for companies to remember that their notification obligations are dictated by where the affected consumers are located, not where the company is located.

Failure to comply with state breach notification laws may lead to enforcement actions. For example, in 2014 the Office of the Attorney General in California brought an enforcement action against Kaiser Foundation Health Plan, Inc. for delaying in notifying its employees of a breach involving 20,000 employee records after an unencrypted portable memory device containing employee records turned up in a thrift shop.[54] Ultimately, Kaiser settled with the state

attorney general and agreed to pay $150,000 in penalties and attorneys' fees, and to provide its employees with additional training regarding the treatment of sensitive data.[55]

Certain federal statutes also provide federal breach notification requirements. For example, both the Gramm-Leach-Bliley Act ("GLBA"), which applies to "financial institutions," and the Health Insurance Portability and Accountability Act ("HIPAA"), which applies to health care providers, health care plans, and health care clearinghouses, have specific provisions regarding data breach notification.

TAKEAWAY: Be aware of the various breach notification laws that apply to your company. Notification should be part of your incident response plan.

8. COLLECTING INFORMATION FROM CHILDREN UNDER 13

It's 10 p.m. Do you know where your children are? Does their mobile app provider? Children's privacy is another issue that deserves companies' attention. COPPA required the FTC to promulgate and enforce rules related to children's online privacy. The original COPPA Rule became effective in 2000 and was updated through a series of amendments in 2013. These regulations apply to operators of commercial websites and online services (including mobile apps) directed to children under 13 that collect, use, or disclose personal information from children and operators with actual knowledge that they are collecting or maintain personal information from a child under 13. The COPPA Rule contains a number of requirements, including a bar on collecting children's information without first obtaining verifiable parental consent.

The FTC has been active in enforcing the COPPA Rule and has recently shown an interest in bringing charges against companies related to handling their mobile apps. In 2014, the FTC settled charges with Yelp and TinyCo, which included, among other things, requiring the companies to pay $450,000 and $300,000 in civil penalties, respectively.[56] The FTC alleged that Yelp collected information from registrations despite possessing information that indicated that the individuals were under 13. It accused Yelp of failing to use an age-screen with its apps, even though the company had an age-screen mechanism on its website.[57] With TinyCo, the FTC asserted that the company's apps' themes, animated characters and language targeted children and thus fell without the ambit of the COPPA Rule.[58]

TAKEAWAY: Be aware of the special requirements that surround the collection of children's information and take care to comply with them.

ENDNOTES

[1] The author thanks Randi Singer, a partner and co-leader of Weil Gotshal & Manges LLP's Cybersecurity, Privacy and Information Management Group, for contributing this chapter of the book.

[2] 16 C.F.R. 312.2.

[3] 15 U.S. Code § 45 - Unfair methods of competition unlawful; prevention by Commission, available at: https://www.law.cornell.edu/uscode/text/15/45.

[4] See FTC Policy Statement on Deception, available at: https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.

[5] See FTC Policy Statement on Unfairness, available at: https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.

[6] See FTC Privacy & Data Security Update (2014), available at: https://www.ftc.gov/reports/privacy-data-security-update-2014.

[7] "FTC Approves Final Order Settling Charges Against Snapchat," https://www.ftc.gov/news-events/press-releases/2014/12/ftc-approves-final-order-settling-charges-against-snapchat (Dec. 31, 2014).

[8] In the Matter of Snapchat, Inc., Agreement Containing Consent Order, available at: https://www.ftc.gov/system/files/documents/cases/140508snapchatorder.pdf.

[9] This report is available at: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[10] See "FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks", available at https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices.

[11] Draft available at: https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

[12] Consumer Privacy Bill of Rights Falls Short, Groups Say, Law 360 (Mar. 4, 2015), available at: http://www.law360.com/articles/627415/consumer-privacy-bill-of-rights-falls-short-groups-say.

[13] Administration Discussion Draft: Consumer Privacy Bill Of Rights Act, available at: https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

[14] See 15 U.S.C. §§6801-6809.

[15] Available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf.

[16] Available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html.

[17] See "Texas Doubles Down On Tough Breach Law", available at: http://www.informationweek.com/regulations/texas-doubles-down-on-tough-breach-law/d/d-id/1111072.

[18] See, e.g., California Civil Code Section 1798.85, available at http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.81.5. ("A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures").

[19] See Fla. Stat. § 501.171, available at: https://casetext.com/statute/fla-stat-501171-security-of-confidential-personal-information.

[20] Nev. Rev. Stat. § 603A.215(1) ("If a data collector doing business in this State accepts a payment card in connection with a sale of goods or services, the data collector shall comply with the current version of the Payment Card Industry (PCI) Data Security Standard, as adopted by the PCI Security Standards Council or its successor organization, with respect to those transactions, not later than the date for compliance set forth in the Payment Card Industry (PCI) Data Security Standard or by the PCI Security Standards Council or its successor organization").

[21] Mass. 201 CMR 17, available at http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf.

[22] See, e.g., N.Y. Gen. Bus. L. § 399-ddd.

[23] California, Massachusetts and Nevada have a number of very specific laws not common to every state.

[24] See PCI SSC Data Security Standards Overview, available at: https://www.pcisecuritystandards.org/security_standards/index.php.

[25] See About The NAI, available at: https://www.networkadvertising.org/about-nai/about-nai.

[26] http://www.aboutads.info/

[27] Cal. Bus. & Prof. Code § 22575(a).

[28] Privacy on the Go: Recommendations for the Mobile Ecosystem (January 2013), available at http://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf.

[29] 16 C.F.R. 312.2.

[30] "Comply with COPPA: Frequently Asked Questions, FTC," available at https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions.

[31] "Cookies" The EU Internet Handbook, European Commission, available at http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm.

[32] "Web Beacons - Guidelines for Notice and Choice", Network Advertising Initiative, available at: http://www.networkadvertising.org/pdfs/Web_Beacons_11-1-04.pdf.

[33] See "TRUSTe Settles FTC Charges it Deceived Consumers Through Its Privacy Seal Program", available at: https://www.ftc.gov/news-events/press-releases/2014/11/truste-settles-ftc-charges-it-deceived-consumers-through-its.

[34] Id.

[35] Id.

[36] See Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser, available at: https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented.

[37] See "CAN-SPAM Act: A Compliance Guide for Business," available at https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business.

[38] Id.

[39] See FCC Consumer Help Center: Spam: Unwanted Text Messages and Email, available at https://consumercomplaints.fcc.gov/hc/en-us/articles/204930920.

[40] See "How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act", available at: https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm.

[41] State of Cal. Dept. of Justice, Office of the Att'y Gen, Making Your Privacy Practices Public: Recommendations on Developing a Meaningful Privacy Policy (May 2014), available at https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf.

[42] Id.

[43] See "FTC Sues Failed Website, Toysmart.com, for Deceptively Offering for Sale Personal Information of Website Visitors," available at https://www.ftc.gov/news-events/press-releases/2000/07/ftc-sues-failed-website-toysmartcom-deceptively-offering-sale.

[44] Id.

[45] See FTC v. Toysmart, LLC, et. al, First Amended Complaint for Permanent Injunction and Other Equitable Relief, found at https://www.ftc.gov/sites/default/files/documents/cases/toysmartcomplaint.htm.

[46] Id; see also "FTC Announces Settlement With Bankrupt Website, Toysmart.com, Regarding Alleged Privacy Policy Violations," available at https://www.ftc.gov/news-events/press-releases/2000/07/ftc-announces-settlement-bankrupt-website-toysmartcom-regarding.

[47] See "Toysmart to Destroy Data, Be Paid," available at http://articles.latimes.com/2001/jan/10/business/fi-10470.

