Global Certificate in International Risk Management

Cybersecurity and Information Security.

Cybersecurity and Information Security Key Terms and Vocabulary

Cybersecurity: Cybersecurity refers to the practice of protecting systems, networks, and data from digital attacks. It involves implementing measures to prevent unauthorized access, exploitation, or damage to information systems.

Information Security: Information security focuses on protecting the confidentiality, integrity, and availability of data. It encompasses a broader scope than cybersecurity and includes physical security, personnel security, and processes to safeguard information assets.

Threat: A threat is a potential danger that can exploit a vulnerability in a system or network, leading to a security breach. Threats can be intentional (e.g., malicious hackers) or unintentional (e.g., natural disasters).

Vulnerability: A vulnerability is a weakness in a system or network that can be exploited by a threat actor. Vulnerabilities can be due to software flaws, misconfigurations, or inadequate security controls.

Risk: Risk is the likelihood of a threat exploiting a vulnerability and the impact it may have on an organization's assets. Risk management involves identifying, assessing, and mitigating risks to protect information assets.

Attack: An attack is an intentional action by a threat actor to compromise the security of a system or network. Attacks can take various forms, such as malware, phishing, denial of service, or social engineering.

Malware: Malware is malicious software designed to disrupt, damage, or gain unauthorized access to a computer system. Examples of malware include viruses, worms, Trojans, ransomware, and spyware.

Phishing: Phishing is a type of social engineering attack where attackers trick individuals into providing sensitive information, such as passwords or financial details, by posing as a trustworthy entity in electronic communication.

Denial of Service (DoS): A denial of service attack aims to disrupt the normal operation of a system or network by overwhelming it with a flood of traffic, making it inaccessible to legitimate users.

Social Engineering: Social engineering is a technique used by attackers to manipulate individuals into divulging confidential information or performing actions that compromise security. It relies on psychological manipulation rather than technical exploits.

Firewall: A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between an internal network and external networks, such as the internet.

Intrusion Detection System (IDS): An IDS is a security tool that monitors network or system activities for malicious behavior or policy violations. It alerts security administrators when suspicious activities are detected, enabling timely response to potential threats.

Intrusion Prevention System (IPS): An IPS is a security device that not only detects but also actively blocks malicious activities on a network or system. It can automatically respond to threats by blocking communication or initiating other preventive measures.

Encryption: Encryption is the process of converting data into a secure format that can only be read with a decryption key. It ensures that sensitive information remains confidential and secure during transmission or storage.

Public Key Infrastructure (PKI): PKI is a set of policies, procedures, and technologies for managing digital certificates and encryption keys. It enables secure communication and authentication in a networked environment.

Multi-factor Authentication (MFA): MFA is a security mechanism that requires users to provide multiple forms of identification to access a system or application. It typically involves a combination of passwords, biometrics, tokens, or other authentication factors.

Incident Response: Incident response is the process of detecting, responding to, and recovering from security incidents. It involves identifying the nature and scope of an incident, containing its impact, and restoring normal operations.

Penetration Testing: Penetration testing, also known as ethical hacking, is a security assessment technique that simulates real-world cyber attacks to identify vulnerabilities in a system or network. It helps organizations proactively improve their security posture.

Zero-Day Vulnerability: A zero-day vulnerability is a previously unknown security flaw in software or hardware that is exploited by attackers before a fix or patch is available. Zero-day attacks can be particularly damaging as they leave no time for mitigation.

Security Policy: A security policy is a set of rules, guidelines, and procedures that define the security requirements and expectations within an organization. It outlines the responsibilities of users, administrators, and stakeholders in maintaining a secure environment.

Compliance: Compliance refers to the adherence to laws, regulations, industry standards, and organizational policies related to information security. Compliance measures ensure that organizations meet legal requirements and industry best practices to protect sensitive data.

Security Awareness Training: Security awareness training educates users about cybersecurity best practices, threats, and their role in maintaining a secure environment. It aims to enhance user awareness and reduce the likelihood of security incidents caused by human error.

Data Loss Prevention (DLP): DLP is a strategy and technology used to prevent the unauthorized disclosure or leakage of sensitive data. It involves monitoring, detecting, and blocking the transmission of confidential

information outside of authorized channels.

Blockchain: Blockchain is a distributed ledger technology that enables secure and transparent transactions without the need for intermediaries. It uses cryptographic techniques to ensure the integrity and immutability of data stored in blocks.

Cryptography: Cryptography is the practice of securing communication and data through the use of mathematical algorithms. It involves encryption, decryption, digital signatures, and other techniques to protect information from unauthorized access.

Virtual Private Network (VPN): A VPN is a secure network connection that encrypts data transmitted between a user's device and a private network, such as a corporate network or the internet. It ensures confidentiality and privacy by creating a secure tunnel for data transfer.

Endpoint Security: Endpoint security focuses on protecting individual devices, such as computers, smartphones, and tablets, from cyber threats. It includes antivirus software, firewalls, intrusion detection, and other measures to secure endpoints.

Cloud Security: Cloud security involves protecting data, applications, and infrastructure hosted in cloud environments. It addresses unique challenges such as shared responsibility models, data privacy, compliance, and securing cloud-based services.

