Cybersecurity Glossary For

The Inter-American Committee on Ports Organization of American States

Washington, DC

Submitted by
HA – Cyber
HudsonAnalytix, Inc.

Ferry Terminal Building, Suite 300
#2 Aquarium Drive
Camden, NJ 08103
United States of America
www.hudsonanalytix.com

HudsonAnalytix
Complexity made simple.

Date: **1 April 2017**

TO: **Member**
Inter-American Committee on Ports
Organization of American States

FROM: **HudsonAnalytix – Cyber**

REFERENCE: **Glossary on Cybersecurity Terms**

Dear CIP Member:

HudsonAnalytix – Cyber (HA-Cyber), as an Associate member of the CIP, and as an active member of the Technical Advisory Group on Port Safety and Security, is pleased to provide this glossary of commonly used cybersecurity terms for your use and dissemination.

We hope you find this glossary useful as it can provide you, your team, and your partners with a common set of terms that are designed to support shared understanding of cybersecurity across the port industry in our hemisphere.

In addition, should your organization require confidential assistance on the complex subject of cybersecurity, which may include confidential briefings, objective assessments, or training seminars among other needs, we stand ready to support you. My colleague, Andrew Baskin, and I can be reached directly at max.bobys@hudsonanalytix.com or andrew.baskin@hudsonanalytix.com or confidentially any time through the CIP's Washington, DC, office.

Sincerely,

Max J. Bobys
Vice President, Global Strategies

CC: Jorge Duran
Secretariat
Inter-American Committee on Ports
Organization of American States

Term	Definition
Access Control	The discipline, technology, process and/or control for limiting access to an organization's applications, systems, platforms, critical assets, and facilities to authorized entities (e.g., authorized personnel, workflows, and/or data exchanges).
Adware	Specialized advertising software designed to present pop-up messages, windows, or banners on an application that is running. Adware typically captures, tracks, and passes on a user's personal information to third parties without the user's knowledge or agreement. Over time, adware degrades computer performance.
Advanced Persistent Threat (APT)	A cyber attacker or adversary that possesses sophisticated technical capabilities, expertise and resources which allow it to employ a range of tactics, techniques and procedures (e.g., cyber, physical, deception, etc.) to carry out an attack against a targeted victim
Anomaly	Exhibited behavior that is eccentric or inconsistent or deviates from what is considered normal or typical.
Anti-Virus Software	Specialized software that is designed to detect, and, where possible, mitigate malware before it attacks a system. To be effective, anti-virus software must be maintained with the latest updates so that it can effectively identify, isolate, and repair infected files.
Authentication	The process employed to verify the identity and authenticity of a named user, device, system, or application as a condition for gaining access to a protected resource.
Authorization	The process for approving or permitting an individual, application, and/or system to do something.
Availability	The condition for facilitating timely and consistent access to an asset, data set, or information-based system or service.
Backdoor	An undocumented gap in a software application or computer system that allows unauthenticated users access, circumventing security processes.
Backup	A practice designed to save electronic files against inadvertent loss, destruction, damage or unavailability. Methods include high-capacity tape, disc, or cloud-based managed service provided by a third party. Backup efforts should be performed off-site, physically far enough away from the organization's primary site (e.g., administrative headquarters) to reduce the risk of potential environmental risk factors (e.g., earthquake, flood, fire) from impacting both the primary site and the backup site.
Blacklisting Software	Software blacklisting enables the filtering of websites that have been identified and specified as unsafe. Companies sometimes use it to prevent staff from visiting harmful websites, such as those that have been identified as common watering holes. While blacklisting is effective at preventing access to known websites, it is less effective against websites with unknown risks.
Bot	A computer connected to the Internet that has been surreptitiously compromised with malware that direct the computer to perform specific activities directed by a remote administrator with command and control privileges
Brute Force Attack	A methodical process whereby a cyber attacker employs an exhaustive trial and error approach to gaining access to sensitive information. Typically, software is applied to automatically generate massive quantities of