[48] See Bankruptcy Abuse Prevention and Consumer Protection Act of 2005 (Pub.L. 109-8, 119 Stat. 23, enacted April 20, 2005), available at http://www.gpo.gov/fdsys/pkg/BILLS-109s256enr/pdf/BILLS-109s256enr.pdf; see also 11 U.S.C. § 363 Use, sale, or lease of property, available at https://www.law.cornell.edu/uscode/text/11/363.

[49] Erin Staab, Massachusetts Enforces Data Security Regulations Against Out-of-State Entity, Privacy Law Blog (Aug. 13, 2014) http://privacylaw.proskauer.com/2014/08/articles/data-privacy-laws/massachusetts-enforces-privacy-regulations-against-out-of-state-entity/.

[50] Id.

[51] See N.Y. GBS. LAW § 899-aa, Notification; person without valid authorization has acquired private information, available at http://codes.lp.findlaw.com/nycode/GBS/39-F/899-aa.

[52] Id.

[53] See California Civil Code s. 1798.29, available at http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.29; see also California Civ. Code s. 1798.82, available at http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.82.

[54] See Privacy Enforcement Actions, available at https://oag.ca.gov/privacy/privacy-enforcement-actions.

[55] Id.

[56] See "Yelp, TinyCo Settle FTC Charges Their Apps Improperly Collected Children's Personal Information," available at https://www.ftc.gov/news-events/press-releases/2014/09/yelp-tinyco-settle-ftc-charges-their-apps-improperly-collected.

[57] Id.

[58] Id.

CHAPTER 11 :

WHAT DIRECTORS REALLY NEED TO KNOW ABOUT CYBER INSURANCE

There has been no shortage of data breaches occurring on a daily basis in recent months. The age of nation-state hacks, cyber hactivisim, cyber extortion and cyber terrorism is here, and it's not going to go away any time soon.

Dealing with data security issues is no longer just an IT Department concern. It has become a matter of corporate survival and should be incorporated into enterprise risk management and insurance risk transfer mechanisms, just as other hazards of doing business are regularly insured for (like fire insurance coverage or hurricane coverage). With the increasing number of data breaches, cyber insurance has dramatically increased in demand like no other insurance product in recent years. Every Board of Directors should be questioning their officers and management "whether or not their Company should be purchasing cyber insurance to mitigate its cyber risk." If the answer from their management is, "oh, it costs too much, or oh, it will never pay off," second opinions should be obtained. Because neither answer is correct.

For some Boards of Directors and their respective companies, purchasing a comprehensive stand-alone cyber insurance policy that covers both first party and third party costs helps ensure survival of the fittest when security fails and large expenditures must be made rapidly to get the company "back on line." For other more sophisticated companies, cyber insurance may be seen as a way to transfer potential balance sheet risk to an insurance mechanism to protect the company and its shareholders from large, uninsured losses (no different than it would purchase catastrophic property-casualty insurance to protect against natural disasters). Post-Enron and Worldcom, no publicly traded US company would ever forego directors and officers insurance coverage to protect against the securities law exposures of the Company and its officers. Today, no company in the US should forego buying cyber insurance to protect against the real, ever-present risk of a major cyber attack.

Today, it is no longer a matter of "if" data breaches can have a real impact on a Company's bottom line and business performance; it's a question of "when?"

As data breaches accumulate, there are significant costs from forensic investigations, lawsuits, data breach notification expenses, regulatory investigations, regulatory fines attorneys and consultants, PR professionals, and remedial measures. In the blink of an eye, these costs can range from $5 million to $50 million dollars in the few weeks after a reported cyber breach.[1] According to the 2015, Ponemon Cost of Data Breach Report the average cost of responding to a data breach increased 23% in 2014. The cost of responding to a data breach in the United States increased to an estimated $217 per record. Besides these costs, a Company is exposed to intangible factors, such as brand reputation and damage, loss of productivity and the impact on business performance (such as loss of store "foot traffic" because consumers are simply afraid of shopping in their stores anymore); -and-other liabilities, such as Board member liability, shareholder lawsuits for cybersecurity failures and falls in a company's stock price. Further, recent weeks and months have shown us that the plaintiffs' bar seems undeterred from the past in filing new customer driven lawsuits against companies alleging that they failed to adhere to cybersecurity "best practices."[2]

If your Company experienced a data breach today, would your Board be ready?

When a data breach occurs, Directors and C-level executives must be ready with a business continuity and data breach incident response plan to help minimize their Company's liability, exposure and business performance. Here are some questions Directors and C-level executives should be asking and be prepared to answer before a data breach and before the purchase of cyber insurance, as they are fundamental to both good cyber governance and an effective purchase of cyber insurance:

1. What are the Company's most critical intellectual property assets and consumer/customer based informational assets and how are they currently being protected?
2. Where are these assets stored or located? Internally, at a third-party data center (in the US or overseas), or in a cloud-based environment? If the Company's most critical assets are not intellectual property or customer related information, but are instead hard "infrastructure" assets like computer controlled mechanical devices, turbines or pipelines, how are these assets being protected from a cyber attack?
3. What are the Company's practices with respect to diligencing the cybersecurity practices of third-party vendors and suppliers that may have access to the Company's servers?
4. Has the Company formally adopted a cyber-security standard or practice like the NIST Cyber Framework, or ISO 27001, and what mechanism does the Company have to document discussions concerning compliance with those standards? Similarly if the insured is a regulated entity, there could be other guidance applicable to their operations, such as that issued by the SEC's Office of Compliance, Inspections and Examinations, FINRA or the FFEIC (if the insured is a banking institution).
5. What can go wrong and what could be the gross financial impact of a "significant" data breach?
6. Does the Company have a Chief Information Security Officer? How often does he or she give presentations to the Board of Directors?

7. Does the Company have a "battle - tested" incident response plan that involves all facets of the company (including the board of directors) which includes a communication strategy with customers, investors, and law enforcement?

8. Does the Company have an employee training and awareness problem which focuses on spearphishing and other issues like malvertising and ransomware?

9. How -and- will the Company's current insurance policies respond to the present cybersecurity threat environment when and wherever are hacked?

10. How much cyber insurance can our Company purchase?

Reputational Loss after a Data Breach

Besides data, reputation is the most important asset a company possesses, and also one of the most difficult to protect. According to an Economist Intelligence Unit Report, "Reputation Risk: Risk of Risks"[3] of which 36% of the report's survey respondents are companies in the financial services sector, companies struggle to categorize and quantify reputational risk. Especially after a data breach happens, given the fact that there is no formal ownership of reputational risk, responsibility is spread amongst a wide range of business managers. Nonetheless, companies worry about what could happen to their reputation in the event a data breach happens, and they are deemed by customers, and regulators for failing to live up to minimum standards of service and data protection quality protection measures to customers.[4] While a Company may not be able to precisely quantify reputational risk, Board Directors are advised to prioritize the various threats against their companies' reputations. According to the Economist Intelligence Unit Report, understanding how different aspects of an organization's activities impinge on stakeholder perceptions is therefore a vital aspect of protecting a company's reputation. Furthermore, the report states that there are three distinct tasks to managing reputational risk: establishing reputation to begin with, maintaining it through the rough and tumble of business operations, and restoring it when it has been damaged.

Coordinating and creating a "reputational risk" team should be part of every Company's data breach incident response team. Incurring reputational damage can be fatal, and having a reputational risk team, with the CEO at the team pilot helps to ensure the company's good standing and minimizes reputation damage after a data breach. Once a data breach happens, the reputational risk team must already have a response plan in place to maintain control of their Company's reputation. The reputational risk team, along with the CEO bears the responsibility of acknowledging their Company's concern and commitment whilst showing that the Company is in control of the situation and are working with any relevant authorities to ensure it won't happen again.

