# Today’s Security Professional

**Exam Essentials**

**The three core objectives of cybersecurity are confidentiality, integrity, and availability.** Confidentiality ensures that unauthorized individuals are not able to gain access to sensitive information. Integrity ensures that there are no unauthorized modifications to information or systems, either intentionally or unintentionally. Availability ensures that information and systems are ready to meet the needs of legitimate users at the time those users request them.

**Nonrepudiation prevents someone from denying that they took an action.** Nonrepudiation means that someone who performed some action, such as sending a message, cannot later deny having taken that action. Digital signatures are a common example of nonrepudiation. They allow anyone who is interested to confirm that a message truly originated with its purported sender.

**Security controls may be categorized based on their mechanism of action and their intent.** Controls are grouped into the categories of managerial, operational, physical, and technical based on the way that they achieve their objectives. They are divided into the types of preventive, detective, corrective, deterrent, compensating, and directive based on their intended purpose.

**Data breaches have significant and diverse impacts on organizations.** When an organization suffers a data breach, the resulting data loss often results in both direct and indirect damages. The organization suffers immediate financial repercussions due to the costs associated with the incident response, as well as long-term financial consequences due to reputational damage. This reputational damage may be difficult to quantify, but it also may have a lasting impact. In some cases, organizations may suffer operational damage if they experience availability damages, preventing them from accessing their own information.

**Data must be protected in transit, at rest, and in use.** Attackers may attempt to eavesdrop on network transmissions containing sensitive information. This information is highly vulnerable when in transit unless protected by encryption technology. Attackers also might attempt to breach data stores, stealing data at rest. Encryption serves to protect stored data as well as data in transit. Data is also vulnerable while in use on a system and should be protected during data processing activities.

**Data loss prevention systems block data exfiltration attempts.** DLP technology enforces information handling policies to prevent data loss and theft. DLP systems may function at the host level, using software agents to search systems for the presence of sensitive information. They may also work at the network level, watching for transmissions of unencrypted sensitive information. DLP systems detect sensitive information using pattern-matching technology and/or digital watermarking.

**Data minimization reduces risk by reducing the amount of sensitive information that we maintain.** In cases where we cannot simply discard unnecessary information, we can protect information through deidentification and data obfuscation. The tools used to achieve these goals include hashing, tokenization, and masking of sensitive fields.

# Cybersecurity Threat Landscape

**Exam Essentials**

**Threat actors differ in several key attributes.** We can classify threat actors using four major criteria. First, threat actors may be internal to the organization, or they may come from external sources. Second, threat actors differ in their level of sophistication and capability. Third, they differ in their available resources and funding. Finally, different threat actors have different motivations and levels of intent.

**Threat actors come from many different sources.** Threat actors may be very simplistic in their techniques, such as unskilled attackers using exploit code written by others, or quite sophisticated, such as the advanced persistent threat posed by nation-state actors and organized crime. Hacktivists may seek to carry out political agendas, whereas competitors may seek financial gain. Employees and other users may pose an insider threat by working from within to attack your organization. The use of unapproved shadow IT systems may also expose your data to risk.

**Attackers have varying motivations for their attacks.** Attackers may be motivated by many different drivers. Common motivations for attack include data exfiltration, espionage, service disruption, blackmail, financial gain, philosophical or political beliefs, revenge, disruption and chaos, or war. Some attackers may believe they are behaving ethically and acting in the best interests of society.

**Attackers exploit different vectors to gain initial access to an organization.** Attackers may attempt to gain initial access to an organization remotely over the Internet, through a wireless connection, or by attempting direct physical access. They may also approach employees over email or social media. Attackers may seek to use removable media to trick employees into unintentionally compromising their networks, or they may seek to spread exploits through cloud services. Sophisticated attackers may attempt to interfere with an organization's supply chain.

**Threat intelligence provides organizations with valuable insight into the threat landscape.** Security teams may leverage threat intelligence from public and private sources to learn about current threats and vulnerabilities. They may seek out detailed indicators of compromise and perform predictive analytics on their own data. Threat intelligence teams often supplement open source and closed source intelligence that they obtain externally with their own research.

**Security teams must monitor for supply chain risks.** Modern enterprises depend on hardware, software, and cloud service vendors to deliver IT services to their internal and external customers. Vendor management techniques protect the supply chain against attackers seeking to compromise these external links into an organization's network. Security professionals should pay particular attention to risks posed by outsourced code development, cloud data storage, and integration between external and internal systems.

# Malicious Code

**Exam Essentials**

**Understand and explain the different types of malware.** Malware includes ransomware, Trojans, worms, spyware, bloatware, viruses, keyloggers, logic bombs, and rootkits. Each type of malware has distinctive elements, and security analysts need to know what identifies each type of malware, how to identify it, what controls are commonly deployed against it, and what to do if you encounter it.

