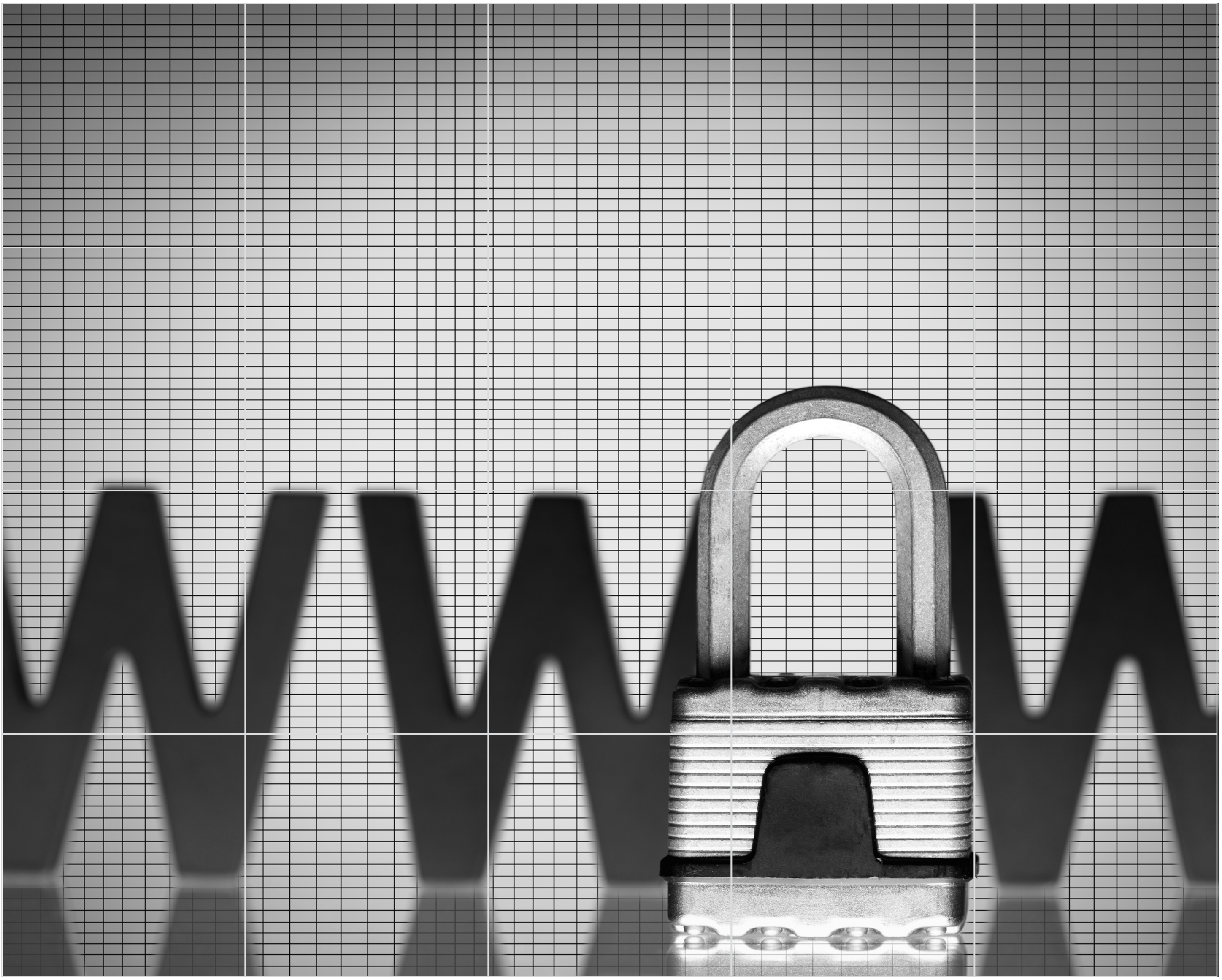
Weil

Cybersecurity for the C-Level



Director Glossary of Defined Cybersecurity Terms

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, record, information technology system or resource, material, process, relationship, or reputation that has value.

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.

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).

Glossary adapted, in part, from list of common cybersecurity terms published by the Department of Homeland Security, available at http://niccs.us-cert.gov/glossary.

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.

B

Behavior Monitoring

Observing activities of users, information systems, and processes and measuring the activities against organizational policies and rules, 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: 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 security, economy, public health or safety, environment, or any combination of these things.

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 cryptoanalysis 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.

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.

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, adversely effects, or 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.

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; and 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.

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.

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, 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.

Weil

weil.com

BEIJING
BOSTON
BUDAPEST
DALLAS
DUBAI
FRANKFURT
HONG KONG
HOUSTON
LONDON
MIAMI
MUNICH
NEW YORK
PARIS
PRAGUE
PRINCETON
PROVIDENCE
SHANGHAI
SILICON VALLEY
WARSAW
WASHINGTON, DC

Weil, Gotshal & Manges LLP