Cyber Glossary

Content Links:

Cyber Security

basics you need to know to protect your business from hackers

Access
To gain use of a system or program, the information stored within it, or retrieve information/data from a system

Access Authority
An entity responsible for monitoring and granting access privileges for other authorized entities. (NIST Glossary)

Access Control
A technical mechanism in hardware or software that permits or denies user access to information resources based on specific attributes, most commonly a user's identity.

Account Management
An activity that involves 1) the process of requesting, establishing, issuing, and closing user accounts; 2) tracking users and their respective access authorizations; and 3) managing these functions. (NIST Glossary)

Application
A software program hosted by an information system. (NIST Glossary)

Application Service Provider
A company that gives individuals or businesses access through the Internet to specialized software applications and other

Authorization
Access privileges granted to a user, program, or process or the act of granting those privileges. (NIST Glossary)

Availability
Ensuring timely and reliable access to and use of information. (NIST Glossary)

Basic Service Set (BSS)
A set of components that connect to a wireless medium and communicate with each other. (http://www.webopedia.com/TERM/B/Basic_Service_Set.html)

Bring Your Own Device (BYOD)
An enterprise policy used to permit partial or full integration of user-owned mobile devices for business purposes. (http://www.isaca.org/knowledge center/documents/glossary/cybersecurity_fundamentals_glossary.pdf

Cloud Computing
You are leasing computing resources or storage from another company that manages it. It is not under your ownership or control. A model for enabling on-demand network access to a shared pool of configurable IT capabilities/ resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (NIST Definition of Cloud Computing (NIST SP 800-145))

a. **Community cloud** – a shared storage area that allows multiple companies the same resources. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises. (NIST SP 800-145)

b. **Hybrid cloud** – using multiple cloud storage options, such as community cloud and private cloud, together. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but

Back to top

are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds). (NIST SP 800-145)

c. **Infrastructure as a Service (IaaS)** – leasing hardware like a copier/printer that you have on your property and use, but it is managed and serviced by the leasing company. This hardware is not customizable. The capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls). (NIST SP 800-145)

d. **Private cloud** – a cloud resource that is dedicated to your business, it stores your information independently from other companies data. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises. (NIST SP 800-145)

e. **Software as a Service (SaaS)** – purchasing software and paying a monthly service fee to use it rather than purchasing the hard disc copy. The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings. (NIST SP 800-145)

Computer Security

Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated. (NIST Glossary)

Cryptocurrency

A digital currency in which encryption techniques are used to regulate the generation of units and verify the transfer of funds, operating independently of a central bank. (http://www.oxforddictionaries.com/us/definition/american_english/cryptocurrency)

Cyber Hygiene

A set of practices individuals and organizations perform regularly to maintain the health and security of users devices, networks, and data. (https://www.techtarget.com/searchsecurity/definition/cyber-hygiene)

Cyber Infrastructure

Electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are 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. (NIST Glossary)

Cyber Maturity Model
A mechanism to have cyber resilience controls, methods and processes assessed according to management best practice, against a clear set of external benchmarks. (CPMI/IOSCO Cyber Guidance)

Cyber Resilience
Ability to anticipate, absorb, adapt to, rapidly respond to and recover from disruption caused by a cyber-attack. Also known as information system resilience. (CPMI/IOSCO Cyber Guidance)

Cyber Security
The ability to protect or defend the use of cyberspace from cyber-attacks. (NIST Glossary)

Data
A set of information.

Data Asset
Any entity that is comprised of data or information-based resource. (NIST Glossary)

Data Loss Prevention (DLP)
A comprehensive approach (covering people, processes, and systems) of implementing policies and controls designed specifically to discover, monitor, and protect confidential data wherever it is stored, used, or in transit over the network and at the perimeter. Also known as data leakage prevention. (Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook)

Data Security
Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure. (NIST Glossary)

Dependent Business
A relationship with another business entity that relies on the continued operational viability of that non-related entity. (http://www.mynewmarkets.com/articles/98062/business-income-from-dependent-properties)