	simultaneous “guesses” in the hopes that one will eventually succeed.
Business Impact Analysis (BIA)	A quantitative analysis that distinguishes critical and non-critical organizational controls, functions, processes, and activities and prioritizes their impact as a result of a compromise or loss of an application, system or platform. Asset criticality and/or sensitivities are then qualitatively and/or quantitatively assessed and the acceptability of the identified risk, including recovery costs, is then determined.
Clear Desk Policy	An established policy that instructs employees to ensure that all desks are cleared at the end of each business day. All files, documents, papers, and media should be appropriately stored, and any sensitive materials should be secured in a manner consistent with established information security policies in order to ensure that no unauthorized individuals can access or view the material outside normal working hours.
Clear Screen Policy	An established policy that instructs employees to ensure that all computer screens are configured to ensure that computer contents, as depicted on electronic displays, are protected from unauthorized viewing. Compliance with this policy requires appropriately configuring the workstation’s screen saver and requiring user identification and password authentication in order to access the system.
Common Operating (Operational) Picture (COP)	Often reflected in a single display (or set of displays), a COP is the consolidation and integration of multiple and relevant activities and technologies that have been configured to collect, analyze, alert on, visualize, and use cybersecurity information, including status and event summary information. It is designed to provide situational awareness, facilitate collaboration and support informed decision-making on cybersecurity matters.
Computer Security Incident	A violation of established computer security policies, including acceptable use policies or other standardized security practices as defined within the organization’s security plans. (See also Incident)
Confidentiality	The protected state achieved by a set of clearly defined rules and authorized restrictions that determine data access and /or disclosure. It includes constraints designed to protect data related to personal privacy and other proprietary information. For an information-based or managed asset, confidentiality is sustained by only allowing authorized and authenticated individuals, processes and/or devices access to it.
Configuration Management	A set of defined processes and controlled activities designed to establish and maintain the integrity of an asset, application, system or platform throughout its lifecycle. Configuration management usually involves documented specifications and procedures for managing information technology and operational technology based systems, assets or platforms. It also provides a common means for tracking and managing the initialization, change, and long-term monitoring of their configurations.
Contingency Plan	A plan, typically expressed as a management procedure, for supporting response activities in the event an asset, application, system, and/or platform capability lost, interrupted or compromised. It is often the first plan stakeholders use to characterize what happened, understand why it occurred, and identify initial mitigation activities. It may also directly reference Company and Facility Security Plans as well as Continuity of Operations and/or Disaster Recovery plans in the event of a major disruption.

Continuous Monitoring	A risk management approach to achieving and sustaining an ongoing awareness of an organization's cybersecurity state. Continuous monitoring collects, analyzes, alerts, visualizes, and supports informational technology, operational technology and security practitioners by identifying anomalous events, vulnerabilities and threats across the organization's operating environment. Its purpose is to support incident response activities and risk management decision-making.
Controls	A set of defined operational policies and/or technical procedures, which may be either manual or automated, that support information technology, operational technology and business processes in the protection of data confidentiality, integrity, and availability.
Cookie	A cookie is a small file downloaded from a website that stores an information packet on the viewer's browser. They are used to store collected data such as login and personal identification information, site behaviors, preferences, and pages viewed. Although convenience-oriented, cookies represent security vulnerabilities. Browsers can be configured to alert on cookies, and users can accept or erase cookies.
Cyber Attack	An event that is launched via the Internet against a target with the intent to deny, disrupt, destroy, or exploit a computer-enabled operating environment. Many cyber attacks are intended to compromise for exploitation purposes or destroy the integrity of targeted data, steal data, or manipulate data for nefarious purposes.
Cyber Ecosystem	The interconnected information infrastructure of an organization's enterprise that facilitates electronic data exchange, communication and interactions among authorized users, applications, systems, platforms, and processes.
Cybersecurity	The capability to protect or defend against unauthorized access to or use of cyberspace from cyber attacks. It consists of the collective measures implemented to defend a computer or computer-enabled system against cyber-enabled threats, such as hackers, Hacktivists, foreign intelligence services, and organized criminal syndicates, among others.
Cybersecurity Architecture	A foundational element supporting an organization's enterprise architecture, cybersecurity architecture consists of the structure and related behaviors of security-focused technologies, processes, systems, operational practices, and personnel responsibilities that align to the organization's defined objectives. See also: enterprise architecture and network architecture.
Cybersecurity Event	A visible incident that occurs in a networked-enabled environment or computer-enabled system related to defined cybersecurity requirements. A cybersecurity event affects data confidentiality, integrity, or availability. See also event.
Cybersecurity Impact	The consequences resulting from a cybersecurity event, which also includes the effect on the cybersecurity capabilities and processes currently in place.
Cybersecurity Plan	A document that identifies and defines the cybersecurity requirements and associated controls necessary for meeting those requirements.
Cybersecurity Policy	A set of principles, measures, and conditions that have been defined to support cybersecurity capabilities and planning across an organization.
Cybersecurity Program	An integrated set of coordinated activities that include governance, strategic planning, executive sponsorship, reporting, and training that is managed to meet defined cybersecurity objectives for an organization. While cybersecurity programs can be implemented at a divisional or practice-level, a higher (enterprise) level can often benefit an organization by coordinating investment