**Explain common indicators of malicious activity associated with malware types.** Indicators of compromise associated with malware vary based on the type of malware and how it is designed and used. Common examples of IoCs associated with malware include command and control (C&C) traffic patterns, IP addresses, hostnames, and domains. Use of system utilities in unexpected ways, lateral movement between systems, creation of files and directories, encryption of files, and data exfiltration are also commonly seen, particularly with Trojans and rootkits. Signatures for malware are commonly used to identify specific files associated with given malware packages although malware writers use defensive techniques intended to make this harder.

**Understand the methods to mitigate malware.** Malware may require specialized techniques and processes to remove it or to deal with the impact of the malware. Techniques range from manual removal to the use of tools to identify and remove malicious files, and often rely on reinstallation of a system or restoration from a known good backup to ensure all malware is removed.

# Social Engineering and Password Attacks

**Exam Essentials**

**Many techniques are used for social engineering.** Many adversarial and security techniques rely on social engineering. Phishing and its related techniques of smishing and vishing seek to gain information using social engineering techniques. Misinformation and disinformation campaigns are used to change opinions and to shift narratives. Malicious actors will impersonate whomever they need to acquire information, to gain access or credentials, or to persuade individuals to take action. Pretexting is often used with impersonation to provide a believable reason for the action or request. Business email compromise and brand impersonation are both used to make malicious emails and other communications appear legitimate and thus more likely to fool targets into taking desired action. Watering hole attacks focus on sites that target frequently visit, while typosquatters rely on users who make typos while entering URLs.

**Passwords can be acquired and cracked in many ways.** Password attacks can be conducted both online against live systems and offline using captured password stores. Brute-force attacks like spraying and dictionary attacks as well as password cracking can recover passwords in many circumstances. Unencrypted or plain-text passwords and improper or unsecure storage methods like the use of MD5 hashes make attacks even easier for attackers who can access them.

# Security Assessment and Testing

**Exam Essentials**

**Many vulnerabilities exist in modern computing environments.** Cybersecurity professionals should remain aware of the risks posed by vulnerabilities both on-premises and in the cloud. Improper or weak patch management can be the source of many of these vulnerabilities, providing attackers with a path to exploit operating systems, applications, and firmware. Weak configuration settings that create vulnerabilities include open permissions, unsecured root accounts, errors, weak encryption settings, insecure protocol use, default settings, and open ports and services. When a scan detects a vulnerability that does not exist, the report is known as a false positive. When a scan does not detect a vulnerability that actually exists, the report is known as a false negative.

**Threat hunting discovers existing compromises.** Threat hunting activities presume that an organization is already compromised and search for indicators of those compromises. Threat hunting efforts include the use of advisories, bulletins, and threat intelligence feeds in an intelligence fusion program. They search for signs that attackers gained initial access to a network and then conducted maneuver activities on that network.

**Vulnerability scans probe systems, applications, and devices for known security issues.** Vulnerability scans leverage application, network, and web application testing to check for known issues. These scans may be conducted in a credentialed or noncredentialed fashion and may be intrusive or nonintrusive, depending on the organization's needs. Analysts reviewing scans should also review logs and configurations for additional context. Vulnerabilities are described consistently using the Common Vulnerabilities and Exposures (CVE) standard and are rated using the Common Vulnerability Scoring System (CVSS). CVE and CVSS are components of the Security Content Automation Protocol (SCAP).

**Penetration testing places security professionals in the role of attackers.** Penetration tests may be conducted in a manner that provides the testers with full access to information before the test (known environment), no information at all (unknown environment), or somewhere in between those two extremes (partially known environment). Testers conduct tests within the rules of engagement and normally begin with reconnaissance efforts, including war driving, war flying, footprinting, and open source intelligence (OSINT). They use this information to gain initial access to a system. From there, they seek to conduct privilege escalation to increase their level of access and lateral movement/pivoting to expand their access to other systems. They seek to achieve persistence to allow continued access after the vulnerability they initially exploited is patched. At the conclusion of the test, they conduct cleanup activities to restore systems to normal working order and remove traces of their activity.

**Bug bounty programs incentivize vulnerability reporting.** Bug bounty programs allow external security professionals to probe the security of an organization's public-facing systems. Testers who discover vulnerabilities are provided with financial rewards for their participation. This approach is a good way to motivate hackers to work for good, rather than using discovered vulnerabilities against a target.

**Recognize the purpose and types of security audits.** Audits are formal examinations of an organization's security controls. They may be performed by internal audit teams or independent third-party auditors. At the conclusion of an audit, the audit team makes an attestation about the adequacy and effectiveness of the organization's security controls.