While a Company may not be able to insure their reputation with a specific coverage limit, stand-alone cybersecurity insurance can help guard and minimizes reputational damage by offering a "crisis management" communications team that helps assist a company after a crisis happens. The communications team can help compliment your company's reputational risk team and provides a panel of experts who can help advise and assist the Company in developing a communications strategy and manage the response to a potentially damaging crisis.[5]

Incorporating Cyber Insurance Into Your Data Breach Incident Response Plan -Today

Many Directors today have openly shared that they feel unprepared, lack technical skills and do not understand cyber risk. Fortunately, many Directors have transitioned their thinking and have realized that cyber risk, formerly seen as the IT Director's problem is now also their problem, responsibility and fiduciary duty to oversee. Today, when a data breach happens, Boards and Companies are immediately publicly scrutinized. This is why it is best for Directors and Companies to be proactive today, and explore how cyber insurance can help manage cyber risk exposures rather than leave the cybersecurity gap unfunded when security fails. Purchasing appropriate amounts of cyber insurance can play a significant role in protecting your Company's bottom line, rather than cost you millions of balance sheet dollars you could have insured for with insurance dollars.

Evaluating Cyber Insurance Policies

Once you are ready to explore the purchase of cyber insurance it is important to carefully evaluate the plethora of cyber insurance policy options from a variety of angles. The types of coverage offered by cyber insurance policies vary dramatically by insurance carrier, so it is good to start by talking with a knowledgeable insurance broker who has experience with cyber insurance policies.

When evaluating and considering the purchase of a cyber insurance policy, there are several important things to consider prior to investing in a policy:

- Determine how much insurance you need and how much risk you can afford to retain. Once the amount of insurance you need is determined, figure out how much you can afford to pay out of pocket before any cyber insurance claims may be paid. This will help you determine your self -insured retention or deductible;
- Review the types of coverage provided. While cyber insurance policies are not standard policies, and vary widely, coverage typically falls into five categories: third party liability coverage, breach response and remediation costs, business interruption costs, and fines and penalties. An experienced and knowledgeable cyber insurance broker or insurance coverage attorney can help you evaluate your coverage options and determine which coverages your company should have to cover the range of damages, costs and expenses;
- If you are a retailer, understand what coverage the policy provides in case of a data breach if the retailer faces claims for damages under provisions of PCI-DSS 3.1;
- Know what triggers the policy. Will your cyber insurance coverage be triggered for a stolen or lost unencrypted laptop or USB flash drive? Loss related to the failure to secure data? Loss related to a breach caused by a negligent employee? Data held in the cloud, but lost or stolen due to a data breach?;
- What is excluded in the policy? It is crucial to learn what is excluded in the cyber insurance policy your Company is considering as the purpose of purchasing coverage is to cover your risks, and not exclude them. Are acts of cyber-terrorism or cyber-extortion covered under the words of the policy? What happens to coverage if it is determined that the data breach in question was an act of war against the United States by another country? Will you stand-alone cybersecurity insurance policy still kick in?;

- What types of data are covered? Some carriers specify the types of data covered, while others do not. Some things to consider: How is sensitive data defined in the specific cyber policy? Are paper records included (e.g. patient records left in a dumpster or on the side of the road for the garbage disposal company that "somehow" end up stolen)? Finally, make sure that if you store your information with a third-party cloud services provider, and that provider is breached, your stand-alone cyber insurance policy would provide coverage for Claims arising out of the breach;
- What response costs and services are covered in the event of a breach? Most carriers offer coverage for breach response costs and breach services. You will want to check to see if the following are covered (at least) in the cyber insurance policy and offer: crisis management and breach notifications, credit monitoring, loss of business income, privacy regulatory defense and penalties, computer forensics investigation, and the hiring of a privacy attorney. Breach notification costs are especially important because they may not only just apply in the United States, but they could apply outside the United States as well depending upon where your operations are located;
- Find out if you can select your own vendors or counsel. Often, companies prefer to select their own vendor or counsel, especially if they have a pre-existing relationship with these professionals. For smaller insured who may not have had a breach incident before, find out if your carrier will help select a vendor for you. Many of the leading carriers handle breaches everyday, and their mission-critical advice could be exactly what your organization needs if it is unsure how to proceed.

THE IMMEDIATE ADVANTAGES OF CYBER INSURANCE

Stand-alone cyber insurance offers Companies an immediate solution to transfer the associated first and third-party costs of a data breach, and offers the crisis management expertise and assistance that is crucial when responding to a data breach.

Immediate advantages of cyber insurance coverages include:

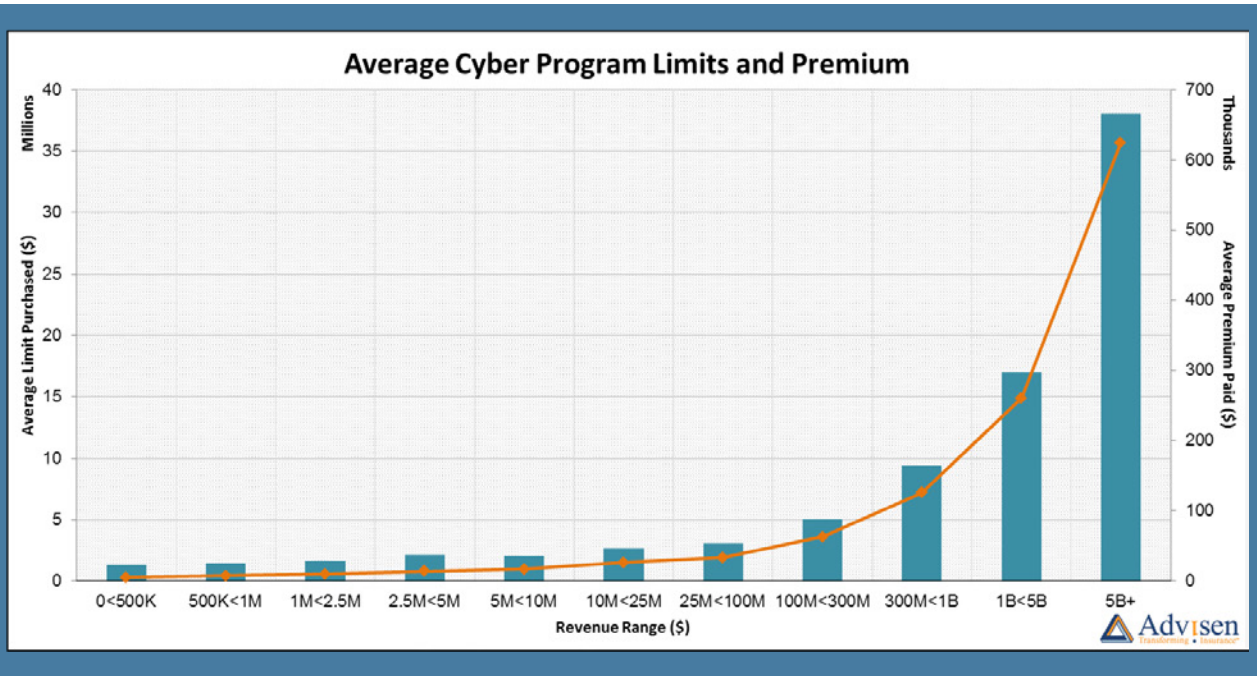
(Please note: the below mentioned cyber insurance coverages will vary depending on the specific policies and endorsements selected):

- **CUSTOMER NOTIFICATION EXPENSES:** Provides coverage for the expenses associated with notifying the affected individuals and depending on the policy selected there could also be coverage to set up a call center to handle calls from the notified individuals. Today, customers are very sensitive to how a Company notifies them when their sensitive data has been put at harm. This is a crucial part of the data breach incident response as customers, as well as regulators will be lining up with questions about the extent of the breach and the steps that are being taken to minimize the damage that has already been done.
- **CREDIT/IDENTITY THEFT MONITORING:** Provides coverage for expenses incurred to monitor the credit of an affected individual for at least 1 year (which is a requirement under many states' laws). When a data breach happens, customers are more susceptible to identity and/or medical fraud. By having a standalone cyber insurance policy that offers customers a 1-year credit/identity

theft monitoring program this should help decrease this potential damage exposure. Given these state law requirements, such credit monitoring should be a mandatory part of any cyber insurance program.