Device
A unit of physical hardware or equipment that provides one or more computing functions within a computer system. It can provide input to the computer, accept output or both. A device can be any electronic element with some computing ability that supports the installation of firmware or third-party software. (https://www.techopedia.com/definition/2185/device)

Digital Asset
Any digital material owned by an enterprise or individual. (http://www.pcmag.com/encyclopedia/term/41283/digital-asset)

Distributed Control Systems (DCS)
A type of automated control system that is distributed throughout a machine to provide instructions to different parts of the machine. Instead of having a centrally located device controlling all machines, each section of a machine has its own computer that controls the operation. (http://www.businessdictionary.com/definition/distributed-control-system-DCS.html)

Electronic Data
A subset of information in an electronic format that allows it to be retrieved or transmitted. (NIST Glossary)

Enterprise
An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management. (NIST Glossary)

External Network
A network not controlled by the organization. (NIST Glossary)

Full Disk Encryption
The process of encrypting all the data on the hard disk drive used to boot a computer, including the computer's operating system, and permitting access to the data only after successful authentication with the full disk encryption product. (NIST Glossary)

Industrial Control System
An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems (SCADA) used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems using programmable logic controllers to control localized processes. (NIST Glossary)

Information Systems
Electronic and paper-based systems and physical components used to access, store, transmit, protect, and eventually dispose of information. Information systems can include networks (computer systems, connections to business partners and the Internet, and the interconnections between internal and external systems). (FFIEC Information Security Booklet)

Information Technology (IT)
Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. (NIST Glossary)

Internal Network
A network where: (i) the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or (ii) cryptographic encapsulation or similar security technology provides the same effect. An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned. (NIST Glossary)

Internet
The single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the Internet Architecture Board (IAB), and (b) the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN). (NIST Glossary)

Internet Service Provider
A company that provides its customers with access to the Internet. (FFIEC IT Examination Handbook)

Mobile Application
A type of application software designed to run on a mobile device, such as a smartphone or tablet computer. Mobile applications frequently serve to provide users with similar services to those accessed on PCs. Also known as an "app." (https://www.techopedia.com/definition/2953/mobile-application-mobile-app)

Mobile Code
Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. (NIST Glossary)

Mobile Device
Portable cartridge/disk-based, removable storage media (e.g., floppy disks, compact disks, USB flash drives, external hard drives, and other flash memory cards/drives that contain nonvolatile memory). Portable computing and communications device with information storage capability (e.g.,

notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). (NIST Glossary)

Network
Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. (NIST Glossary; SP 800-53)

Network Access
Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet). (NIST Glossary)

Operations Technology
The hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise. (Gartner IT Glossary)

Portable Communications Equipment
Portable communications and data management devices have the primary purpose of which is the transmission, receipt and management of electronic data or provision of applications via a public electronic communications service. They may also have secondary voice or telephonic facilities that do not exclude them from this definition. (https://www.admin.ox.ac.uk/finance/epp/expenses/guide/pdas_computers/)

Portable Electronic Device
Any nonstationary electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes but is not limited to laptops, personal digital assistants, pocket personal computers, palmtops, MP3 players, cellular telephones, thumb drives, video cameras, and pagers. (NIST Glossary)

Portable Media
A handheld multimedia device that can play digital music, image, and movie files that have been downloaded from the Internet or stored on a personal computer. (http://whatis.techtarget.com/definition/portable-media-center)

Security
A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach. (NIST Glossary)

Security Policy
A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data. (NIST Glossary)

Sensitive Information
Information whose loss, misuse, unauthorized access to, or modification could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy. (NIST Glossary)

Service Level Agreement
Defines the specific responsibilities of the service provider and sets the customer expectations (NIST Glossary)

Service Set Identifier (SSID)
A case sensitive, 32 alphanumeric character unique identifier attached to the header of

packets sent over a wireless local-area network (WLAN) that acts as a password when a mobile device tries to connect to the basic service set (BSS) – a component of the IEEE 802.11 WLAN architecture. (www.webopedia.com/TERM/S/SSID.html)

Software
Computer programs and associated data that may be dynamically written or modified during execution. (NIST Glossary)

Supervisory Control and Data Acquisition Systems (SCADA)
A system of hardware and software meant to control industrial processes locally or remotely to monitor, gather, and process real-time data. This is in an attempt to mitigate downtime.