**Understand the stages of the vulnerability life cycle.** The stages of the vulnerability life cycle are vulnerability identification, analysis, response and remediation, validation of remediation, and reporting. Vulnerability identification can come from scans, penetration tests, responsible disclosure or bug bounty programs, and audit results. Analysis involves confirming the vulnerability, prioritizing it using CVSS and CVE, and considering organization-specific factors. Responses include applying patches, isolating affected systems, implementing compensating controls, transferring risk through insurance, or formally accepting the risk. Validation ensures the vulnerability is no longer present, and reporting informs stakeholders about the findings, actions, trends, and recommendations for improvement.

# Application Security

**Exam Essentials**

**Understand secure software development concepts.** Software should be created using a standardized software development life cycle that moves software through development, test, staging, and production environments. Developers should understand the issues associated with code reuse and software diversity. Web applications should be developed in alignment with industry-standard principles such as those developed by the Open Worldwide Application Security Project (OWASP).

**Know how to analyze the indicators associated with application attacks.** Software applications may suffer from a wide range of vulnerabilities that make them susceptible to attack. You should be familiar with these attacks, including memory injection, buffer overflow, and race condition attacks. You should also understand web-specific attacks, such as Structured Query Language injection (SQLi) and cross-site scripting (XSS). Understanding the methods behind these attacks helps security professionals build adequate defenses and identify attacks against their organizations.

**Know how to implement application security controls.** Application security should be at the forefront of security operations principles. This includes protecting code through the use of input validation. Web applications that rely on cookies for session management should secure those cookies through the use of transport encryption. Code should be routinely subjected to code review as well as static and dynamic testing. Code signing provides end users with assurance that code came from a trusted source. Sandboxing allows the testing of code in an isolated environment.

**Explain the common benefits and drawbacks of automation and scripting related to secure operations.** The main benefits of automation are achieving efficiency and saving time, enforcing baselines, standardizing infrastructure configurations, scaling in a secure manner, retaining employees, lowering reaction times, and serving as a workforce multiplier. The main drawbacks are complexity, cost, creating a single point of failure, building up technical debt, and maintaining ongoing supportability.

**Explain common use cases of automation and scripting for cybersecurity.** Security professionals use automation and scripting techniques in many different use cases. These include user and resource provisioning, creating guard rails, managing security groups, creating and escalating tickets, enabling and disabling services and access, performing continuous integration and testing, and making use of application programming interfaces (APIs).

# Cryptography and PKI

**Exam Essentials**

**Understand the goals of cryptography.** The four goals of cryptography are confidentiality, integrity, authentication, and non-repudiation. Confidentiality is the use of encryption to protect sensitive information from prying eyes. Integrity is the use of cryptography to ensure that data is not maliciously or unintentionally altered. Authentication refers to uses of encryption to validate the identity of individuals. Non-repudiation ensures that individuals can prove to a third party that a message came from its purported sender.

**Explain the differences between symmetric and asymmetric encryption.** Symmetric encryption uses the same shared secret key to encrypt and decrypt information. Users must have some mechanism to exchange these shared secret keys. The Diffie–Hellman algorithm provides one approach. Asymmetric encryption provides each user with a pair of keys: a public key, which is freely shared, and a private key, which is kept secret. Anything encrypted with one key from the pair may be decrypted with the other key from the same pair.

**Explain how digital signatures provide non-repudiation.** Digital signatures provide non-repudiation by allowing a third party to verify the authenticity of a message. Senders create digital signatures by using a hash function to generate a message digest and then encrypting that digest with their own private key. Others may verify the digital signature by decrypting it with the sender's public key and comparing this decrypted message digest to one that they compute themselves using the hash function on the message.

**Understand the purpose and use of digital certificates.** Digital certificates provide a trusted mechanism for sharing public keys with other individuals. Users and organizations obtain digital certificates from certificate authorities (CAs), who demonstrate their trust in the certificate by applying their digital signature. Recipients of the digital certificate can rely on the public key it contains if they trust the issuing CA and verify the CA's digital signature.

**Demonstrate familiarity with emerging issues in cryptography.** Tor uses perfect forward secrecy to allow anonymous communication over the Internet. The blockchain is an immutable distributed public ledger made possible through the use of cryptography.

# Identity and Access Management

**Exam Essentials**

**Identities are the foundation of authentication and authorization.** Users claim an identity through an authentication process. In addition to usernames, identities are often claimed through the use of certificates, tokens, SSH keys, or smartcards, each of which provides additional capabilities or features that can help with security or other useful functions. Identities use attributes to describe the user, with various attributes like job, title, or even personal traits stored as part of that user's identity.

**Single sign-on and federation are core elements of many identity infrastructures.** Single sign-on (SSO) is widely used to allow users to log in once and use resources and services across an organization or federation. While there are many SSO technologies and implementations, LDAP, OAuth, and SAML are critical for many modern SSO designs.

