DEFINITIONS OF SELECT CYBERSECURITY TERMINOLOGY

NYSAC — NEW YORK STATE ASSOCIATION OF COUNTIES | CTG UNIVERSITY AT ALBANY State University of New York | NEW YORK STATE Homeland Security and Emergency Services | NEW YORK STATE OF OPPORTUNITY. Office of Information Technology Services

The purpose of this document is to provide non-technical leaders with an unofficial, yet useful, "quick reference" of definitions of select cybersecurity terminology to support their understanding of the cybersecurity environment.

This document is not meant to serve as a "how-to" guide or contain all the information necessary for leaders to take action, it is only meant to support an overall understanding of cybersecurity terms.

TABLE # 1: General Cybersecurity Terms

Term	Definition
Cybersecurity	Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. Cybersecurity goes beyond information technology and is the responsibility of every workforce member.
Chief Information Security Officer (CISO)	CISOs are responsible for cybersecurity strategy and are accountable for managing and monitoring the cybersecurity program.
Cybersecurity Governance	Cybersecurity governance is the processes by which decisions are made about cybersecurity risk, and ensures effective programs are established that manage that risk to a degree that is acceptable to the organizational leadership. Governance defines organization-wide priorities, processes, metrics, tolerances, and implementation methods. Cybersecurity governance: • Consists of the executive level decision-making processes and the policies and procedures for overseeing the cybersecurity program • Provides the necessary control and influence an organization's leaders need to have over their cybersecurity programs • Establishes clear definitions and assigns roles and responsibilities • Defines processes, tolerances, metrics, priorities, and implementation methods • Links the organization's cybersecurity programs into decision-making processes that enable the organization's elected leaders to understand and minimize the cybersecurity risks that their organization faces.

Cybersecurity Program	A documented set of your organization's information security policies, procedures, guidelines, and standards. It also includes a collection of effective security management practices and controls, such as risk assessment, awareness, and threat defense. • Create a current profile: An evaluation of your current security status • Conduct a risk assessment • Create a target profile (What additional controls from your "current profile" would you like to add? Who needs to be in the loop about the changes needed to reach the target profile?) • Determine, analyze, and prioritize gaps (What are the gaps between your current and target profile? What action is needed to fill those gaps?) • Bring key stakeholders to the table to confirm an analysis and implementation plan • Implement your plan-of-action. Develop and track metrics to ensure you stay on track.
Cybersecurity Policies	Governance documents which prescribe and proscribe course(s) of action or behavior with respect to the acquisition, deployment, implementation or use of information technology resources.
Cybersecurity Insurance	The insurance policies that address first- and third-party losses as a result of a computer-based attack or malfunction of an organization's information technology systems. There are three main components of cyber insurance: coverage and exclusions, security questionnaires, and rate schedules.
Cybersecurity Training	The process and procedures that involve educating the workforce to understand cybersecurity issues, how to identify risks, and be proactive to mitigate cyber vulnerabilities. 1. Invest in or create a cybersecurity training guide 2. Ensure that cyber training addresses relevant risk assessment findings (see "Cybersecurity Program") 3. Provide interactive training courses 4. Schedule regular testing 5. Compile test results and improve through adjustments to the training program and content 6. Implement and enforce new policies 7. Re-train workforce members on a regular basis 8. Be consistent with all the steps
Cyber Attack	An attack, via cyberspace, targeting an organization's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information

Cyber Breach	An incident wherein information is accessed, stolen or taken from a system without the knowledge or authorization of the system's owner. Note: For legal determination of a breach, counties should consult the definition in the NYS Information Security Breach Notification Act of 2005 *(currently "unauthorized access or acquisition of computerized data which compromises the security, confidentiality or integrity of private information").*
Cyber Framework	A collection of best practices that an organization should follow to manage its cybersecurity risk.