Internet of Things (IoT) Security: IoT security is concerned with securing interconnected devices and systems that communicate over the internet. It addresses vulnerabilities in IoT devices, data privacy, network security, and the integrity of IoT ecosystems.

Threat Intelligence: Threat intelligence is information about potential threats, vulnerabilities, and cyber attacks that can help organizations proactively defend against security incidents. It includes data on emerging threats, attack techniques, and threat actors.

Artificial Intelligence (AI) in Security: AI is increasingly used in cybersecurity to automate threat detection, response, and decision-making processes. AI-powered tools can analyze large volumes of data, identify patterns, and enhance security operations.

Machine Learning: Machine learning is a subset of AI that enables systems to learn and improve from data without being explicitly programmed. It is used in cybersecurity for anomaly detection, threat prediction, and behavioral analysis.

Security Operations Center (SOC): A SOC is a centralized facility that monitors, detects, analyzes, and responds to security incidents in real-time. It provides round-the-clock surveillance and incident response capabilities to protect an organization's assets.

Red Team vs. Blue Team: In cybersecurity, red teams simulate attackers to test an organization's defenses, while blue teams defend against these simulated attacks. Red team engagements help identify weaknesses, while blue team activities focus on strengthening security controls.

Ransomware: Ransomware is a type of malware that encrypts a victim's data and demands payment for decryption. It is a growing threat to organizations and individuals, often leading to data loss, financial losses, and operational disruptions.

Supply Chain Security: Supply chain security focuses on securing the flow of goods, services, and information across the supply chain. It addresses risks such as counterfeit products, data breaches, and disruptions that can impact the security of products or services.

Security Incident: A security incident is an event that compromises the confidentiality, integrity, or availability of information assets. Incidents can range from minor policy violations to major security breaches that require immediate response and remediation.

Business Continuity Planning: Business continuity planning involves developing strategies and procedures to ensure essential business functions can continue in the event of a disruption. It includes disaster recovery, crisis management, and continuity of operations planning.

Mobile Security: Mobile security focuses on protecting smartphones, tablets, and other mobile devices from security threats. It includes measures such as device encryption, secure app development, mobile device management, and secure communication protocols.

Authentication: Authentication is the process of verifying the identity of a user or device before granting access to a system or application. It typically involves providing credentials, such as passwords, biometrics, tokens, or digital certificates.

Authorization: Authorization is the process of granting or denying access to resources based on a user's authenticated identity and permissions. It ensures that users can only access the information and perform the actions they are authorized to do.

Network Security: Network security focuses on securing the communication infrastructure of an organization, including routers, switches, firewalls, and network devices. It aims to protect data in transit, prevent unauthorized access, and detect network threats.

Incident Response Plan: An incident response plan outlines the steps and procedures to follow when a security incident occurs. It includes roles and responsibilities, communication protocols, containment measures, recovery processes, and lessons learned for future improvements.

Regulatory Compliance: Regulatory compliance refers to the adherence to laws, regulations, and industry standards related to information security. Compliance requirements vary by industry and geography and may include data protection, privacy, and reporting obligations.

Security Audit: A security audit is a systematic evaluation of an organization's security controls, policies, and procedures to assess compliance with security requirements. It helps identify weaknesses, gaps, and areas for improvement in the security posture.

Incident Classification: Incident classification categorizes security incidents based on severity, impact, and type to prioritize response and allocate resources effectively. Common classifications include low, medium,

high, critical, and informational incidents.

Root Cause Analysis: Root cause analysis is a methodical process to identify the underlying reasons for a security incident or problem. It helps organizations understand the factors contributing to incidents and implement corrective actions to prevent recurrence.

Security Awareness Program: A security awareness program educates employees, contractors, and stakeholders about cybersecurity risks, best practices, and policies. It aims to foster a security-conscious culture and reduce the human factor in security incidents.

Policy Enforcement: Policy enforcement ensures that security policies, procedures, and guidelines are followed consistently across an organization. It may involve technical controls, user training, monitoring, and enforcement mechanisms to uphold security standards.

Security Controls: Security controls are safeguards, countermeasures, or protective measures implemented to mitigate risks and protect information assets. They can be administrative, technical, or physical controls designed to address specific security requirements.

Data Privacy: Data privacy refers to the protection of personal information and sensitive data from unauthorized access, use, or disclosure. It encompasses legal requirements, ethical principles, and organizational practices to safeguard individuals' privacy rights.

Security Architecture: Security architecture is the design and structure of security controls, technologies, and processes within an organization. It defines how security requirements are implemented to protect information assets and support business objectives.

Security Incident Response Team (SIRT): A SIRT is a dedicated team responsible for managing and responding to security incidents within an organization. It coordinates incident response activities, communicates with stakeholders, and ensures timely resolution of security events.

Security Operations: Security operations involve the day-to-day management, monitoring, and maintenance of security controls and processes. It includes activities such as incident detection, analysis, response, reporting, and continuous improvement of security practices.

Security Governance: Security governance encompasses the strategic management of security policies, risk management, compliance, and oversight within an organization. It establishes accountability, decision-making processes, and controls to guide security initiatives.

