Device and Mobile Security:

QUESTION 1:

Mobile security:

Mobile security, also known as wireless security, refers to the measures taken to protect smartphones, tablets, laptops, smartwatches and other portable computing devices and the networks they connect to, from threats and vulnerabilities associated with wireless computing.

The goal of mobile security is to ensure the confidentiality, integrity and availability of data stored or transmitted by mobile devices. Mobile security is typically part of an organization's comprehensive security strategy.

Mobile security important:

Securing mobile devices has become increasingly important as the number of devices and the ways those devices are used have expanded dramatically. In the enterprise, this is particularly problematic when employee-owned devices connect to the corporate network.

Mobile security is important for the following reasons:

Protects sensitive data: Mobile devices contain a large amount of personal data and sensitive information, such as contact lists, emails, passwords and financial data. It's imperative that mobile security protects this data from illegal access and potential misuse.

Prevents data breaches: Cybercriminals are increasingly targeting mobile devices as potential entry points for illegal access to corporate networks and sensitive data. Setting up comprehensive mobile security measures helps prevent data breaches and the potential financial and reputational damage they can cause.

Mitigates mobile-specific attacks: Mobile devices are vulnerable to specific security threats, such as malware, phishing schemes, vishing attacks, SIM swap attacks and network vulnerabilities. Mobile security helps protect data integrity and confidentiality by recognizing and minimizing threats specific to mobile devices.

Protects business assets: Mobile devices are frequently used in the workplace to access business apps, sensitive data and confidential information. Securing mobile devices protects these valuable company assets from illegal access or compromise.

Ensures regulatory compliance: Many companies must ensure they follow specific regulations and compliance regarding the security of sensitive data. Businesses that use mobile security can follow these requirements while avoiding financial and legal penalties.

Provides user privacy and trust: When using mobile apps and services, users anticipate that their personal information will be secure. By giving mobile security priority, businesses can win over the trust of their customers and show that they're committed to protecting their privacy.

Mobile security threats

Corporate data on devices increases the draw for cybercriminals who can target both the device and the back-end systems they tap into with mobile malware or undetected spyware. IT departments work to ensure that employees know what the acceptable use policies are and that administrators enforce those guidelines.

Security breaches. Without mobile device security measures, organizations can be vulnerable to malicious software, data leakage and other mobile cyber threats. Security breaches can cause widespread disruptions to the business, including complicating IT operations and affecting user productivity if systems must shut down.

Phishing and smishing attacks: Phishing attacks trick users into divulging their personal information, such as passwords or credit card details, by posing as trustworthy entities. Phishing attacks typically occur through emails, text messages or fake websites designed to look legitimate. Phishing attempts that are carried out through SMS or text messages are also known as smishing attacks.

Open Wi-Fi: Open Wi-Fi hotspots, such as those found in coffee shops and hotel rooms, can pose risks to mobile devices. When using open public connections, a device might be susceptible to man-in-the-middle-attacks (MiTM) in which hackers intercept connections between a browser and a mobile device to get access to personal information, spread malware and seize control. To achieve this, cybercriminals can also create honeypot Wi-Fi hotspots that appear legal and free.

Mobile ransomware : The rise in the use of mobile devices for business purposes has increased the frequency and severity of mobile ransomware, a unique and dangerous type of malware. It encrypts files on mobile devices and requests a ransom for the decryption key, which is necessary to unlock the encrypted data.

Biometric spoofing : Biometric spoofing in mobile security is the intentional alteration or replication of biometric characteristics to deceive mobile devices that rely on biometric authentication for security. Using

fraudulent or manipulated biometric data, attackers can impersonate someone else and mislead authentication mechanisms into granting them access to secured systems. For example, attackers might use forged fingerprints to impersonate a real user's fingerprint features to gain access through Touch ID on an Apple iPhone or iPad. They can achieve this by replicating the victim's fingerprints on items they've touched, such as a doorknob and creating false fingerprints with materials such as gelatin or silicone.