TABLE # 2: CATEGORIES OF CYBER ATTACKS

Term	Definition
Data Loss	Also known as data breach, this can be one of the most damaging cyberattacks, depending on the importance of your data. Your organization's election information, financial data, and PII (personally identifiable information) may be at risk of being exposed or used maliciously. Note: For legal determination of a breach, counties should consult the definition in the NYS Information Security Breach Notification Act of 2005 *(currently "unauthorized access or acquisition of computerized data which compromises the security, confidentiality or integrity of private information").*
Disruptive	This type of attack is designed to disrupt or impair your organization's ability to function properly. Examples of this type of attack include ransomware and Distributed Denial of Service (DDoS). This type of attack can last days or weeks. In the case of a disruptive ransomware attack, an unprepared organization may find themselves with no choice but to pay the ransom.
Destructive	In this attack, adversaries such as malicious insiders and hacktivists deliver destructive attacks designed to harm an organization by damaging its IT infrastructure or data. A destructive attack could be as simple as deleting data or wiping all the software off a computer.
Disinformation	This attack spreads false information about a workforce member or an organization's activities and inflicts reputational, financial, and even legal damage. Malicious disinformation about an organization can spread quickly through many different social and digital channels.

TABLE # 3: Examples of Cyber Attacks

Term	Definition
Malware	Malware is an umbrella term for all types of malicious software, from worms and viruses to spyware and ransomware. Two common sources of malware infection for an organization are workforce members visiting compromised or malicious websites and workforce members engaging with phishing emails, clicking links or opening attachments. Once malware gets a foothold, it can be difficult and expensive to remove. Popular malware: • Remote Access Trojan: Allows the attacker "backdoor" entry into systems. • Ransomware: Encrypts data until a ransom is paid. • Spyware: Logs key strokes to gather data such as passwords. • Adware: Exposes the victim to potentially malicious ads. • Worm: Malicious program which self-replicates, spreading without user interaction. • Virus: Malicious programs which must be activated in some way.
Phishing	A digital form of social engineering that uses authentic-looking—but bogus—e-mails to request information from users or direct them to a fake web site that requests information
Social Engineering	The practice of exploiting human psychology instead of technical system vulnerabilities. This type of attack is difficult to defend against because it focuses on workforce members who may be unprepared for it. Social engineering leverages individuals' traits such as a desire to be helpful or productive to get them to inappropriately divulge information or provide access to facilities. One step organizations may take to defend against social engineering is to educate their workforce on what types of information can or cannot be disclosed and to whom.
Distributed Denial of Service - DDoS	This attack makes a service such as a website unusable by "flooding" it with malicious traffic or data from multiple sources. This in turn renders legitimate organizational communications slow or impossible and may have other undesirable effects.
Spoofing	Mimicking legitimate network traffic for a malicious purpose. For example, sending an email disguised to look like it is coming from someplace besides its actual origin. In this example, the IP address may be changed, and the email address may mimic a known domain.
APT (Advanced Persistent Threat)	An adversary with sophisticated levels of expertise and significant resources that gains access using multiple attack vectors (e.g., cyber vulnerabilities, physical, and social engineering) to generate opportunities to achieve its objectives. These attacks remain undetected for an extended period of time and can prove difficult to eradicate (persistent).

Business E-mail Compromise	Business email compromise (BEC) is a type of email cyber-crime in which an attacker targets a business to defraud the company. The BEC attack may use a compromised email account within the organization or an external "look-alike" account that is very similar to the organization's email addressing scheme. From there, the adversary may impersonate an executive or finance team member to submit false invoices, initiate fraudulent wire transfers or steal data.

