Glossary

Cybersecurity

Terms and definitions from Course 1

A

Adversarial artificial intelligence: A technique that manipulates artificial intelligence (AI) and machine learning (ML) technology to conduct attacks more efficiently

Antivirus software: A software program used to prevent, detect, and eliminate malware and viruses

Asset: An item perceived as having value to an organization

Availability: The idea that data is accessible to those who are authorized to access it

B

Business Email Compromise (BEC): A type of phishing attack where a threat actor impersonates a known source to obtain financial advantage

C

Cloud security: The process of ensuring that assets stored in the cloud are properly configured and access to those assets is limited to authorized users

Compliance: The process of adhering to internal standards and external regulations

Computer virus: Malicious code written to interfere with computer operations and cause damage to data and software

Confidentiality: Only authorized users can access specific assets or data

Confidentiality, integrity, availability (CIA) triad: A model that helps inform how organizations consider risk when setting up systems and security policies

Cryptographic attack: An attack that affects secure forms of communication between a sender and intended recipient

Cybersecurity (or security): The practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorized access or criminal exploitation

D

Database: An organized collection of information or data

Data point: A specific piece of information

H

Hacker: Any person who uses computers to gain access to computer systems, networks, or data

Hacktivist: A person who uses hacking to achieve a political goal

Health Insurance Portability and Accountability Act (HIPAA): A U.S. federal law established to protect patients' health information

I

Integrity: The idea that the data is correct, authentic, and reliable

Internal threat: A current or former employee, external vendor, or trusted partner who poses a security risk

Intrusion detection system (IDS): An application that monitors system activity and alerts on possible intrusions

L

Linux: An open-source operating system

Log: A record of events that occur within an organization's systems

M

Malware: Software designed to harm devices or networks

N

National Institute of Standards and Technology (NIST) Cyber Security Framework (CSF): A voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk

Network protocol analyzer (packet sniffer): A tool designed to capture and analyze data traffic within a network

Network security: The practice of keeping an organization's network infrastructure secure from unauthorized access

O

Open Web Application Security Project (OWASP): A non-profit organization focused on improving software security

Order of volatility: A sequence outlining the order of data that must be preserved from first to last

P

Password attack: An attempt to access password secured devices, systems, networks, or data

Personally identifiable information (PII): Any information used to infer an individual's identity

Phishing: The use of digital communications to trick people into revealing sensitive data or deploying malicious software

Physical attack: A security incident that affects not only digital but also physical environments where the incident is deployed

Physical social engineering: An attack in which a threat actor impersonates an employee, customer, or vendor to obtain unauthorized access to a physical location

Privacy protection: The act of safeguarding personal information from unauthorized use

Programming: A process that can be used to create a specific set of instructions for a computer to execute tasks

Protected health information (PHI): Information that relates to the past, present, or future physical or mental health or condition of an individual

Protecting and preserving evidence: The process of properly working with fragile and volatile digital evidence

S

Security architecture: A type of security design composed of multiple components, such as tools and processes, that are used to protect an organization from risks and external threats

Security controls: Safeguards designed to reduce specific security risks

Security ethics: Guidelines for making appropriate decisions as a security professional

Security frameworks: Guidelines used for building plans to help mitigate risk and threats to data and privacy

Security governance: Practices that help support, define, and direct security efforts of an organization

Security information and event management (SIEM): An application that collects and analyzes log data to monitor critical activities in an organization

Security posture: An organization's ability to manage its defense of critical assets and data and react to change

Sensitive personally identifiable information (SPII): A specific type of PII that falls under stricter handling guidelines

Social engineering: A manipulation technique that exploits human error to gain private information, access, or valuables

Social media phishing: A type of attack where a threat actor collects detailed information about their target on social media sites before initiating the attack

Spear phishing: A malicious email attack targeting a specific user or group of users, appearing to originate from a trusted source

SQL (Structured Query Language): A programming language used to create, interact with, and request information from a database

Supply-chain attack: An attack that targets systems, applications, hardware, and/or software to locate a vulnerability where malware can be deployed

T

Technical skills: Skills that require knowledge of specific tools, procedures, and policies

Threat: Any circumstance or event that can negatively impact assets

Threat actor: Any person or group who presents a security risk

Transferable skills: Skills from other areas that can apply to different careers

U

USB baiting: An attack in which a threat actor strategically leaves a malware USB stick for an employee to find and install to unknowingly infect a network

V

Virus: refer to “computer virus”

Vishing: The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source

W

Watering hole attack: A type of attack when a threat actor compromises a website frequently visited by a specific group of users