- **PRIVACY AND SECURITY LIABILITY:** Provides coverage for the Company's liability arising from a security breach. As we noted above, It's not unusual today for a Company to find themselves on the defendant side of a lawsuit the day after the breach is announced. Some general categories of liability coverage may include:
    - Negligence by the Company, for failure to follow "best practices" in cyber protection
    - A violation of a privacy or consumer data protection law,
    - Breach of contract (I.e., merchant service agreements relating to PCI-DSS),
    - Regulatory Investigations arising from a breach.
- **BUSINESS INTERRUPTION:** (depending on the policy selected) Offers coverage for the Company's loss of income incurred as the direct result of a cyber peril or a cloud computing provider's systems failure or impairment due to a cyber peril first discovered during the period of the policy.
- **CYBER EXTORTION:** Offers the Company coverage if a hacker demands ransom as a condition of not carrying out a cyber threat. With all of the sophisticated malware attacks as of late, this coverage is becoming a valuable component. Some examples of extortion threats may include:
    - threatening a hacking attack or virus into your computer systems; or
    - threatening to disseminate, divulge or utilize information contained or once contained in your computer systems; or,
    - threatening to damage, destroy or alter your computer systems.
- **HACKER DAMAGE COSTS:** Offers the Company help with the costs incurred to replace or repair the damaged website, intranet, network, computer system, programs, or data.
- **PRIVACY REGULATORY DEFENSE AND PENALTIES:** Offers help with regulatory defense costs and depending upon the policy and where insurable by state law, there could be coverage for civil penalties, and any related expenses arising from regulatory proceedings not related to compensatory awards.
- **COMPUTER FORENSICS INVESTIGATION:** When a data breach happens, one of the first parties that must be called in is a forensics investigator to determine the extent of the breach, the cause and what types of data were stolen.
- **DATA BREACH COACH (AKA "PRIVACY" ATTORNEY:** Offers the Company help with navigating the various state (and, if applicable, international) privacy laws and determining who needs to notified and when a breach needs to be reported, and also helps with drafting the breach communication documents and notification letters.

HOW MUCH CYBER INSURANCE COVERAGE SHOULD COMPANIES BUY?



We believe the answer to that question for Boards and Companies should be "as much as possible." Once your Company has identified its cyber risks, and is ready to buy a cyber insurance policy, determining how much insurance coverage to buy must be carefully considered. Using industry benchmark data from Companies in your Industry or Sector that may have experienced a data breach or from sources such as the Ponemon Research Institute can help determine the appropriate amount of coverage your Company should purchase.

According to a 2013 Ponemon Study, "Managing Cybersecurity as a Business Risk: Cyber Insurance in the Digital Age", when asked to predict their company's maximum financial exposure of security exploits and data breaches for the next 24 months, the average estimate was approximately $163 million.

Unless your Board and Company has experienced a data breach, most companies lack or have limited data on how the financial impact of a security exploit and data breach would affect them. What makes Boards and Companies especially vulnerable is that the costs and chances of a data breach occurrence are unknown as there is no normal distribution of outcomes on which to base the probabilities of future effects. Cyber attacks come without warning, and Directors must do more to anticipate them and prepare for them. This is why we feel Companies must prepare and buy cyber insurance now, and purchase as much cyber insurance coverage as can be obtained.

INSURING YOUR BOARD AND COMPANY'S CYBER RISK

Cyber insurance is not a "one size fits all" policy as no two Companies are the same nor should their cyber insurance policies be. Further, no two Insurers are the same in responding to cyber-related claims. To help your Board and Company determine your applicable cyber risk exposures and the possible insurance coverages needed, below is a checklist of first and third-party risk exposures that can (depending upon the carrier and cyber insurance policy purchased) be covered through cyber insurance:

First-party Cyber Risk Exposures:

- ✔ Loss or damage to digital assets - loss or damage to data or software programs, resulting in cost being incurred in restoring, updating, recreating or replacing these assets to the same condition they were in prior to the loss or damage.
- ✔ Business interruption from network downtime - interruption in service or failure of the network, resulting in loss of income, increased cost of operation and/or cost being incurred in mitigating and investigating the loss.
- ✔ Cyber extortion - attempt to extort money by threatening to damage or restrict the network, release data obtained from the network and/or communicate with the customer base under false pretenses to obtain personal information.
- ✔ Theft of money and digital assets - direct monetary losses from electronic theft of funds / money from the organization by hacking or other type of cyber intrusion.
- ✔ Customer notification/Public Relations expenses - legal, postage and advertising expenses where there is a legal or regulatory requirement to notify individuals of a security or privacy breach, including credit monitoring program costs and PR media assistance.

Third-party Cyber Liability Exposures

- ✔ Security and privacy breaches - investigation, defense cost and civil damages associated with security breach, transmission of malicious code, or breach of third-party or employee privacy rights or confidentiality, including failure by outsourced service provider.
- ✔ Investigation of privacy breach - forensics investigation, defense cost, regulatory penalties and fines (may not be insurable in certain states) resulting from an investigation or enforcement action by a regulator as a result of security and privacy liability.
- ✔ Loss of third party data - liability for damage to or corruption / loss of third-party data or information, including payment of compensation to customers for denial of access, failure of software, data errors and system security failure.

EVALUATING AND KNOWING YOUR CYBER INSURANCE CARRIER'S CLAIMS PAYING AND HANDLING REPUTATION IS CRUCIAL

It is crucial that Boards check to make sure the cyber insurance carrier they are considering has a good claims paying and claims handling history.

When a cyber/data breach event happens, there should be no doubt or question as to whether or not a cyber insurance claim is going to be covered or not. Companies should have full confidence that their cyber insurance carrier is going to quickly and promptly respond to an incident in real-time based upon their superb claims paying and claims handling history. Many carriers hire coverage counsel to deal with claims rather than deal with them internally. Though this is not the "kiss of death," our experience is that not all coverage counsel are made equally. Some are very knowledgeable and helpful. Some are, well, not so much.

Today's cyber insurance policy needs to be able to respond to tomorrow's cyber/data breach incidents, promptly and without question. This is why Directors need to work with experienced cyber insurance experts who have the expertise not only in the sophisticated cyber insurance coverages and policies that are available today but also the knowledge of a cyber insurance carrier's claims paying and handling reputation. Your cyber counsel is likely also well versed in defending lawsuits covered by insurance should also be consulted.

CYBER TERRORISM

Cyber terrorism is a real, even imminent threat that affects Companies and governments globally. With today's interconnected networks and devices, cyber attacks can happen anywhere and at any time. Many cyber attacks originate from, or are at the direction of, foreign governments. In recent years, we have seen attacks from hacktivist groups, such as Lulszec and Anonymous, and it is believed that the US Government has classified these hacktivist groups as terrorist organizations. This further complicates cyber insurance claims that could be denied in the event such hacktivist groups are classified as terrorist organizations, and is the cause of your Company's cyber attack or data breach.

Cyber insurance policy language varies on whether cyber terrorism will be covered or not. Most cyber insurance policies will be silent regarding the origin of a cyber attack. Some cyber insurance policies will expressly cover cyber terrorism claims. The choice is easy on this one.