**Passwords, passwordless authentication, and multifactor authentication all have roles to play in authentication systems.** Passwords best practices include configuration common settings like password length, complexity, reuse, expiration, and age. Understanding what each setting helps with and why it might be configured to specific settings is an important task for security professionals. Password managers help to limit password reuse and to manage passwords for organizations when implemented with enterprise solutions. Multifactor authentication relies on additional factors beyond passwords, including biometrics and hardware- and software-based tokens like security keys and authenticator applications. Multifactor requires the use of distinct factors: potential factors include something you know, something you have, something you are, or somewhere you are.

**Account types and account policies determine what users can do and privileged accounts must be managed and controlled.** Types of user accounts include users, guests, administrative (privileged) accounts, and service accounts. Provisioning and deprovisioning accounts as well as managing the account life cycle are key to ensuring that accounts have appropriate rights and that they do not remain after they are no longer needed. Privileged access management focuses on privileged accounts and rights, and leverages techniques like just-in-time permission granting and removal and short-lived, ephemeral accounts that exist just for the time needed to accomplish a task.

**Access control schemes determine what rights accounts have.** Important access control schemes include attribute-based access control (ABAC), which employs user attributes to determine what access the user should get. Role-based access control (RBAC) makes decisions based on roles, whereas rule-based access control (also sometimes called RBAC) uses rules to control access. In addition to knowing these access control schemes, be familiar with mandatory access control (MAC), which relies on the system administrator to control access, and discretionary access control (DAC), which allows users to make decisions about access to files and directories they have rights to. PAM (privileged access management) is focused on controlling administrative accounts. Finally, test takers also need to know how to use and apply common filesystem permissions.

# Resilience and Physical Security

**Exam Essentials**

**Redundancy builds resilience.** Redundant systems, networks, and even datacenters are a key element in ensuring availability. Redundant designs need to address the organizational risks and priorities that your organization faces to ensure the best trade-offs between cost and capabilities. Geographic dispersal; load balancers and clustering; power protection and redundancy; RAID; backups; and diversity of technologies, systems, cloud service providers, and platforms are all ways to build and ensure resiliency. Considerations include availability, resilience, cost, responsiveness, scalability, ease of deployment, risk transference, ease of recovery, patch availability, inability to patch, power, and compute. Capacity planning helps to ensure that there is enough capacity to handle issues and outages including ensuring you have enough people, technology, and infrastructure to recover. Multicloud environments as well as platform diversity can help ensure that a single technology or provider's outage or issue does not take your organization offline, but they create additional complexity and costs.

**Backups help ensure organizations can recover from events and issues.** Backups are designed to meet an organization's restoration needs, including how long it takes to recover from an issue and how much data may be lost between backups. Backup locations and frequency are determined based on the organization's risk profile and recovery needs, with offsite backups being a preferred solution to avoid losing backups in the same disaster as the source systems. Snapshots, journaling, and replication each have roles to play in ensuring data is available and accessible. Encryption is used to keep backups secure both in-transit and at rest.

**Response and recovery are critical when failures occur.** Failures will occur, so you need to know how to respond. Having a disaster recovery location, like a hot, warm, or cold site or a redundant cloud or hosted location, can help ensure that your organization can return to operations more quickly. Having a predetermined restoration order provides a guideline on what needs to be brought back online first due to either dependencies or importance to the organization. Testing, including tabletop exercises, failover testing, simulations, and parallel processing, are all common ways to ensure response and recovery will occur as planned.

**Physical security controls are a first line of defense.** Keeping your site secure involves security controls like fences, lighting, alarms, bollards, access control vestibules, cameras, and other sensors. Ensuring that only permitted staff are allowed in using locks, badges, and guards helps prevent unauthorized visitors. Sensors must be selected to match the environment and needs of the organization. Infrared, ultrasonic, pressure, and microwave sensors have different capabilities and costs. Brute-force attacks, as well as attacks against RFID and environmental attacks, need to be considered in physical security design.

# Cloud and Virtualization Security

**Exam Essentials**

**Explain the three major cloud service models.** In the anything-as-a-service (XaaS) approach to computing, there are three major cloud service models. Infrastructure-as-a-service (IaaS) offerings allow customers to purchase and interact with the basic building blocks of a technology infrastructure. Software-as-a-service (SaaS) offerings provide customers with access to a fully managed application running in the cloud. Platform-as-a-service (PaaS) offerings provide a platform where customers may run applications that they have developed themselves.