	planning and resource allocation, aligning business processes and procedures, and other resources and capabilities, as may be required.
Cybersecurity Program Strategy	A set of defined actions tailored to the organization's specific cybersecurity capabilities and related performance objectives.
Cybersecurity Risk	The risk to an organization's information technology and/or operational technology-based assets and resources, along with its supporting functions, processes, and reputation as a result of unauthorized access, compromise, exploitation, disruption, denial, or destruction.
Data Breach (Also *" Data Spill")*	The unauthorized access to, exfiltration of, or disclosure of confidential and/or privileged information to a third party or entity that does not have authorization to access, view, or utilize the information.
Denial of Service Attack (DoS)	A type of cyber-enabled attack that results in the temporary or indefinite disruption of authorized access to an application, system, platform or other resource. It typically involves the overloading of a targeted system with an overwhelming number of needless requests, preventing legitimate requests from being addressed. A Distributed Denial of Service (DDoS) attack involves the attacker employing thousands of unique IP addresses to simultaneously carry out an attack.
Dependency Risk	The risk to an organization due to a supplier, vendor, service provider, or other external party on which the delivery of a critical service or key function depends. It is evaluated and measured by the possibility and severity of damage that may be experienced by an application, information technology system, operational technology asset or platform in the event of a compromise.
De-Provisioning	It is a risk management process that defines the revocation or removal of an individual's user identity and associated privileges enabling authenticated access to a facility, application, system, or platform.
Digital Certificate	A form of electronic credentials (e.g., virtual ID or passport) that supports trusted communications and/or business transactions over the Internet. It contains an individual's name, a defined identification (e.g., serial number), expiration date, a copy of the certificate holder's public key (used for encryption and digital signatures), and the digital signature of the certificate-issuing authority for verifying the certificate.
Domain Hijacking	A form of cyber attack that occurs when an attacker takes over a domain registration by blocking the victim's Domain Name Server (DNS) and then illegally replaces it with its own without the authorization of the original registrant.
Encryption	A cryptographic method used to encode a set of information for the purpose of protecting it from unauthorized access or modification prior to sending it to a specified recipient. The recipient then decodes the message using an encryption key.
Enterprise	The highest organizational level of a defined entity.

Enterprise Architecture	The organizational blueprint, design, and description of an organization's entire information technology and operational technology operating environment. It identifies how applications, systems, and platforms are configured, integrated, and connected across internal and external boundaries. It also identifies how they are sustained, how they support the organization's performance objectives, and how they support enterprise-level security capabilities.
Event	An observable occurrence in an asset, application, system, network, or platform. Risk criteria established by the organization inform how some events are characterized and escalated for response and mitigation actions.
Event and Incident Response, Continuity of Operations	The organization and sustainment of an integrated set of plans, procedures, and capabilities that are designed to support the detection, analysis, and response to cybersecurity events. In addition, they are designed to provide guidance to support continued operations through a declared cybersecurity event in a manner that is both aligned and commensurate with the risk to the organization's capabilities and overall objectives.
Exfiltration	The unauthorized removal, transfer or relocation of privileged information from an information system.
Firewall	A hardware device or software link in a network that is designed to inspect data packets (e.g., data traffic) between devices, systems or networks. They can be configured to restrict network traffic according to defined rules.
Cyber Governance	A framework for defining and providing strategic direction and guidance for an organization to ensure that it manages cyber risks while meeting its performance obligations. This involves the appropriate development of policies, as well as allocation of human capital, technical, and financial resources. An effective cyber governance framework assumes active sponsorship of leadership, regulatory-related compliance activities, and alignment of strategic objectives.
Guidelines	Practices that have been developed using references from recognized subject matter experts, authoritative sources and adopted best practices as per community consensus. They are used internally, can be modified/adapted to support maritime transportation specific requirements, or used across an industry.
Hacker	An individual or group of individuals who attempt to access computer-enabled applications, systems, or platforms without appropriate authorization or credentials.
HTTPS	Literally "hypertext transfer protocol." It provides enhanced security when used together with Secure Socket Layer (SSL) security mechanism. It is commonly identified in the first part of a URL (e.g. "http:"). Website visitors are encouraged to look for the "https" when on a webpage that requests logon or payment or personal information.
Identity	A set of attributable characteristics or other defined values (e.g., a randomly generated user identification number) that have been assigned and can be verified in a manner that can distinguish one individual or entity from another.
Incident	An event that arises out of deliberate or accidental circumstances, violating established security policies and/or protocols that can result in harmful consequences to critical assets, applications, systems, platforms, and/or other critical infrastructure elements. A declared incident should warrant activation of incident response resources in order to respond to and contain its impact to the organization, and limit its effects on peripheral systems, platforms, operating environments, or other dependent assets. See also computer security incident and event.