When exploring the purchase of a cyber insurance policy, your Company must be vigilant for the inclusion of any terrorism exclusion as well as "act of war" exclusions in order to determine the scope of available coverage. Some policies are silent on terrorism, while others contain terrorism exclusions, and only a few provide terrorism coverage. Most policies contain act of war exclusions, but contours of what is an act of war are not well defined. Given recent events in 2014 and 2015, the wording of both exclusions should be reviewed accordingly..

WHERE ARE PROPERTY DAMAGE CLAIMS RELATED TO A CYBER ATTACK COVERED?

After recent information released by the Department of Homeland Security that US critical infrastructure (e.g. pipelines and power grids) could be subject to a catastrophic cyber attack, many Companies and legal and risk management personnel were forced to rethink the boundaries of their cyber insurance coverage.

The question is in reality four-fold: (1) what sort of damage might we suffer if our power plants, pipelines, or network servers were critically damaged during a cyber attack, (2) what would the repair or replacement cost be calculated at, (3) since time would likely be of the essence, what would that fact add to the repair or replacement cost (e.g. would it double the cost of the repair?), and (4) would such damage potentially be covered by insurance?

Though we cannot answer all these questions, as not all insurance policies are alike, the above questions should be asked by the board of directors of senior management since recent cyber attacks have thrown in new categories of damages not foreseen under traditional stand-alone cyber insurance policies as we have described above. Though stand-alone cyber insurance policies do cover some portion of first-party business interruption losses, they do not cover all forms of first-party exposure, like property damage claims. It is a fact that most stand-alone cyber insurance policies will exclude property damage claims.

This reality then begs the question of whether traditional General Liability or Property/Casualty insurance policies provide a better solution to first-party cyber insurance claims. The answer to this question is, "it depends on the policy and its exclusions." It is thus beyond the scope of this book to examine all forms and coverage sections of property/casualty insurance policies to see if they would apply in the event of a cyber attack. Rather, the point of this book is to raise the tough questions that board members should be thinking about in today's cybersecurity environment. The scope of what insurance coverage might be available for a cyber attack goes right to the heart of good enterprise risk management, i.e. what are our cyber related risks? What is our risk appetite (i.e. what are we comfortable in self-insuring)? And what risks can we hope to mitigate/insure so as to lessen the balance sheet burden of a potentially very expensive remediation and recovery effort? These are all very important questions. Directors should endeavor to arrive at good answers to them, before it is discovered that their company was the subject of a cyber attack.

WHERE DOES OUR DIRECTORS AND OFFICERS ("D&O") LIABILITY INSURANCE COME INTO PLAY FOR A CYBER ATTACK?

This is another good question that we have been hearing a lot recently. A Company's D&O insurance does not come in to play really in any of the areas we described above. That is for stand-alone cyber insurance coverage. Where the D&O does come into play is if, upon the announcement of the discovery of a major cyber attack, a Company's stock drops by 25% and it and the board is subsequently sued in a securities fraud class action. The securities class action would be a claim under the D&O coverage. So would a shareholder derivative action (a suit brought on behalf of the Company) against the board of directors for failure to properly oversee the cybersecurity policies and procedures of the Company. We mention to the D&O here only because in today's environment, it is hard to separate the losses associated with a cyber attack into one distinct bucket. As was the case in the Target cyber attack, the breach and loss of data implicated many potential different buckets of losses and insurance.

Five Things Every Board Needs to Know When Buying Cyber Insurance:

1. Identify your Company's cyber risks and determine which risks to avoid, accept, mitigate, or transfer through insurance, and obtain a cyber insurance policy that aligns with your Board's cyber risk management strategy.

2. Whilst cyber insurance helps offer an extra layer of defense in a Company's robust cybersecurity program, it is not a substitute for managing your Company's cyber risk. But standalone cyberinsurance will help provide valuable loss mitigation services, experienced and helpful claim handling service, and serve to help offset some, if not all, of the expense of a cybersecurity breach.

3. Don't rely on your Commercial General Liability policy or your Property policy to cover a data breach, as it most likely will not. Standalone cyber insurance policies offer broader coverage and should be explored by every Board, along with an evaluation of the sufficiency of the Company's Directors and Officers liability insurance program.

4. Work with experienced and knowledgeable cyber insurance brokers and insurance coverage lawyers who specialize in the various cyber insurance coverages and policies to make sure your Company gets the best policy that it can. Often times, this means Boards must bypass their current insurance broker due to that broker's lack of knowledge and experience in cyber insurance.

5. Evaluate and know your cyber insurance carrier's claims paying and claims handling history and reputation before purchasing a cyber insurance policy.

SUMMARY

While no Director or Company can predict if and when a cyber attack or a data breach will happen to them, cyber insurance helps minimize the damage if the worst should happen.

Companies are, generally, not protecting themselves properly against their exposure to costs associated with a data breach. It's an expense that is often overlooked and not incorporated into a Company's budget. With cyber attacks and data breaches rapidly increasing with no end in sight, the associated costs that are incurred when responding to these incidents needs to be planned for in advance vs. depleting balance sheet assets that could have been insured for with insurance dollars.

When a data breach happens today, regulators seem to be more understanding that incidents can happen but when they do happen (and they will), how a Company responds to such events is more important than ever. Regulators and affected individuals will be paying close attention to how an incident is being dealt with and how a Company responds as well as what is being done to ensure such an incident does not happen again.

Cyber insurance with data breach response services helps Directors and Companies to proactively prepare today for the unknown data breach response costs of tomorrow.

Cyber liability is a growing issue for Directors and Companies globally and it is no longer acceptable to turn a blind eye or be ill-prepared for such a potential large loss.

If your Company has not yet purchased a cyber insurance policy, it must do so now.

ENDNOTES

[1] See Home Depot Form 8-K, dated September 18, 2014, noting, among other things, "The Company's fiscal 2014 diluted earnings-per-share guidance includes estimates for the cost to investigate the data breach, provide credit monitoring services to its customers, increase call center staffing, and pay legal and professional services, all of which are expensed as incurred in a gross amount of approximately $62 million…."

[2] See "UCLA Health faces lawsuit for privacy breach in recent cyber attack," available at http://dailybruin.com/2015/08/11/ucla-health-faces-lawsuit-for-privacy-breach-in-recent-cyber-attack/; "Anthem's big data breach is already sparking lawsuits," available at http://fortune.com/2015/02/06/anthems-big-data-breach-is-already-sparking-lawsuits/.

[3] Economist Intelligence Unit Report, "Reputation Risk: Risk of Risks " Link: http://databreachinsurancequote.com/wp-content/uploads/2014/10/Reputation-Risks.pdf.

[4] See, "Half of Holiday Shoppers Say They'll Avoid Stores That Got Hacked, Survey Finds," found at http://www.huffingtonpost.com/2014/10/20/shoppers-hacked-stores-survey_n_6004306.html.

[5] See e.g. "Cybersecurity Insurance," available at http://www.dhs.gov/cybersecurity-insurance ("Traditional commercial general liability and property insurance policies typically exclude cyber risks from their terms, leading to the emergence of cybersecurity insurance as a "stand alone" line of coverage. That coverage provides protection against a wide range of cyber incident losses that businesses may suffer directly or cause to others, including costs arising from data destruction and/or theft, extortion demands, hacking, denial of service attacks, crisis management activity related to data breaches, and legal claims for defamation, fraud, and privacy violations.").

[6] "Managing Cybersecurity as a Business Risk: Cyber Insurance in the Digital Age", Ponemon Institute Research Report, August 2013, http://assets.fiercemarkets.com/public/newsletter/fiercehealthit/experian-ponemonreport.pdf.