Security Awareness: Security awareness is the knowledge, understanding, and behavior of individuals regarding cybersecurity risks and best practices. It aims to empower users to recognize and respond to security threats, ultimately enhancing the organization's security posture.

Emerging Threats: Emerging threats are new or evolving risks that pose challenges to cybersecurity defenses. They may exploit novel attack vectors, vulnerabilities, technologies, or trends, requiring organizations to adapt their security strategies and controls.

Security Incident Report: A security incident report documents the details, impact, and response to a security incident. It provides a comprehensive account of the incident, including timelines, evidence, actions taken, lessons learned, and recommendations for improvement.

Security Awareness Campaign: A security awareness campaign is a coordinated effort to raise awareness, educate, and engage users in cybersecurity best practices. It may include training sessions, newsletters, posters, quizzes, simulations, and other activities to promote security awareness.

Security Risk Assessment: A security risk assessment evaluates the threats, vulnerabilities, and potential impacts on an organization's information assets. It helps identify and prioritize risks, assess controls, and develop mitigation strategies to reduce security risks.

Security Incident Handling: Security incident handling involves the detection, analysis, containment, eradication, and recovery from security incidents. It follows predefined procedures, communication protocols, and best practices to minimize the impact of incidents on an organization.

Security Awareness Training Program: A security awareness training program provides instruction, resources, and activities to educate users about cybersecurity risks and best practices. It aims to empower users to recognize, prevent, and respond to security threats effectively.

Security Posture: Security posture refers to an organization's overall security readiness, resilience, and effectiveness in protecting information assets. It reflects the strength of security controls, policies, processes, and culture in mitigating security risks and threats.

Security Incident Response Plan: A security incident response plan outlines the procedures, roles, responsibilities, and actions to take in response to a security incident. It provides a structured approach to managing incidents, containing threats, and restoring normal operations.

Security Incident Detection: Security incident detection involves monitoring, analyzing, and identifying signs of unauthorized or malicious activities in an organization's systems, networks, or applications. Early detection enables prompt response and mitigation of security threats.

Security Incident Response Process: The security incident response process defines the steps, workflows, and decision-making criteria for managing security incidents. It guides incident responders in detecting, analyzing, containing, eradicating, recovering, and documenting incidents effectively.

Security Incident Response Team (SIRT) Role: The SIRT plays a crucial role in managing security incidents, coordinating response activities, communicating with stakeholders, and restoring normal operations. It comprises experts in incident detection, analysis, containment, and recovery to address security events effectively.

Security Incident Recovery: Security incident recovery involves restoring affected systems, data, and services to their normal state after a security incident. It includes cleanup, remediation, validation, and post-incident analysis to ensure the organization's resilience and readiness for future incidents.

Security Incident Response Plan Testing: Testing the security incident response plan involves simulating

security incidents, conducting tabletop exercises, and evaluating the effectiveness of response procedures. It helps identify gaps, refine processes, train responders, and enhance the organization's preparedness for real incidents.

Security Incident Response Tools: Security incident response tools assist organizations in detecting, analyzing, reporting, and responding to security incidents. These tools include security information and event management (SIEM) systems, endpoint detection and response (EDR) solutions, forensic analysis tools, and incident response platforms.

Security Incident Response Metrics: Security incident response metrics measure the performance, effectiveness, and efficiency of incident response activities. They track key performance indicators (KPIs), such as mean time to detect (MTTD), mean time to respond (MTTR), incident resolution time, and incident response team productivity, to evaluate the organization's incident response capabilities.

Security Incident Response Playbook: A security incident response playbook is a predefined set of response procedures, checklists, and workflows for addressing specific types of security incidents. It guides incident responders in following consistent, structured, and effective response steps to mitigate threats, contain impacts, and restore normal operations.

Security Incident Response Communication: Security incident response communication involves informing stakeholders, management, employees, customers, partners, and regulatory authorities about a security incident. It includes timely notifications, updates, alerts, advisories, and status reports to ensure transparency, accountability, and coordinated response efforts.

Security Incident Response Team Coordination: Effective coordination among members of the security incident response team is essential for managing security incidents efficiently and minimizing their impact. It involves clear role assignments, communication protocols, decision-making processes, collaboration tools, and regular training to ensure a coordinated and cohesive response to security events.

Security Incident Response Documentation: Security incident response documentation includes logs, reports, evidence, findings, analysis, and actions taken during the response to a security incident. It provides a comprehensive record of the incident, response activities, lessons learned, recommendations, and improvements for future incident handling.

Security Incident Response Lessons Learned: Security incident response lessons learned are insights, observations, and recommendations derived from analyzing security incidents after they occur. They help organizations identify weaknesses, gaps, and opportunities for improvement in incident response processes, tools, training, and coordination to enhance their readiness for future incidents.

Security Incident Response Best Practices: Security incident response best practices are guidelines, recommendations, and standards for effective incident detection, analysis, containment, eradication, recovery, and post-incident activities. They help organizations establish robust incident response capabilities, improve response efficiency, and reduce the impact of security incidents on their operations, reputation, and stakeholders.