**Describe the four major cloud deployment models.** Public cloud service providers deploy infrastructure and then make it accessible to any customers who wish to take advantage of it in a multitenant model. The term *private cloud* is used to describe any cloud infrastructure that is provisioned for use by a single customer. A community cloud service shares characteristics of both the public and private models. Community cloud services do run in a multitenant environment, but the tenants are limited to members of a specifically designed community. Hybrid cloud is a catch-all term used to describe cloud deployments that blend public, private, and/or community cloud services together.

**Understand the shared responsibility model of cloud security.** Under the shared responsibility model of cloud security, cloud customers must divide responsibilities between one or more service providers and the customers' own cybersecurity teams. In an IaaS environment, the cloud provider takes on the most responsibility, providing security for everything below the operating system layer. In PaaS, the cloud provider takes over added responsibility for the security of the operating system itself. In SaaS, the cloud provider is responsible for the security of the entire environment, except for the configuration of access controls within the application and the choice of data to store in the service.

**Implement appropriate security controls in a cloud environment.** Cloud customers should understand how to use the controls offered by providers and third parties to achieve their security objectives. This includes maintaining resource policies and designing resilient cloud implementations that achieve high availability across multiple zones. From a storage perspective, cloud customers should consider permissions, encryption, replication, and high availability. From a network perspective, cloud customers should consider the design of virtual networks with public and private subnets to achieve appropriate segmentation. From a compute perspective, customers should design security groups that appropriately restrict network traffic to instances and maintain the security of those instances.

# Endpoint Security

**Exam Essentials**

**Understand operating system and hardware vulnerabilities.** Operating systems may be vulnerable, host vulnerable services or applications, or may have weak or insecure configurations that need to be addressed. Patching, configuration management, and security baselines all play a role in operating system security. Hardware security frequently focuses on firmware updates and security as well as life cycle management to properly address end-of-life and legacy hardware issues.

**Hardening and protecting systems relies on security tools and technology to keep systems secure.** Securing endpoint devices requires considering the entire device: how it boots, how data is secured, how it is configured, what services it provides, if its communications are secure, and how it is protected against network threats. Fortunately, security professionals have a wide range of tools, including secure and trusted boot, to protect against attacks on the boot process or drivers. Antivirus, antimalware, EDR, XDR, and data loss prevention tools provide insight into what systems are doing and where issues may exist while adding more controls that administrators and security professionals can use to keep systems and data secure. Network security tools like host intrusion prevention and detection systems, host firewalls, and similar tools can detect and often stop attacks from the network.

**Hardening endpoints also relies on configuration, settings, policies, and standards to ensure system security.** Although tools and technology are important to protect endpoints, configuration and settings are also an important part of the process. Disabling unnecessary services, changing default passwords, applying settings in the Windows Registry or operating systems settings in Linux, and otherwise using built-in and add-on configuration options to match security configurations to the device's risk profile is critical. Finally, patch management for the operating system and the applications installed on devices protects against known vulnerabilities and issues.

**Specialized systems like SCADA, ICS, and IoT systems exist throughout your organization and require unique security solutions.** SCADA and ICS or industrial control systems are used to manage and monitor factories, power plants, and many other major components of modern companies. IoT systems are Internet-connected devices that perform a wide variety of tasks, from monitoring to home automation and more. They may be controlled by third parties or have other security implications that must be addressed as part of a security plan to keep each endpoint secure.

**Explain the importance of asset management for software, data, and hardware.** Assets must be managed from acquisition through their life cycle until disposal or decommissioning. Proper management includes ensuring that ownership and classification are maintained and tracked, and that inventories of assets are up to date and include appropriate information to support operations, security, and incident response needs.

**Drive encryption and sanitization help prevent data exposure.** Encrypting drives and media helps keep them secure if they are stolen or lost. Full-disk encryption covers the entire drive, whereas volume or file encryption protects portions of the contents. Sanitizing drives and media involves wiping them using a secure deletion process, or their destruction to ensure that the data cannot be recovered. Using appropriate processes based on the security requirements for the data and the type of drive or media involved is critical to making sure that the data is properly removed.

# Network Security

**Exam Essentials**

**The foundation of network security is a secure design.** Networks must be designed with security in mind. Considerations include the attack surface of the network and its attached devices, which drives placement and segmentation into different security zones based on risk or security requirements. Understanding what will happen when failures occur and dealing with those failures also influences design and choices around high availability. NAC and 802.1X protect networks from untrusted devices being connected, whereas port security and port-level protections like loop prevention and broadcast storm protection ensure that malicious or misconfigured systems do not cause network issues. Network taps and monitoring ports allow packet capture by creating a copy of traffic from other ports. VPNs are used to tunnel network traffic to another location, and they can be encrypted or simply tunneled. Key concepts like physical isolation, logical segmentation, use of secure protocols, use of reputation services, and tools like software-defined networking, zero trust, SD-WAN, and SASE all have their place in secure network design.