Cryptojacking : Cryptojacking is a type of mobile threat where unauthorized individuals use someone else's mobile device to mine Bitcoin and other cryptocurrencies without their knowledge or consent. In 2019, several applications infected with cryptojacking JavaScript were discovered on the Microsoft Store. These apps, including Fast-search Lite and Battery Optimizer, exploited users' devices to mine cryptocurrency.

MitM attacks : MitM attacks occur when an attacker intercepts network traffic to eavesdrop on or change sent data. Mobile devices are especially vulnerable to MitM attacks. This is because SMS messages can be easily intercepted if mobile applications use the unencrypted Hypertext Transfer Protocol instead of the secure Hypertext Transfer Protocol Secure to transport potentially sensitive information.

Compromised data: A lack of mobile security can lead to compromised employee, business or customer data. If an employee leaves a tablet or smartphone in a taxi or at a restaurant, for example, sensitive data, such as customer information or corporate intellectual property, can be put at risk.

Unnecessary app permissions : Application security is also a mobile security concern. One problem is mobile apps that request too many privileges, which enables them to access various data sources on the device. Leaked corporate contacts, calendar items and even the location of certain executives could put a company at a competitive disadvantage.

Infections and malware: Another concern is malicious software or Trojan-infected applications that are designed to look like they perform normally, but secretly upload sensitive data to a remote server. Malware attacks are a common mobile security concern. Experts say Android devices face the biggest threat, but other platforms can attract financially motivated cybercriminals if they adopt near-field communications and other mobile payment technologies.

The following is an overview of how mobile security works:

- ***Device security.*** *From a device configuration standpoint, many organizations implement policies that require devices to be locked with a password or to use biometric authentication. Organizations also use mobile device security software to deploy and manage devices, audit the OS levels used and remotely wipe a device. For instance, an organization might want to remotely wipe a phone that an employee accidentally left in public.*
- ***Application protection.*** *Mobile apps are susceptible to mobile security attacks. Mobile security aims to safeguard applications by using methods such as code analysis, secure coding practices and app vetting processes to detect and prevent harmful or susceptible apps from being loaded on devices.*
- ***Network security.*** *Mobile devices frequently connect to a variety of networks, including unsecured Wi-Fi and cellular networks. Mobile security entails shielding devices from network-based risks including MitM attacks by using secure network protocols, virtual private networks (VPNs) and network monitoring software.*
- ***Operating system (OS) protection.*** *Safeguarding a device's underlying OS is also part of mobile security. This includes keeping the OS current with the latest security patches and updates, as well as using OS security features such as sandboxing and permission controls to prevent unauthorized access to critical data.*

- ***Mobile device management.*** *Organizations use MDM services to control and secure staff mobile devices. With MDM, businesses can remotely manage and keep an eye on devices, enforce security policies and ensure everyone is following security requirements.*
- ***End-user practices.*** *End-user mobile security best practices might include avoiding public Wi-Fi networks or connecting to corporate resources through a VPN. IT staff can also educate users on mobile threats such as malicious software and seemingly legitimate apps that are designed to steal data.*

the types of mobile device security:

Mobile device security often centers around the use of MDM. MDM capabilities are often available in enterprise mobility management and unified endpoint management tools, which evolved from the early device-only management options.

However, organizations typically use other security tools to enhance their mobile device security which include the following:

- ***VPNs.*** *VPNs provide a secure connection between a mobile device and a private network, letting users send and receive data as if the device were physically linked to the private network. VPNs use encryption technology to safeguard data transported over shared or public networks, thus improving the security of remote access to company resources.*
- ***Mobile data encryption.*** *Encryption is a critical component of mobile device security, as it entails encoding data to render it illegible by unauthorized users. Data can be encrypted both at rest and in transit. Mobile data encryption helps to protect critical data even if the device is lost or stolen.*
- ***Mobile application security.*** *Mobile applications can pose security risks if not developed or downloaded from verified sources, resulting in compromised devices and data theft. Organizations can reduce mobile application security risks by adopting app vetting, code analysis and secure coding practices.*
- ***Secure web gateway.*** *A secure web gateway enhances mobile security, as it safeguards against online security threats by enforcing security policies and defending against phishing and malware in real time.*

This enables secure mobile web browsing and stops users from accessing fraudulent websites or downloading harmful content.