Information Assets	Information or data that the organization has identified and/or classified as essential to the functioning of the mission. This also includes operational data (e.g., process data, command and control information), security plans, network diagrams, confidential designs, intellectual property, customer and financial information, and contracts.
Information Sharing and Communications	Information sharing involves the conscientious exchange of knowledge, expertise, data, and threat information. It assumes pre-existing relationships among internal as well as trusted external third parties (e.g., advisors, partners, law enforcement agencies, port state control authorities, etc.) with whom to share cybersecurity information, including any relevant information about current or emergent cyber threats, threat actors, or maritime industry-specific vulnerabilities, as well as lessons-learned and similar findings.
Information Technology (IT)	Any application, asset, equipment, system, platform, or interconnected system or subsystem that involves the creation, consumption, exchange, dissemination, processing, management, protection, and/or storage of discrete electronic information. In the context of this publication, the definition includes any and all interconnected and/or dependent systems supporting shore-based and shipboard operating environments, and the operational technologies that they support and/or operate.
Insider Threat	Represents a malicious threat to the organization from employees, contractors, or service providers who enjoy trusted privileged access to controlled assets, applications, systems, and/or platforms.
Integrity	In the context of cybersecurity, integrity is the preservation of information authenticity and correctness. It involves the protection of information from improper or unauthenticated alteration or destruction. Information can be in the form of electronic files, commands, instructions and queries.
Internet Protocol (IP) Address	A computer's IP address is a unique series of four 8-bit numbers, separated by periods. It is the identification assigned to all computers and network devices connected to a TCP/IP network. In short, it represents the device's inter-network address. All websites also have an IP address. IP addresses are managed globally by the Internet Assigned Numbers Authority (IANA), and by five regional Internet registries.
Keystroke Logging	Keystroke logging (also referred to as 'keylogging') is the surreptitious recording of computer keyboard keystrokes that are captured as the victim types. Recorded keystrokes are then automatically transmitted to the attacker. This form of attack can be accomplished through either software or hardware. Attackers typically employ keylogging to capture victim user names, passwords and other personal data, such as credit card information.
Least Privilege	A control established by an organization that allows only a minimum level of access for authorized users who require it in order to perform their assigned duties and responsibilities. The purpose of least privilege is to mitigate risks related to the possible misuse and corruption of authorized privileges related to specific functions, processes and/or services.
Logging	Recordkeeping is either a manual or automated process designed to monitor and track user activity and behaviors. As part of an information technology or operational technology system or networked environment, logging is an automated process. Manual processes include the application of physical processes (e.g., manual sign in or use of smart cards) employed to control access to restricted environments, such as vessels, shore-side facilities and office environments. Regular auditing of logs (either manually or through the use of automated tools) supports a critical cyber risk management process that provides situational awareness to security practitioners.