CHAPTER 12:

ABANDON ALL HOPE, YE WHO LOG ON HERE[1]

I bet after reading many of the previous chapters, you might have agreed with the thrust of the above referenced Buzzfeed article. It seems that no matter what we do or what hardware or software we have installed, our servers are eminently hackable. Even the brand new car that my wife so desperately wants (I am having second thoughts that some bright young college student might want to "experiment" with her car one day) now appears to have potential vulnerabilities.

But if we were to take the author's point to an illogical extreme, then we might as well call the Internet a do-over, and start over again with a security-based, security conscious Internet. Since that will not be happening anytime soon, we can only suggest the following key takeaways. For companies to better protect themselves:

1. No matter how complicated it is, boards must be more actively engaged when it comes to cybersecurity. Not just 4 board meetings a year, for 15 minutes a meeting. One hour a meeting per quarter - at least - unless there is a known data breach, in which case the board should meet as frequently as it needs to. All must be present for the meeting, including the CISO and the outside advisors. It's a relatively straight-forward conversation. How many attacks have we seen over the last quarter? Were we able to defend against them? What are we doing right? What are we doing wrong? How can we improve our cybersecurity posture to make our digital assets more secure from a holistic fashion? Imagine if this sort of discussion happened at every board meeting?

2. Every company's IT department must spend a minimum of four hours a quarter doing IP asset identification, valuation and classification. The highest valued 10% of those assets get protected like Fort Knox. Impenetrable. Put them off-line somewhere. Segment them. Encrypt them at a minimum of 256 bit (if not higher if you are able). Do something different with them than with lesser valued data. But please do something to get them out of harm's way. And you don't have to keep credit card or other personal information that might have expired or become stale years ago. Clean "house" on your server. Expunge what information you are not required to keep or don't have to keep any longer.

3. No more password only log-ons - #deathtothepassword -- all companies from now on need multi-factor authentication. Biometric authentication would be a thing of beauty. Behavioral authentication even better. For those who continue to use passwords as their sole means of accessing the network, employees who use "password," "0123456," or "qwerty" should be banished to the Icelandic office of their respective companies. The same for employees or companies that store passwords in a file named "Password."

4. Thou shalt patch known critical application vulnerabilities on an ASAP basis. Other vulnerabilities within 48 hours of release depending upon their criticality.

5. Mandatory employee training on phishing, spearphishing and business email high-jacking given the prevalence of socially-engineered scams. Once a month. With reporting packages to see which employees get it and which don't. For those who don't, well they need to do pushups.

6. Every organization must have an incident response plan, and a business continuity plan. Period. And they both must be practiced quarterly. Resiliency is the name of the game, when recent history has proven that anyone can get hacked.

7. Required Reading: the NIST Cybersecurity Framework and the April 29, 2015 Department of Justice Incident Response Memorandum. Adopt the recommendations present in both documents into your cybersecurity and cyber governance practices ASAP.

8. Every organization needs a big-data, anomaly-based intrusion detection/prevention system to help correlate and better identify that thousands of alerts they get everyday. You can't chase down every alert. A finely-tuned intrusion detection/prevention system might help separate the wheat from the chaff.

9. All organizations need to share threat information within their peer group, formally or informally. Let's not wait for Congress to do something brilliant. That won't happen in time to prevent the next big cyber attack.

10. Mandatory endpoint security protection for all iPhones, androids, laptops, iPads, etc. - and there must be a secure inventory and identification of all those devices. If the employee doesn't have the protection installed, he or she doesn't get access to the network. No soup for them.

11. Consider mandatory encryption of PII and sensitive data, in rest, in motion, in use, on your server or in the cloud. Wherever your data may be.

12. All remote access to the internet must be done via VPN. No unsecure Internet ports. Ever.

13. Do you want to self-insure for a cyber breach and pay millions in balance sheet assets to clean up the mess resulting from a sophisticated cyber attack, or do you want to consider cyber insurance to provide the best possible cushion for those assets?

We urge any board to pick 4 of the above takeaways. Even five or more if they are daring. Some don't cost a lot of money. Some are well worth the cost. There are business judgments that will need to be made. And boards must make them in order to satisfy their cybersecurity oversight fiduciary duties. Or potentially jeopardize their company's enterprise value and their individual well-being.

Is what we are doing today for cybersecurity working? Clearly, "No."

Can we do better? Absolutely.

Do you want to remain "in the pack" of companies being picked off every day? - or out in front of the pack? There is no "safety in numbers" here.

Do you want a friction-filled cybersecurity environment with maximum defenses when a hacker comes knocking, or do you want them to slip and slide into your network without a sweat?

You need to decide - soon - how to best navigate the cyber-storm we are presently in. The life of your company or your firm may depend upon it.

ENDNOTES

[1] This was the name of a funny, sad, but true article we found after BlackHat 2015, which is available at http://www.buzzfeed.com/josephbernstein/so-fing-fd?utm_content=buffer3af08&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer#.leWrL9VJWy.

ABOUT ADVISEN

Advisen is leading the way to smarter and more efficient risk and insurance communities. Through its information, analytics, ACORD messaging gateway, news, research, and events, Advisen reaches more than 150,000 commercial insurance and risk professionals at 8,000 organizations worldwide. The company was founded in 2000 and is headquartered in New York City, with offices in the US and the UK.

ABOUT AIG

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit our website at www.aig.com. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries, and coverage is subject to actual policy language. Non-insurance products and services may be provided by independent third parties. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insureds are therefore not protected by such funds.

Investigations · Compliance Solutions · Cyber Defense

ABOUT K2

K2 Intelligence is an industry-leading investigative, compliance and cyber defense services firm founded in 2009 by Jeremy M. Kroll and Jules B. Kroll, the originator of the modern corporate investigations industry. Over the last 40 years, Jules, Jeremy, and their teams have built a reputation not only for investigative, analytic and advisory excellence but for the independence and insight they bring to investigations. With offices in New York, London, Madrid, Tel Aviv and Geneva, K2 Intelligence advises governments, companies, boards and individuals in business areas including: Complex Investigations & Disputes; Anti Money Laundering and Regulatory Compliance; Integrity Monitoring & Compliance; Data Analytics & Visualization; Board Advisory; and Cybersecurity Investigations & Defense.
For more information, visit www.k2intelligence.com

GLOSSARY

DIRECTOR AND OFFICER GLOSSARY OF DEFINED CYBERSECURITY TERMS[1]

A

Active Attack
An actual assault perpetrated by an intentional threat source that attempts to alter a system, its resources, its data, or its operations.

Advanced Persistent Threat
An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception).

Alert
A notification that a specific attack has been detected or directed at an organization's information systems.

Antispyware Software
A program that specializes in detecting and blocking or removing forms of spyware.

Antivirus Software
A program that monitors a computer or network to detect or identify major types of malicious code and to prevent or contain malware incidents. Sometimes by removing or neutralizing the malicious code.

Asset
A person, structure, facility, information, and records, information technology systems and resources, material, process, relationships, or reputation that has value.

Extended Definition: Anything useful that contributes to the success of something, such as an organizational mission; assets are things of value or properties to which value can be assigned.

Attack Pattern
Similar cyber events or behaviors that may indicate an attack has occurred or is occurring, resulting in a security violation or a potential security violation. *Extended Definition:* For software, descriptions of common methods for exploiting software systems.

Attack signature
A characteristic or distinctive pattern that can be searched for or that can be used in matching to previously identified attacks.

Authentication
The process of verifying the identity or other attributes of an entity (user, process, or device).

Authenticity
A property achieved through cryptographic methods of being genuine and being able to be verified and trusted, resulting in confidence in the validity of a transmission, information or a message, or sender of information or a message.

Authorization
A process of determining, by evaluating applicable access control information, whether a subject is allowed to have the specified types of access to a particular resource. *Extended Definition:* The process or act of granting access privileges or the access privileges as granted.