- ***Mobile threat defense (MTD).*** *MTD systems safeguard mobile devices against various threats, including malware, phishing attempts and network-based attacks. These systems detect and mitigate mobile risks through behavioral analysis, machine learning and real-time threat intelligence.*

Mobile device security vendors and products

Numerous vendors offer mobile device management and security tools. Examples of the tools available include the following:

- *Check Point Software Harmony Mobile.*
- *Google Endpoint Management.*
- *Hexnode Unified Endpoint Management.*
- *IBM Security MaaS360.*
- *Microsoft Enterprise Mobility + Security.*
- *Symantec Endpoint Protection Mobile.*
- *Trend Micro Mobile Security for Enterprises.*
- *Verizon Lookout Mobile Endpoint Security.*
- *VMware Workspace One Unified Endpoint Management.*
- *Zimperium Mobile Threat Defense.*

Tools and Technologies for Cyber Security:

QUESTION 1:

There are many varieties of cyber attacks that happen in the world today. If we know the various types of cyberattacks, it becomes easier for us to protect our networks and systems against them. Here, we will closely examine the top ten cyber-attacks that can affect an individual, or a large business, depending on the scale.

Elevate your cybersecurity acumen with our intensive Cyber security Bootcamp, where you'll delve into the diverse landscape of cyber attacks. From phishing to malware, ransomware to DDoS attacks, our comprehensive program equips you with the skills to anticipate, prevent, and mitigate a wide range of threats.

Let's start with the different types of cyberattacks on our list:

1. Malware Attack

This is one of the most common types of cyberattacks. "Malware" refers to malicious software viruses including worms, spyware, ransomware, adware, and trojans.

The trojan virus disguises itself as legitimate software. Ransomware blocks access to the network's key components, whereas Spyware is software that steals all your confidential data without your knowledge. Adware is software that displays advertising content such as banners on a user's screen.

Malware breaches a network through a vulnerability. When the user clicks a dangerous link, it downloads an email attachment or when an infected pen drive is used.

Let's now look at how we can prevent a malware attack:

Use antivirus software. It can protect your computer against malware. Avast Antivirus, Norton Antivirus, and McAfee Antivirus are a few of the popular antivirus software.

Use firewalls. Firewalls filter the traffic that may enter your device. Windows and Mac OS X have their default built-in firewalls, named Windows Firewall and Mac Firewall.

Stay alert and avoid clicking on suspicious links.

Update your OS and browsers, regularly.

2. Phishing Attack

Phishing attacks are one of the most prominent widespread types of cyberattacks. It is a type of social engineering attack wherein an attacker impersonates to be a trusted contact and sends the victim fake mails.

Unaware of this, the victim opens the mail and clicks on the malicious link or opens the mail's attachment. By doing so, attackers gain access to confidential information and account credentials. They can also install malware through a phishing attack.

Phishing attacks can be prevented by following the below-mentioned steps:

Scrutinize the emails you receive. Most phishing emails have significant errors like spelling mistakes and format changes from that of legitimate sources.

Make use of an anti-phishing toolbar.

Update your passwords regularly.

3. Password Attack

It is a form of attack wherein a hacker cracks your password with various programs and password cracking tools like Aircrack, Cain, Abel, John the Ripper, Hashcat, etc. There are different types of password attacks like brute force attacks, dictionary attacks, and keylogger attacks.

Listed below are a few ways to prevent password attacks:

Use strong alphanumeric passwords with special characters.

Abstain from using the same password for multiple websites or accounts.

Update your passwords; this will limit your exposure to a password attack.

Do not have any password hints in the open.

4. Man-in-the-Middle Attack

A Man-in-the-Middle Attack (MITM) is also known as an eavesdropping attack. In this attack, an attacker comes in between a two-party communication, i.e., the attacker hijacks the session between a client and host. By doing so, hackers steal and manipulate data.

As seen below, the client-server communication has been cut off, and instead, the communication line goes through the hacker.

MITM attacks can be prevented by following the below-mentioned steps:

Be mindful of the security of the website you are using. Use encryption on your devices.

Refrain from using public Wi-Fi networks.

