radian national training

Radian National Training On Air Podcast

Cybersecurity Definitions Quick Reference Guide

Awareness

- **Cybersecurity** - Measures that are used to protect the confidentiality, integrity and availability of systems and information.
- **Cyberthreat** - Any circumstance or event with the potential to harm systems or information.
- **Vulnerability** – When there is a flaw or weakness in a system or network that could be exploited to cause damage or allow an attacker to manipulate the system in some way.
- Vulnerability is different from a "cyberthreat" in that while a cyberthreat may involve an outside element, computer system vulnerabilities exist on the asset (computer) to begin with. Additionally, they are not usually the result of an intentional effort by an attacker—though cybercriminals will leverage these flaws in their attacks, leading some to use the terms interchangeably.
- **Cyberrisk** – Refers to any risk of financial loss, disruption or damage to the reputation of an organization resulting from the failure of its information technology systems.

Activity

- **Hacking** – Gaining of unauthorized access to data in a system or computer. Also, the misuse of a computer or system to break the security of another computing system to steal data, corrupt systems or files, commandeer the environment or disrupt data–related activities in any way.
- **Exploit** – A malicious application or script that can be used to take advantage of a computer's vulnerability.

Incident

- ***Data Breach** - Security incident in which malicious insiders or external attackers gain unauthorized access to confidential data or sensitive information such as medical records, financial information or personally identifiable information (PII). Data breaches are one of the most common and most costly types of cybersecurity incidents.
- **Breach** - When a hacker successfully exploits a vulnerability in a computer or device, and gains unauthorized access to its files and network.
- *Data breach definition and classification may vary from state to state

Attacks

- **DDoS** – Stands for Distributed Denial of Service – a form of cyberattack. This attack aims to make a service such as a website unusable by "flooding" it with malicious traffic or data from multiple sources (often botnets).
- **SIDOS** – Self Imposed Denial of Service: When security rules are set too strict and this prevents legitimate business objectives from being achieved.
- **Cyberattack** – Any attempt to expose, alter, destroy, steal, or gain unauthorized access to, or make unauthorized use of an asset.
- **Social Engineering** – Technique used to manipulate and deceive people to gain sensitive and private information. Scams based on social engineering are built around how people think and act. Once a hacker understands what motivates a person's actions, they can usually retrieve exactly what they're looking for – like financial data and passwords.
- **Phishing** or **Spear Phishing** – Technique used by hackers to obtain sensitive information. For example, using hand–crafted email messages designed to trick people into divulging personal or confidential data such as passwords and bank account information.

Malware

- **Malware** – Broad name for any type of malicious software designed to cause harm or damage to a computer, server, client or computer network and infrastructure without end–user knowledge. Cyber-attackers create, use and sell malware for many different reasons, but it is most frequently used to steal personal, financial or business information. Malware is an umbrella term that describes all forms of malicious software designed to wreak havoc on a computer. Common forms include: viruses, trojans, worms and ransomware.
- **Ransomware** – Ransomware is a type of malware designed to extort victims for financial gain. Once activated, ransomware prevents users from interacting with their files, applications or systems until a ransom is paid, usually in the form of an untraceable currency like Bitcoin.
- **Bots** – A group of automated programs, like worms, that all are directed by a single authority. BOTS are used across the Internet for both legitimate and elicit purposes. Google collects all that wonderful website data using Bots which crawl the internet looking for new websites to index. Bots account for 52% of all the Internet traffic today. There's more machine–to–machine activity than there are people–to–machine.
- **Virus** – a type of malware aimed to corrupt, erase or modify information on a computer before spreading to others.
- **Worm** – A piece of malware that can replicate itself in order to spread the infection to other connected computers.
- **Trojan** – A Trojan horse, or Trojan, is a type of malicious code or software that looks legitimate but can take control of your computer. It is designed to damage, disrupt, steal or inflict harm on your data or network.

Defense

- **Firewall** – this is a defensive technology designed to keep the bad guys out.
- **Encryption** – The process of encoding data to prevent theft by ensuring the data can only be accessed with a key.
- **Access Measures** – Include authentication controls, biometrics, timed access and virtual private network (VPN).
- **Workstation Defense**: Measures include anti-virus and anti-spam software.
- **Pen-testing** – Short for "penetration testing," this practice is a means of evaluating security using hacker tools and techniques with the aim of discovering vulnerabilities and evaluating security flaws.
- **Data Protection** - Methods include hashing, secure data transmission, and encrypted backups.
- **Perimeter Defense** - Includes firewalls, intrusion detection systems and prevention systems.