**Network appliances are used to provide security services to networks and systems.** There are many types of network appliances. Jump servers provide a secure way to access systems in another security zone. Load balancers spread load among systems and can use different scheduling options as well as operational modes like active/active or active/passive designs. Proxy servers either centralize connections from a group of clients out to a server or from a group of servers out to clients, often as a load-balancing strategy. Web filters filter content and URLs to limit what information can enter and exit a network based on rules, and data loss prevention systems monitor to ensure that data that shouldn't leave systems or networks is identified and flagged, sent securely, or stopped. IDS and IPS devices identify and take action based on malicious behavior, signatures, or anomalies in traffic. Data collection devices like sensors and collectors help with data gathering. Firewalls, including next-generation firewalls, web application firewalls, and unified threat management appliances, are used to build security zones and are placed at trust boundaries. UTM devices combine many of these security features and capabilities into a single appliance or system. Access control lists are used by many devices, including switches and routers to determine what traffic can flow through them based on rules.

**Network security services and management techniques help make sure that a network stays secure.** Out-of-band management puts management interfaces on a separate VLAN or physical network or requires direct connection to help prevent attackers from gaining access to management interfaces. DNS security is also limited, but DNSSEC helps validate DNS servers and responses. DNS servers must be properly configured to prevent zone transfers and other DNS attacks. Email security leverages DMARC, DKIM, and SPF to validate senders and domains. TLS is used broadly to protect network traffic, acting as a wrapper for many other protocols. Monitoring services and systems helps ensure that they remain online and accessible but require care due to the amount of information that can be generated and the fact that false positives are possible if the validation and monitoring does not fully validate service responses. File integrity monitors check to see if files have been changed and can alert on changes or restore existing files to a pre-change or pre-deletion state. Honeypots and honeynets are used to gather information about attackers, and honeyfiles and honeytokens are used to identify potential breaches and attackers who have gathered information from systems in your environment. Network devices are hardened, much like other devices, often based on standards and benchmarks.

**Secure protocols provide ways to send and receive information securely.** Many original Internet protocols are not secure—they do not provide encryption or authentication and can be captured and analyzed or modified. Using secure versions of protocols or using an alternate secure service and protocol is an important part of ensuring that a network is secure. Key protocols include voice and video protocols like SRTP; email protocols like IMAPS and POPS; and security protocols like DMARC, DKIM, and SPF. File transfers can be done via SFTP or FTPS instead of FTP, and directory services can be moved from LDAP to LDAPS. Some protocols do not have as many or as complete secure options. In fact, DNS, routing, and DHCP all have limited options for secure communications. Network administrators must take these into account while designing and operating their networks.

**Network attacks drive network security decisions and design.** On-path attacks redirect traffic through a system that an attacker controls, allowing them to observe and potentially modify traffic. DNS attacks include domain hijacking, DNS poisoning, and URL redirection, but can be partially countered through the use of DNSSEC. Credential replay attacks take advantage of poorly designed or insecure protocols to send valid authentication hashes or other artifacts pretending to be a legitimate user. Malicious code ranging from worms to denial-of-service tools can impact networks and must be accounted for in design. Denial-of-service attacks and distributed denial-of-service attacks consume resources or target services to cause them to fail. Reflected denial-of-service attacks use spoofed source addresses to cause traffic to be sent to targets, whereas amplified denial-of-service attacks use small queries to get large results, amplifying their impact.

# Wireless and Mobile Security

**Exam Essentials**

**Modern enterprises rely on many types of wireless connectivity.** There are many wireless connectivity options for organizations and individuals. Devices may connect via cellular networks, which place the control of the network in the hands of cellular providers. Wi-Fi is widely used to connect devices to organizational networks at high speed, allowing ease of mobility while providing security using enterprise security protocols. Bluetooth provides connectivity between many devices and cellular is used to provide access from mobile devices and systems that can't connect to Wi-Fi or wired networks.

**Secure wireless network designs take existing networks and physical spaces into account.** Site surveys include physical tours of a facility using tools that can identify existing wireless networks and access points as well as signal strengths and other details that help map the location. Network designs take into account channel spacing, access point placement, and even the composition of the building when placing access points.

**Cryptographic and authentication protocols provide wireless security.** Both WPA2 and WPA3 are used in modern Wi-Fi networks. These protocols provide for both simple authentication protocols, like WPA2's preshared key mode, and for enterprise authentication models that rely on RADIUS servers to provide user login with organizational credentials. Both rely on cryptographic protocols to encrypt data in transit. Devices are frequently configured to use a variant of the Extensible Authentication Protocol (EAP) that supports the security needs of the organization and that is supported by the deployed wireless devices.

**Understand mobile device vulnerabilities.** Sideloading involves copying programs from an external device or system, allowing them to be added to a device and potentially bypassing the device's application store. Jailbreaking provides root access to devices providing greater control but also creating security concerns because it bypasses the device's native security model.