Supply Chain
A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers. (NIST Glossary)

System
Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. (NIST Glossary)

Token
Something that the User possesses and controls (typically a key or password) that is used to authenticate the User's identity. (NIST Glossary)

Uniform Resource Locator (URL)
The global address of documents and other resources on the World Wide Web. (http://www.webopedia.com/TERM/U/URL.html)

User
Individual or (system) process authorized to access an information system. (NIST Glossary)

Vulnerability Assessments
Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. (NIST Glossary)

Vulnerability Scans
Security technique used to identify security weaknesses in a computer system. (https://www.techopedia.com/definition/4160/vulnerability-scanning)

Wired Equivalent Privacy (WEP)
A security protocol, specified in the IEEE 802.11 standard, that is designed to provide a WLAN with a level of security and privacy comparable to what is usually expected of a wired LAN. WEP is no longer considered a viable encryption mechanism due to known weaknesses. (NIST Glossary)

Wireless Local-Area Network (WLAN)
A wireless distribution method for two or more devices that use high-frequency radio waves and often include an access point to the Internet. (https://www.techopedia.com/definition/5107/wireless-local-area-network-wlan)

WPA/WPA2
Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) security protocols and security certification programs to secure wireless computer networks. (http://www.pcmag.com/encyclopedia/term/54879/wpa)

WORM (Write Once Read Many)
A data storage technology that allows data to be written to a storage medium a single time and prevents the data from being erased or modified. Data stored on a WORM-compliant device is considered immutable; authorized users can read the data as often as needed,

but they cannot change it. (https://www.techtarget.com/searchstorage/definition/WORM-write-once-read-many) (See Worm in Cyber Attack for additional definition)

Back to top

Cyber Attack

what the hackers do

Advanced Persistent Threat

An adversary that possesses 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). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives. (NIST Glossary)

Attack

Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. (NIST Glossary)

Attack Surface

The sum of an information system's characteristics in the broad categories (software, hardware, network, processes and human) which allows an attacker to probe, enter, attack or maintain a presence in the system and potentially cause damage to the institution. A smaller attack surface means that the institution is less exploitable and an attack less likely. However, reducing attack surfaces does not necessarily reduce the damage an attack can inflict. (Committee on Payments and Market Infrastructure and Board of the International Organization of Securities Commissions Guidance on cyber resilience for financial market infrastructures (CPMI/IOSCO Cyber Guidance))

Attack Vector

A path or means, potential or realized, by which a hacker can gain access to a computer or network server in order to deliver a payload or effect a malicious outcome. (http://searchsecurity.techtarget.com/dictionary/definition/1005812/attack-vector.html)

Brick

To cause an electronic device to become completely and irrevocably nonfunctional.

Computer Network Attack (CNA)

Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (NIST Glossary)

Computer Security Incident

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. (NIST Glossary)

Computer System Disruption

An event which causes unplanned interruption in operations or functions for an unacceptable length of time. (Committee for National Security Systems Instruction 4009 (CNSSI 4009))

Cross Site Scripting

A vulnerability that allows attackers to inject malicious code into an otherwise benign website. These scripts acquire the permissions of scripts generated by the target website and can therefore compromise the confidentiality and integrity of data transfers between the website and client. Websites are vulnerable if they display user supplied data from requests or forms without sanitizing the data so that it is not executable. (NIST Glossary)

Cyber Incident
Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. (NIST Glossary)

Cyberextortion
Is a crime involving an attack or threat of an attack coupled with a demand for money or some other response in return for stopping or remediating the attack. (https://www.techtarget.com/searchsecurity/definition/cyberextortion)

Cyber Threat
A circumstance or event with the potential to intentionally or unintentionally exploit one or more vulnerabilities in an institution's systems, resulting in a loss of confidentiality, integrity or availability. (CPMI/IOSCO Cyber Guidance)

Data Breach (aka Data Compromise)
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. (National Initiative for Cybersecurity Careers and Studies Cyber Glossary (NICCS Glossary))