B

Behavior Monitoring
Observing activities of users, information systems, and processes and measuring the activities against organizational policies and rule, baselines of normal activity, thresholds, and trends.

Bot
A computer connected to the Internet that has been surreptitiously / secretly compromised with malicious logic to perform activities under remote the command and control of a remote administrator. *Related term:* A member of a larger collection of compromised computers known as a botnet.

Bot Master
The controller of a botnet that, from a remote location, provides direction to the compromised computers in the botnet. *Synonym(s):* bot herder

Botnet
A collection of computers compromised by malicious code and controlled across a network.

Bug
An unexpected and relatively small defect, fault, flaw, or imperfection in an information system or device.

C

Cloud Computing
A model for enabling on-demand network access to a shared pool of configurable computing capabilities or resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Critical Infrastructure
The systems and assets, whether physical or virtual, so vital to society that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment,

or any combination of these matters.

Cryptographic Algorithm
A well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output.

Cryptography
The use of mathematical techniques to provide security services, such as confidentiality, data integrity, entity authentication, and data origin authentication.

Cryptology
The mathematical science that deals with cryptanalysis and cryptography.

Cyber Exercise
A planned event during which an organization simulates a cyber disruption to develop or test capabilities such as preventing, detecting, mitigating, responding to or recovering from the disruption.

Cyber Infrastructure
The information and communications systems and services composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements:

- Processing includes the creation, access, modification, and destruction of information.
- Storage includes paper, magnetic, electronic, and all other media types.
- Communications include sharing and distribution of information.

Cybersecurity
The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation.

Cyberspace
The interdependent network of information technology infrastructures, that includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

D

Data Breach
The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information.

Data Integrity
The property that data is complete, intact, and trusted and has not been modified or destroyed in an unauthorized or accidental manner.

Data Loss
The result of unintentionally or accidentally deleting data, forgetting where it is stored, or exposure to an unauthorized party.

Digital Forensics
The processes and specialized techniques for gathering, retaining, and analyzing system-related data (digital evidence) for investigative purposes.

Digital Rights Management
A form of access control technology to protect and manage use of digital content or devices in accordance with the content or device provider's intentions.

Digital Signature
A value computed with a cryptographic process using a private key and then appended to a data object, thereby digitally signing the data.

Disruption
An event which causes unplanned interruption in operations or functions for an unacceptable length of time.

Distributed Denial Of Service
A denial of service technique that uses numerous systems to perform the attack simultaneously.

Dynamic Attack Surface
The automated, on-the-fly changes of an information system's characteristics to thwart actions of an adversary.

E

Encryption
The process of transforming plaintext into ciphertext.

Enterprise Risk Management
A comprehensive approach to risk management that engages people, processes, and systems across an organization to improve the quality of decision making for managing risks that may hinder an organization's ability to achieve its objectives.

Event
An observable occurrence in an information system or network.

Extended Definition: Sometimes provides an indication that an incident is occurring or at least raise the suspicion that an incident may be occurring.

Exfiltration
The unauthorized transfer of information from an information system.

Exploit
A technique to breach the security of a network or information system in violation of security policy.

Exploitation Analysis
In the NICE Workforce Framework, cybersecurity work where a person: Analyzes collected information to identify vulnerabilities and potential for exploitation.

Exposure
The condition of being unprotected, thereby allowing access to information or access to capabilities that an attacker can use to enter a system or network.

F

Failure
The inability of a system or component to perform its required functions within specified performance requirements.

Firewall
A capability to limit network traffic between networks and/or information systems.

Extended Definition: A hardware/software device or a software program that limits network traffic according to a set of rules of what access is and is not allowed or authorized.

H

Hacker
An unauthorized user who attempts to or gains access to an information system.

I

Incident
An occurrence that actually or potentially results in adverse consequences to (adverse effects on) (poses a threat to) an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.

Extended Definition: An occurrence that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Incident Management
The management and coordination of activities associated with an actual or potential occurrence of an event that may result in adverse consequences to information or information systems.

Incident Response
Cybersecurity work where a person responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats; uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.

Incident Response Plan
A set of predetermined and documented procedures to detect and respond to a cyber incident.

Indicator
An occurrence or sign that an incident may have occurred or may be in progress.

Information System Resilience
The ability of an information system to: (1) continue to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (2) recover effectively in a timely manner.

Inside (R) Threat
A person or group of persons within an organization who pose a potential risk through violating security policies.

Extended Definition: One or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm.

Intrusion Detection
The process and methods for analyzing information from networks and information systems to determine if a security breach or security violation has occurred.

Investigation
A systematic and formal inquiry into a qualified threat or incident using digital forensics and perhaps other traditional criminal inquiry techniques to determine the events that transpired and to collect evidence.

M

Macro Virus
A type of malicious code that attaches itself to documents and uses the macro programming capabilities of the document's application to execute, replicate, and spread or propagate itself.

Malicious Applet
A small application program that is automatically downloaded and executed and that performs an unauthorized function on an information system.

Malicious Code
Program code intended to perform an unauthorized function or process that will have adverse impact on the confidentiality, integrity, or availability of an information system.

Malicious Logic
Hardware, firmware, or software that is intentionally included or inserted in a system to perform an unauthorized function or process that will have adverse impact on the confidentiality, integrity, or availability of an information system.

Malware
Software that compromises the operation of a system by performing an unauthorized function or process.

Mitigation
The application of one or more measures to reduce the likelihood of an unwanted occurrence and/or

lessen its consequences.

Extended Definition: Implementing appropriate risk-reduction controls based on risk management priorities and analysis of alternatives.

Moving Target Defense
The presentation of a dynamic attack surface, increasing an adversary's work factor necessary to probe, attack, or maintain presence in a cyber target.

N

Network Resilience
The ability of a network to:

(1) provide continuous operation (i.e., highly resistant to disruption and able to operate in a degraded mode if damaged);
(2) recover effectively if failure does occur; and
(3) scale to meet rapid or unpredictable demands.

P

Passive Attack
An actual assault perpetrated by an intentional threat source that attempts to learn or make use of information from a system, but does not attempt to alter the system, its resources, its data, or its operations.

Penetration Testing
An evaluation methodology whereby assessors search for vulnerabilities and attempt to circumvent the security features of a network and/or information system.

Phishing
A digital form of social engineering to deceive individuals into providing sensitive information.

Privacy
The assurance that the confidentiality of, and access to, certain information about an entity is protected.

R

Recovery
The activities after an incident or event to restore essential services and operations in the short and medium term and fully restore all capabilities in the longer term.

Resilience

The ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption.

S

Secret Key
A cryptographic key that is used for both encryption and decryption, enabling the operation of a symmetric key cryptography scheme.

Spam
The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

Spear Phishing
An e-mail spoofing fraud attempt that targets a specific organization, or a specific individual with an organization or organization department, seeking unauthorized access to confidential data.

Spoofing
Faking the sending address of a transmission to gain illegal (unauthorized) entry into a secure system.

Spyware
Software that is secretly or surreptitiously installed into an information system without the knowledge of the system user or owner.

T

Tabletop Exercise
A discussion-based exercise where personnel meet in a classroom setting or breakout groups and are presented with a scenario to validate the content of plans, procedures, policies, cooperative agreements or other information for managing an incident.

Trojan Horse
A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

U

Unauthorized Access
Any access that violates the stated security policy.

V

Virus

A computer program that can replicate itself, infect a computer without permission or knowledge of the user, and then spread or propagate to another computer.

Vulnerability
A characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard.

W

Worm
A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread itself.

[1] This Glossary was adapted from (but simplified by me) for business executives, directors and officers from the National Institute of Standards and Technology "Glossary of Key Information Security Terms," which is available at http://www.nist.gov/manuscript-publication-search.cfm?pub_id=913810.