**Securing underlying wireless infrastructure requires strong network device administration and security practices.** Wireless controllers and access points must be protected, and installation considerations are important to consider for wireless devices. Like other network devices, controllers and APs need to be regularly patched and updated and must be configured securely. They also must have protected administrative interfaces and should be configured to log and report on the network, their own status, and security issues or potential problems. Heatmaps and site surveys help administrators understand the environment they are deploying into and operating in.

**Managing mobile devices relies on both deployment methods and administrative tools.** Deployment methods include bring your own device; choose your own device; corporate-owned, personally enabled; and corporate owned, business only. The risks and rewards for each method need to be assessed as organizations choose which model to deploy their devices in. Once that decision is made, tools like mobile device management or unified endpoint management can be used to configure, secure, manage, and control the devices in a wide range of ways, from deploying applications to securely wiping devices if they are lost or stolen. You need to understand the capabilities and limitations of MDM and UEM products as well as the devices and operating systems that they can manage.

# Monitoring and Incident Response

**Exam Essentials**

**The incident response cycle and incident response process outline how to respond to an incident.** The Security+ exam's incident response cycle includes preparation, detection, analysis, containment, eradication, recovery, and lessons learned. A response process may not be in a single phase at a time, and phases may move forward or backward depending on discoveries and further events. Organizations train their staff and hold exercises like tabletop exercises, walk-throughs, and simulations to allow their teams to practice incident response.

**Threat hunting uses data to identify potential indicators of compromise.** IoCs are a critical part of a modern threat hunter's toolkit. They include detecting things like account lockout, concurrent session usage, impossible travel, attempted access to blocked content, resource consumption, resource inaccessibility, out-of-cycle logging, and missing logs, among many other potential IoCs. IoCs are documented and published through threat feeds and other services and sources.

**Data sources and data management for incident response provide insight into what occurred as well as investigative and detection tools.** Security information and event management (SIEM) tools are used in many organizations to gather and analyze data using dashboards, automated analysis, and manual investigation capabilities. Information such as vulnerability scan output, system configuration data, system and device logs, and other organizational data are ingested and analyzed to provide broad insight into events and incidents. Network traffic information is gathered using NetFlow, sFlow, and packet analyzers, among other tools. They provide useful information about bandwidth usage as well as details about which systems communicated, the ports and protocols in use, time and date, and other high-level information useful for incident analysis. In addition to log and event information, metadata from files and other locations is commonly used for incident investigation and incident response.

**Mitigation techniques ensure that the impact of incidents are limited.** Incident responders use a variety of techniques to mitigate and contain and recover from incidents. One of the most common tasks is to change configuration for endpoint security solutions as well as devices. That may include using allow lists or block/deny lists, quarantining files or devices, making firewall changes, using MDM or DLP tools, adding content or URL filtering rules, or revoking or updating certificates. At the network and infrastructure level, isolation, containment, and segmentation are all used to separate systems involved in incidents from other systems or networks. Root cause analysis is used to determine why an incident was able to happen or why it happened and to guide preparation work to avoid future incidents.

# Digital Forensics

**Exam Essentials**

**Legal holds and e-discovery drive some forensic activities.** Organizations face legal cases and need to respond to legal holds, which require them to preserve and protect relevant information for the active or pending case. E-discovery processes also require forensic and other data to be provided as part of a legal case. Organizations must build the capability and technology to respond to these requirements in an appropriate manner to avoid losing cases in court and to support incident response processes.

**Acquisition techniques and procedures ensure usable and admissible forensic data.** Different system components and resources are more likely to be changed or lost during the time it takes for a forensic acquisition. Thus, forensic practitioners refer to the order of volatility to determine what is the most volatile and what is the least volatile. Your forensic acquisition process should take the order of volatility into account as well as the circumstances of your acquisition process as part of incident response or legal holds to determine what to capture first.

**There are many options for acquisition tools, and selecting the right tool combines technical needs and skillsets.** Image acquisition tools provide the ability to copy disks and volumes using a bit-by-bit method that will capture the complete image including unused or slack space. Acquisition processes vary based on where the data is located, including acquisition using snapshots of virtual machines, data volume copies for cloud environments, and disk images for workstations and mobile devices. Incident responders must bear in mind both maintaining a chain of custody and the specific technical requirements of the system or devices they are capturing data from.

**Validation and preservation of forensic data is a key part of the forensic process.** Hashing drives and images ensures that the acquired data matches its source. Forensic practitioners continue to commonly use MD5 or SHA1 despite issues with both hashing methods because adversarial techniques are rarely at play in forensic examinations. Checksums can be used to ensure that data is not changed, but they do not create the unique fingerprints that hashes are also used to provide for forensic artifacts. Preservation requires following chain-of-custody processes as well as forethought about the use of write blockers, forensic copies, and documented processes and procedures.