Data at Rest
Data in computer storage while excluding data that is traversing a network or temporarily residing in computer memory to be read or updated. (http://searchstorage.techtarget.com/definition/data-at-rest)

Data in Transit
Data that is moving across public or "untrusted" network such as the Internet, and data that is moving within the confines of private networks such as corporate Local Area Networks (LANs). (SANS, InfoSec Reading Room)

Data Loss
The exposure of proprietary, sensitive, or classified information through either data theft or data leakage. (NIST Glossary)

Denial of Service Attack
The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.) (NIST Glossary)

Encrypt
Generic term encompassing encipher and encode. (NIST Glossary)

Encryption
The process of changing plaintext into ciphertext for the purpose of security or privacy (NIST Glossary)

Exfiltration
The unauthorized copying, transfer or retrieval of data from a computer or server. (https://www.techopedia.com/definition/14682/data-exfiltration)

Exploit
Any method used by hackers to gain unauthorized access to computers, the act itself of a hacking attack, or a hole in a system's security that opens a system to an attack. (https://www.techopedia.com/definition/4275/exploit)

Firewall
A hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy. (NIST Glossary)

Firmware
The programs and data components of a cryptographic module that are stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution. (NIST Glossary)

Host-Based Intrusion Detection System (HIDS)
IDSs which operate on information collected from within an individual computer system. This vantage point allows host-based IDSs to determine exactly which processes and user accounts are involved in a particular attack on the Operating System. (NIST Glossary; SP 800-36)

Information Security
The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. (NIST Glossary)

Information Security Architecture
An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise's mission and strategic plans. (NIST Glossary)

Insider Threat
This can be any person with inside access to your businesses information systems. These could be recently terminated employees, vendors, or contractors with malicious intent.

Internet Protocol
Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks. (NIST Glossary)

Interruption in Service
Unavailability or decrease in quality of service due to unexpected behavior of that particular service, or an incident impacting consumers that results in a service not being delivered at a level they reasonably expected. (ATIS 0100012.2007 Standard Outage Classification)

Intrusion Detection
The process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents. (NIST Glossary)

Intrusion Detection System (IDS)
Software that automates the intrusion detection process. (NIST Glossary)

Intrusion Prevention
The process of performing intrusion detection and attempting to stop detected possible incidents. (NIST Glossary)

Intrusion Prevention System (IPS) – System(s) which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets. (NIST Glossary)

Malicious Code
Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code. (NIST Glossary)

Malware
A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. (NIST Glossary)

Multi-Factor Authentication
Authentication using two or more factors to achieve authentication. Factors include: (i) something you know (e.g. password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). (NIST Glossary)

Network-Based Intrusion Detection System (NIDS)
IDSs which detect attacks by capturing and analyzing network packets. (NIST Glossary)

Network Security
Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (NIST Glossary)

Operational Security (OPSEC)
Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures. (NIST Glossary)

Patch
An update to an operating system, application, or other software issued specifically to correct particular problems with the software. (NIST Glossary)

Penetration Testing
A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system. (NIST Glossary)

Phishing
A malicious email meant to trick you into clicking on a link, downloading an attachment, enabling macros, providing personal information, or providing payment. This includes threats of harm, promise of rewards, or attempts pretending to be a legitimate company or individual".

a. Smishing
A malicious text meant to trick you into clicking on a link, providing personal information, or providing payment. This includes threats of harm, promise of rewards, attempts pretending to be a legitimate company or individual, or simply a blank text with just the URL.

b. Vishing
A malicious phone call meant to trick you into providing confidential information or payment information. This usually takes the form of pretending to be a customer, pretending to be a vendor, or pretending to be a financial service provider looking for payment information (i.e. calling about your car's insurance or warranty).