Malware	A generic term for software that compromises the operating system of an IT or networked asset with different types of generic or customized malicious code.
Man-in-the-Middle Attack	A type of attack that involves a threat actor who poses as an online vendor or financial institution and encourages a victim to sign in using their credentials over a Secure Sockets Layer (SSL) connection. The attacker then uses the victim's credentials to access the valid server in order to steal targeted information (e.g., intellectual property, financial data, etc.)
Maturity	In the context of cyber risk management maturity is a measure of the extent to which a process, practice or capability has been adopted within an organization's cybersecurity program and employed across its enterprise.
Monitoring	Monitoring involves the collection, aggregation, recording, analysis, and distribution of specific information sets related to application, system and user behaviors. It supports an ongoing process regarding the identification and analysis of risks to an organization's critical assets, applications, systems, platforms, processes, and personnel.
Multifactor Authentication	The required application of two or more factors a user must employ to authenticate to an application, system or platform. Applicable factors can include: A) something you know (e.g., a unique password); B) something you have (e.g., an identification device); C) something you are (e.g., a biometric, such as a fingerprint); or D) you are where you say you are (e.g., a GPS token or device).
Network	Two or more computer systems or networked devices connected to share information, software, and hardware.
Network architecture	A framework that portrays the overall structure of Information Technology and Operational Technology assets, systems and platforms (including integrated systems). It describes the behavioral rules supporting the communications and interconnectedness among IT and/or OT assets. See also enterprise architecture and cybersecurity architecture.
Operational Resilience	The organization's overall capability to recognize, adapt and respond to risks that affect its critical assets, applications, systems, and/or platforms. A key characteristic of operational risk management, operational resilience is further reinforced and enabled by physical security practices, business continuity and continuity of operations.
Operational Risk	The potential impact on key assets, applications, processes and/or platforms, including their related services, that could result from insufficient capabilities or failed internal processes, systems or technologies, or the deliberate or inadvertent actions of people, or external events.
Operations Technology (OT)	Programmable controls, systems, or devices that are engineered to direct, monitor or interact with systems facilitating physical processes, such as industrial control systems, building management, cargo management, security, engine controls, etc.
Password	A confidential set of alphanumeric characters that is combined to use as a means of authentication for confirming a user's identity in order to access an application, system, platform, or integrated set of systems.
Password Sniffing	A wiretapping tactic that passively collects information from a local area network in order to obtain passwords.
Patch	A small, customized security update issued by a software provider in order to correct known bugs in existing software applications. Most software programs and/or operating systems can be easily configured to automatically check for

	patches or other updates.
Provisioning	The creation, maintenance, and activation of a user profile, including roles and access privileges. An organization should continuously monitor and track access rights to ensure the security of the IT, OT, and communications resources.
Ransomware	Computer malware that installs secretly on a system, encrypts the system's data, prevents access to this data, and holds the data hostage or threatens to publish the data until a ransom is paid.
Risk	A probability or threat of a negative circumstance of event caused by vulnerability and that can addressed through pre-emptive action.
Risk Analysis	The definition and understanding of potential consequences to the organization if certain risks were to come to fruition and a determination of appropriate steps to manage those risks.
Risk Assessment	An identification and evaluation of potential risks that result from a certain activity and a determination of an acceptable level of risk for the organization in question.
Risk Management	The estimate and assessment of potential risks and the establishment of actions or procedures to accept, avoid, control, mitigate, or transfer the consequences of those risks.
Risk Management Program	A defined plan to estimate and assess potential risks and establish actions or procedures to mitigate the consequences of those risks.
Risk Management Strategy	A structured approach toward estimating and assessing potential risks and establishing actions or procedures to mitigate the consequences of those risks. This also includes a defined procedure for periodically reviewing the approach to incorporate new information.
Risk Mitigation	Actions taken to reduce the occurrence and/or negative consequences of a risk.
Risk Mitigation Plan	A defined, documented set of actions to take to reduce the occurrence and/or negative consequences of a risk.
Risk Register	A structured repository of identified risks, with information that supports risk management, such as risk nature, risk consequences, and risk mitigation strategy.
Risk Response	The process of developing strategies to reduce the occurrence and/or negative consequences of a risk. These strategies might include acceptance, avoidance, sharing, or transfer.
Router	A network device connected to two or more data lines in different networks that sends data to the next appropriate network. This function is akin to directing the traffic of the internet.
Script	A simple file that contains programmed commands that can be performed by a computer without user direction.
Secure Software Development	The process of including security best practices as an integral part of software development, including code review, security architectures, and other recognized processes and tools. Programmers and software architects with specific training in secure software development are often deeply involved in