TABLE # 4: CYBER PROTECTION TERMS

Term	Definition
Encryption	A technique used to protect the confidentiality of information. The process transforms ("encrypts") readable information into unintelligible text through an algorithm and associated cryptographic key(s).
Network Security	Sets forth who can access your network and once on the network, controls access to data and functions.
Multi Factor Authentication	Using more than one of the following factors to authenticate a system: • Something you know (e.g., user-ID, password, personal identification number (PIN), or passcode) • Something you have (e.g., a one-time password authentication token, 'smart card') • Something you are (e.g., fingerprint, retina scan)
Endpoint Security	A holistic approach to protecting your organization's end-user devices, such as laptops, desktops, and smartphones, whether on the network or by accessing it remotely. Endpoint security leverages controls such as anti-malware software, web filtering, and host-based firewalls to reduce the risk that end-user devices will be entry points for security threats.
Virtual Private Network (VPN)	Extends a private network across a public network and enables users to securely send and receive data across shared or public networks as if their computing devices were directly connected to the private network
Firewall and Intrusion Prevention Systems	These defensive technologies can be positioned at the "edge" of your network (i.e., on your Internet connection) and/or installed on endpoints such as end-user computers. They are designed to monitor network traffic and detect anomalies on several levels that could be indicative of an attack. When this type of traffic is detected, it is not permitted, and IT personnel may be notified of a potential attack.
Zero Trust	The security concept that organizations should not automatically trust anything inside or outside their perimeters and instead must verify anything and everything each time it tries to connect to its systems/data before granting access.

Data Backups	A copy of the important data on a device, a data backup provides an option for restoring a device quickly in the event of data loss (it is important to note that an archive is different than a backup). Effective backup processes include: 1. Periodically and automatically creating a copy of your important data 2. Storing it "offline, in a separate location from the original data" 3. Testing restoration processes periodically to ensure the integrity of your backups 4. Physically securing or encrypting backups, and tracking their location to prevent unauthorized use or access.
Content Filter/ Access Gateway	Technology that prevents user access to questionable or malicious websites and or email messages.

References

Excerpts for the definitions of the above terms were gathered from the following documents and agencies:

Center for Internet Security, Managing Cyber Threats through Effective Governance
https://www.cisecurity.org/white-papers/managing-cyber-threats-through-effective-governance/

Cyber and Infrastructure Security Agency Security Tip (ST04-001)
https://us-cert.cisa.gov/ncas/tips/ST04-001

Cyber Florida at the University of South Florida, Cybersecurity for Local Government
https://flmanagers.com/wp-content/uploads/2021/01/Cybersecurity-for-Local-Government-Guide.pdf

Cybersecurity Framework, NIST
https://www.nist.gov/cyberframework

Cybersecurity & Infrastructure Security Agency
https://www.cisa.gov/cybersecurity

Cybersecurity & Infrastructure Security Agency,
https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Workforce%20Training%20Guide%207.28.21%20508c.pdf

Cybint Solutions, 25 Cybersecurity Terms
https://www.cybintsolutions.com/20-cyber-security-terms-that-you-should-know/

Journal of Cybersecurity, Oxford Academy
https://academic.oup.com/cybersecurity/article/5/1/tyz002/5366419

National Association of Counties, NACo Cyber Security Priorities & Best Practices
https://www.naco.org/resources/naco-cyber-security-priorities-and-best-practices

National Institute of Standards & Technology, Computer Security Resource Center
https://csrc.nist.gov/glossary?index=E

New York State Office of Information Technology Services
https://its.ny.gov/

Norton, Data Backups
https://us.norton.com/internetsecurity-how-to-the-importance-of-data-back-up.html

NYSBOE, Cybersecurity Requirements for Board of Elections
https://www.elections.ny.gov/NYSBOE/download/law/Part6220_ElectionsCyberReg.pdf

Tech Networks of Boston, Cybersecurity Terms You Need to KNow
https://techboston.com/nonprofit-cybersecurity-cheat-sheet/

This document was prepared by:

New York State Association of Counties
https://www.nysac.org/

Center for Technology in Government, University at Albany
https://www.ctg.albany.edu/

NYS Division of Homeland Security and Emergency Services
http://www.dhses.ny.gov/

NYS Office of Information Technology Services
https://its.ny.gov/