Plaintext
Ordinary readable text before being encrypted. (http://searchsecurity.techtarget.com/definition/plaintext)

RAM Scraping
A type of electronic fraud in which malware is installed at a point-of-sale terminal and allows debit or credit card information to be illicitly collected. A RAM scraping attack focuses on the terminal's memory, called random access memory (RAM), during the brief period of time when the terminal communicates transaction data to the back-end system. (http://www.investopedia.com/terms/r/ram-scraping-attack.asp)

Ransomware
A type of malware program that infects, locks or takes control of a system and demands ransom to undo it. Ransomware attacks and infects a computer with the intention of extorting money from its owner. (https://www.techopedia.com/definition/4337/ransomware)

Remote Deposit Capture
A service which allows a user to scan checks and transmit the scanned images and / or

ACH-data to a bank for posting and clearing. (http://www.remotedepositcapture.com/overview/rdc.overview.aspx)

Scareware
A type of malware program that infects your computer and displays messages that are intended to trick the user into thinking that they need to buy and download unnecessary and dangerous software like fake antivirus protection. (Google definitions from Oxford Languages)

Secure Socket Layer (SSL)
A protocol used for protecting private information during transmission via the Internet. Note: SSL works by using a public key to encrypt data that is transferred over the SSL connection. Most Web browsers support SSL, and many Web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with “https:” instead of “http:.” (NIST Glossary)

Security Breach
Any incident that results in unauthorized access of data, applications, services, networks and/or devices by bypassing their underlying security mechanisms. (https://www.techopedia.com/definition/29060/security-breach)

Security Threat
In computer security a threat is a possible danger that might exploit a vulnerability to breach security and therefore cause possible harm. A threat can be either "intentional" or "accidental" or otherwise a circumstance, capability, action, or event. (Internet Engineering Task Force RFC 2828 Internet Security Glossary)

Social Engineering
A general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious. (NIST Glossary)

SQL Injection
An exploit of target software that constructs structure query language (SQL) statements based on user input. An attacker crafts input strings so that when the target software constructs SQL statements based on the input, the resulting SQL statement performs actions other than those the application intended. SQL injection enables an attacker to talk directly to the database, thus bypassing the application completely. Successful injection can cause information disclosure as well as ability to add or modify data in the database. (FFIEC IT Examination Handbook)

Spyware
Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code (NIST Glossary)

Supply Chain Attack
Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle. (NIST Glossary)

Threat
Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. (NIST Glossary)

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. (NIST Glossary)

Unauthorized Access
Any access that violates the stated security policy. (NIST Glossary)

Unauthorized Disclosure
An event involving the exposure of information to entities and persons not authorized access to the information. (NIST Glossary)

Verification
Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity's requirements have been correctly defined, or an entity's attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome). (NIST Glossary)

Virtual Private Network (VPN)
A system or technology that uses a public network, usually the Internet, to transmit encrypted data between a private network and a remote authorized user (http://www.dictionary.com/browse/vpn)

Virus
A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use email programs to spread itself to other computers, or even erase everything on a hard disk. (NIST Glossary)

Vulnerability
A weakness in a system, application, or network that is subject to exploitation or misuse. (NIST Glossary)

Worm
A type of malware that attempts to spread itself to as many devices as possible.

Cyber Insurance

how coverage can help

Cyber Risk

The combination of the probability of an event occurring within the realm of an organizations or person's information assets, computer and communication resources and the consequences of that event for an organization or person. (CPMI/IOSCO Cyber Guidance)

Cybersecurity Risk Assessment

A review to determine a business's information technology assets then what threats or weaknesses to cyber-attack exist. This can be completed prior to getting cyber insurance or after a cyber-attack has been handled. It is typically provided by an insurance carrier and or a cyber service provider prior to a cyber coverage being written.

Cyber Risk Profile

The cyber risk actually assumed, measured at a given point in time. (CPMI/IOSCO Cyber Guidance)

First Party Coverage

Insurance coverage for harm to the insured unrelated to a claim brought by a third party.

Forensic Investigation

The application of investigative and analytical techniques to gather and preserve evidence from a digital device impacted by a cyber-attack. (CPMI/IOSCO Cyber Guidance)

Legal Counsel

Whether a company needs to report a cyber breach depends on federal and state laws and regulations; depending on the complexity of the attack legal counsel is recommended and possibly covered by insurance

Third Party Coverage

Coverage for claims against the policyholder by third parties.