**Forensic reports must be well organized and to the point.** Forensic analysis doesn't end when the technical examination of devices and drives is over. Forensic reports summarize key findings, then explain the process, procedures and tools, and any limitations or assumptions that impact the investigation. Next, they detail the forensic findings with appropriate evidence and detail to explain how conclusions were reached. They conclude with recommendations or overall conclusions in more detail than the summary provided.

# Security and Governance Compliance

**Exam Essentials**

**Security governance practices ensure that organizations achieve their strategic objectives.** Governance programs are the sets of procedures and controls put in place to allow an organization to effectively direct its work. Governance programs may involve the participation of a variety of boards, committees, and government regulators. Centralized governance models use a top-down approach that dictates how subordinate units meet security objectives, whereas decentralized governance models delegate the authority for meeting security objectives as the subordinate units see fit.

**Policy frameworks consist of policies, standards, procedures, and guidelines.** Policies are high-level statements of management intent for the information security program. Standards describe the detailed implementation requirements for policy. Procedures offer step-by-step instructions for carrying out security activities. Compliance with policies, standards, and procedures is mandatory. Guidelines offer optional advice that complements other elements of the policy framework.

**Organizations often adopt a set of security policies covering different areas of their security programs.** Common policies used in security programs include an information security policy, an acceptable use policy, a data ownership policy, a data retention policy, an account management policy, and a password policy. The specific policies adopted by any organization will depend on that organization's culture and business needs.

**Policy documents should include exception processes.** Exception processes should outline the information required to receive an exception to security policy and the approval authority for each exception. The process should also describe the requirements for compensating controls that mitigate risks associated with approved security policy exceptions.

**Change management is crucial to ensuring the availability of systems and applications.** The primary goal of change management is to ensure that changes do not cause outages. Change management processes ensure that appropriate personnel review and approve changes before implementation and ensure that personnel test and document the changes. Change review processes should carefully evaluate the potential impact of any change.

**Organizations face a variety of security compliance requirements.** Merchants and credit card service providers must comply with the Payment Card Industry Data Security Standard (PCI DSS). Organizations handling the personal information of European Union residents must comply with the EU General Data Protection Regulation (GDPR). All organizations should be familiar with the national, territory, and state laws that affect their operations.

**Standards frameworks provide an outline for structuring and evaluating cybersecurity programs.** Organizations may choose to base their security programs on a framework, such as the NIST Cybersecurity Framework (CSF) or International Organization for Standardization (ISO) standards. U.S. federal government agencies and contractors should also be familiar with the NIST Risk Management Framework (RMF). These frameworks sometimes include maturity models that allow an organization to assess its progress. Some frameworks also offer certification programs that provide independent assessments of an organization's progress toward adopting a framework.

**Security training and awareness ensures that individuals understand their responsibilities.** Security training programs impart new knowledge on employees and other stakeholders. They should be tailored to meet the specific requirements of an individual's role in the organization. Security awareness programs seek to remind users of the information they have already learned, keeping their security responsibilities top-of-mind.

# Risk Management and Privacy

**Exam Essentials**

**Risk identification and assessment helps organizations prioritize cybersecurity efforts.** Cybersecurity analysts seek to identify all of the risks facing their organization and then conduct a business impact analysis to assess the potential degree of risk based on the probability that it will occur and the magnitude of the potential effect on the organization. This work allows security professionals to prioritize risks and communicate risk factors to others in the organization.

**Vendors are a source of external risk.** Organizations should conduct their own systems assessments as part of their risk assessment practices, but they should also conduct supply chain assessments as well. Performing vendor due diligence reduces the likelihood that a previously unidentified risk at a vendor will negatively impact the organization. Hardware source authenticity techniques verify that hardware was not tampered with after leaving the vendor's premises.

**Organizations may choose from a variety of risk management strategies.** Risk avoidance strategies change business practices to make a risk irrelevant to the organization. Risk mitigation techniques seek to reduce the probability or magnitude of a risk. Risk transference approaches move some of the risk to a third party. Risk acceptance acknowledges the risk and continues normal business operations despite the presence of the risk.

**Disaster recovery planning builds resiliency.** Disaster recovery plans activate when an organization experiences a natural or human-made disaster that disrupts its normal operations. The disaster recovery plan helps the organization quickly recover its information and systems and resume normal operations.

**Privacy controls protect personal information.** Organizations handling sensitive personal information should develop privacy programs that protect that information from misuse and unauthorized disclosure. The plan should cover personally identifiable information (PII), protected health information (PHI), financial information, and other records maintained by the organization that might impact personal privacy.