	this process.
Secure Socket Layer (SSL)	The standard encryption system for providing a secure link for data exchanged between a website and a user. A website whose URL begins with https is using this system.
Service Level Agreement (SLA)	A contract between a service provider and a customer, including the services the provider will supply and the performance standards the customer expects these services to meet. The performance standards should include cybersecurity requirements.
Situational Awareness	The awareness of the current state of a system or environment and an understanding of how a change in a variable might alter that current state. This awareness stems from having sufficient and accurate data and the ability to appropriately analyze this data to inform decision-making.
Skimming	A method of theft by which a thief installs a device on, typically, a credit card reader that copies information from the magnetic strip on the credit card. The thief is then able to make purchases or withdraw money from an automated teller machine using the pilfered information.
Social Engineering	The psychological manipulation of people in order to obtain unauthorized access to data or systems. This typically involves tricking an unsuspecting person into bypassing normal security controls and divulging confidential information or providing access to business networks.
Social Networking Websites	An online platform on which users create online profiles and post written words, pictures, videos, and other personal information to share with one another. These platforms facilitate the social connection between and among users with similar interests.
Spam	The use of unsolicited and unwanted bulk messages in an attempt to convince the recipient to purchase something or reveal personal information, such as a phone number, address, or bank account information. Email is the most typical medium for spam, but spam also occurs in other areas, such as text messages, instant messages, and social networking websites.
Sponsorship	Senior management support of cybersecurity objectives across an entire organization, often demonstrated through formal declarations or enacted policies. Full sponsorship also involves senior management review, monitoring, and ongoing improvement of the organization’s cybersecurity program.
Spoofing	An attack by which a malicious actor impersonates as a trusted actor by using a trusted IP address to hide the malicious IP address. An attacker might do this to attack a network host, spread malware, steal information, or other actions that require bypassing access controls.
Spyware	Software that is installed covertly on a computer to allow an attacker to steal data and, possibly, personally identifiable information. This malicious software is often combined with software a user voluntarily downloads and will remain on the user’s computer even if the voluntarily downloaded program is deleted.
Supply Chain & Supply Chain Risk	A sequential set of processes, performed by various otherwise unrelated actors, that result in the creation, transportation, and distribution of a product. The supply chain is typically understood to span across the design, development, production, integration, distribution, and disposal of a product. Supply chain risk is the probability or threat to the supply chain of a negative circumstance of an event caused by vulnerability and that can addressed

	through pre-emptive action.
Threat	An action or event that can, through the exploitation of IT, OT, or communications infrastructure vulnerability, cause a risk to become a loss or damage, with negative consequences for the operations and resources of an organization. This could, for example, occur through unauthorized access, denial of service, or spoofing.
Threat and Vulnerability Management	A structured approach toward estimating and assessing threats and vulnerabilities and establishing actions, plans, or procedures to mitigate the consequences of those threats and vulnerabilities. This approach should incorporate the organization's risk assessments and risk mitigation plans.
Threat Assessment	An evaluation of potential threats, including their severity, and their possible effects on an organization's IT, OT, and communications infrastructure.
Threat Profile	The identification of the characteristics of the complete set of threats to a given function. This combines the organization's set of threat assessments to its IT, OT, and communications infrastructure.
Trojan Horse	Malicious software that tricks victims into believing it is innocuous. Typically spread by some sort of social engineering, many Trojan horses provide unauthorized access to a victim's computer, enabling access to personal information, such as banking information and passwords.
Upstream Dependencies	An external actor who must act or complete a task before a function may be performed or completed. Upstream dependencies include certain operating partners, including suppliers.
URL	A method of denoting where a specific web resource is located on a computer network. Also known as a web address.
URL Obfuscation	An attack by which a scammer directs a victim to what appears to be a safe URL but is in fact a malicious link or site. This type of attack is very common in phishing and spamming emails.
Virus	A type of malware that inserts itself into and infects another computer program, then reproduces itself and infects other programs. Because a virus cannot run by itself, it requires the execution of a host program in order to become active. A virus can spread through email attachments, text messages, internet scams, and even mobile app downloads.
Vishing	An attack by which a scammer solicits private information via social engineering over the telephone. Victims are encouraged to share user names, confidential passwords, private financial account information, or credit card numbers.
Vulnerability	A weakness in an IT, OT, or communications system that an attacker might exploit to gain unauthorized access to that system and the information that system stores.
Whaling Attack	A type of phishing attack that targets executives who have access to valuable corporate information. This type of attack uses social engineering mechanisms, often highly personalized with the target executive's name, job title, or other information, to make the executive believe that he or she needs to divulge important information to the attacked, such as bank account data or customer information.
Whitelisting Software	An application that restricts internet usage to all but a pre-approved list of sites. Parents commonly use this type of software to confine their children's internet usage to only those websites the parents have designated as safe.

Worm	A type of malware that, unlike a virus, can run independently, replicate itself on to other hosts on a network, and cause damage to a computer and network, such as, at a minimum, consuming significant network bandwidth.