ADVISEN'S CYBER DATASET

Advisen's Cyber Database is a proprietary relational database of information about various "Cyber risk"-related events which have or could have resulted in significant financial judgments or financial loss to corporate entities.

"Cyber risk" means any risk of financial or physical loss, disruption of services or damage to the assets or reputation of an organization through either a failure of its information or technology systems, or a malicious act affecting their information or technology systems. While system "hacks" and data breaches get the lion's share of publicity, Advisen's Cyber Dataset also includes such risks as:

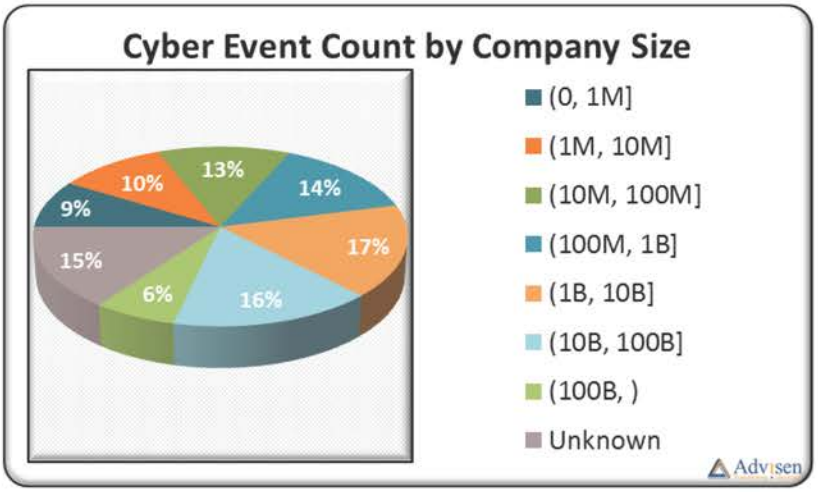
- Digital Data Breach, Loss, or Theft
- System/Network Security Violation or Disruption, including DDOS
- Identity Theft/Fraudulent Use or Access
- Improper Collection of Digital Data
- Improper Disposal/Distribution, Loss or Theft (Printed Records)
- Digital Asset Loss or Theft
- Privacy Violations
- Phishing, Skimming
- Cyber Extortion

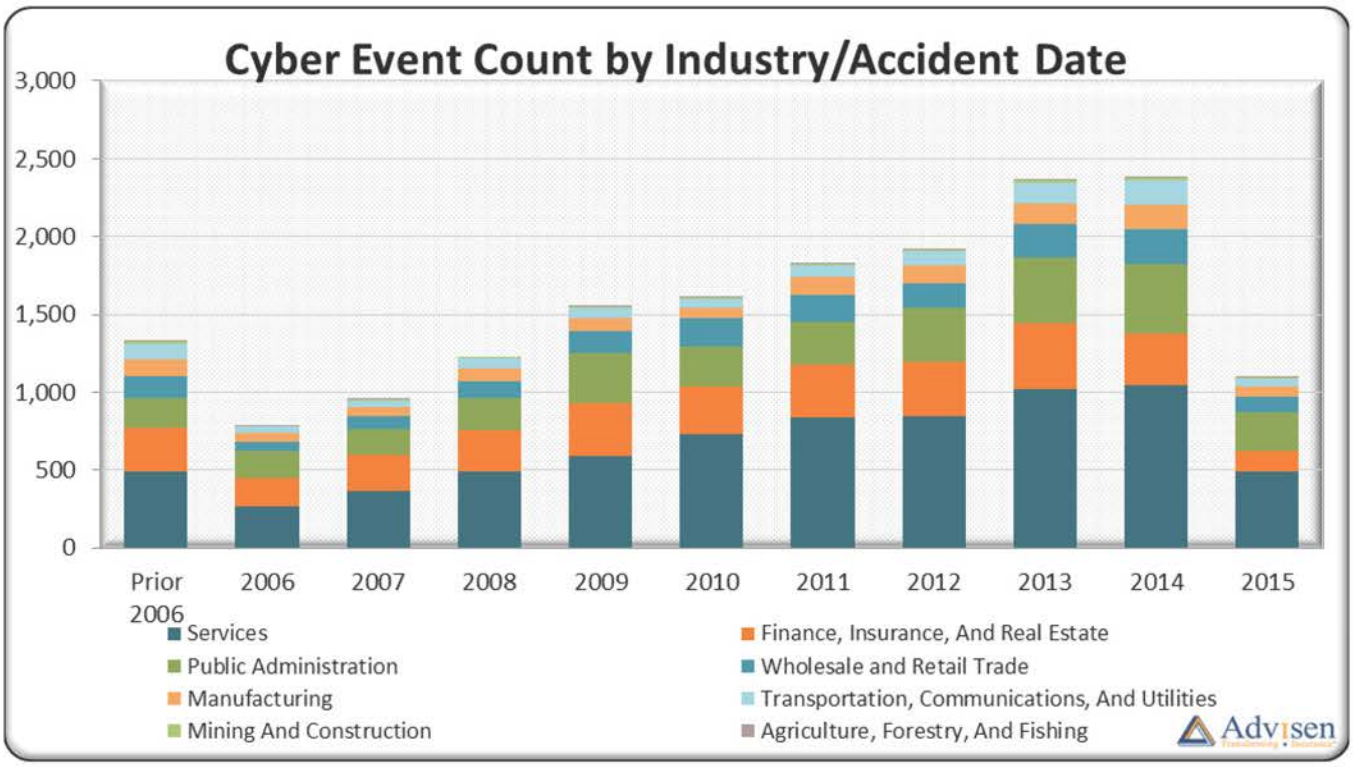
As of October 2015, the Advisen cyber database includes more than **21,000 cases** involving billions of unauthorized disclosures, thefts, or serious disruptions of customer & employee identities, corporate assets, and systems capabilities.

DATA FEEDS DELIVERY

Advisen's Cyber Data Feeds contain **model-ready** Cyber data, married to **current and historic company data**. The intersection of loss and company data supports actuaries building sophisticated proprietary algorithms using **multiple parameters**, such as:

- Company Size
- Industry Code
- Number of Employees
- Company Type
- Accident Date
- Case Type
- Case Status
- Data Type
- Data Media
- Geography





Advisen's Cyber Dataset is growing every day at a fast pace, and Cyber Data Feeds will be refreshed on a monthly or quarterly basis and be delivered in Excel.

CYBER DATA FEATURES

Advisen has developed a unique taxonomy for the cyber database similar to the structure of a cyber-insurance policy, facilitating the **actuarial modeling** and **pattern or trend analysis** for insurance brokers, carriers and reinsurers.

A proportion of Advisen Cyber Data have been linked by interrelated root causes and been identified as **related cases**, allowing the user to model the **aggregation** of the potential risk across the portfolio.

Advisen leverages both Standard Industrial Classification (**SIC**) code system and North American Industry Classification System (**NAICS**). The latter provides a greater level of detail about a firm's activity and more accurately assigns the new technology or cutting-edge industries.

Advisen also provides the **denominator** information, Stat-Master, to support further loss analysis. Stat-Master is a data mart of time series business information and is consisted of Company Attribute File and Census File.

About Advisen Ltd.

Advisen is leading the way to smarter and more efficient risk and insurance communities. Through its information, analytics, ACORD messaging gateway, news, research, and events, Advisen reaches more than 150,000 commercial insurance and risk professionals at 8,000 organizations worldwide. The company was founded in 2000 and is headquartered in New York City, with offices in the US and the UK.

THANK YOU TO OUR SPONSORS!

AIG

K2 Intelligence

Investigations · Compliance Solutions · Cyber Defense