5. SQL Injection Attack

A Structured Query Language (SQL) injection attack occurs on a database-driven website when the hacker manipulates a standard SQL query. It is carried by injecting a malicious code into a vulnerable website search box, thereby making the server reveal crucial information.

This results in the attacker being able to view, edit, and delete tables in the databases. Attackers can also get administrative rights through this.

To prevent a SQL injection attack:

Use an Intrusion detection system, as they design it to detect unauthorized access to a network.

Carry out a validation of the user-supplied data. With a validation process, it keeps the user input in check.

6. Denial-of-Service Attack

A Denial-of-Service Attack is a significant threat to companies. Here, attackers target systems, servers, or networks and flood them with traffic to exhaust their resources and bandwidth.

When this happens, catering to the incoming requests becomes overwhelming for the servers, resulting in the website it hosts either shut down or slow down. This leaves the legitimate service requests unattended.

It is also known as a DDoS (Distributed Denial-of-Service) attack when attackers use multiple compromised systems to launch this attack.

Let's now look at how to prevent a DDoS attack:

Run a traffic analysis to identify malicious traffic.

Understand the warning signs like network slowdown, intermittent website shutdowns, etc. At such times, the organization must take the necessary steps without delay.

Formulate an incident response plan, have a checklist and make sure your team and data center can handle a DDoS attack.

Outsource DDoS prevention to cloud-based service providers.

7. Insider Threat

As the name suggests, an insider threat does not involve a third party but an insider. In such a case; it could be an individual from within the organization who knows everything about the organization. Insider threats have the potential to cause tremendous damages.

Insider threats are rampant in small businesses, as the staff there hold access to multiple accounts with data. Reasons for this form of an attack are many, it can be greed, malice, or even carelessness. Insider threats are hard to predict and hence tricky.

To prevent the insider threat attack:

Organizations should have a good culture of security awareness.

Companies must limit the IT resources staff can have access to depending on their job roles.

Organizations must train employees to spot insider threats. This will help employees understand when a hacker has manipulated or is attempting to misuse the organization's data.

8. Cryptojacking

The term Cryptojacking is closely related to cryptocurrency. Cryptojacking takes place when attackers access someone else's computer for mining cryptocurrency.

The access is gained by infecting a website or manipulating the victim to click on a malicious link. They also use online ads with JavaScript code for this. Victims are unaware of this as the Crypto mining code works in the background; a delay in the execution is the only sign they might witness.

Cryptojacking can be prevented by following the below-mentioned steps:

Update your software and all the security apps as cryptojacking can infect the most unprotected systems.

Have cryptojacking awareness training for the employees; this will help them detect crypotjacking threats.

Install an ad blocker as ads are a primary source of cryptojacking scripts. Also have extensions like MinerBlock, which is used to identify and block crypto mining scripts.

9. Zero-Day Exploit

A Zero-Day Exploit happens after the announcement of a network vulnerability; there is no solution for the vulnerability in most cases. Hence the vendor notifies the vulnerability so that the users are aware; however, this news also reaches the attackers.
Depending on the vulnerability, the vendor or the developer could take any amount of time to fix the issue. Meanwhile, the attackers target the disclosed vulnerability. They make sure to exploit the vulnerability even before a patch or solution is implemented for it.

Zero-day exploits can be prevented by:

Organizations should have well-communicated patch management processes. Use management solutions to automate the procedures. Thus it avoids delays in deployment.

Have an incident response plan to help you deal with a cyberattack. Keep a strategy focussing on zero-day attacks. By doing so, the damage can be reduced or completely avoided.

10. Watering Hole Attack

The victim here is a particular group of an organization, region, etc. In such an attack, the attacker targets websites which are frequently used by the targeted group. Websites are identified either by closely monitoring the group or by guessing.

After this, the attackers infect these websites with malware, which infects the victims' systems. The malware in such an attack targets the user's personal information. Here, it is also possible for the hacker to take remote access to the infected computer.

Let's now see how we can prevent the watering hole attack:

Update your software and reduce the risk of an attacker exploiting vulnerabilities. Make sure to check for security patches regularly.Use your network security tools to spot watering hole attacks. Intrusion prevention systems(IPS) work well when it comes to detecting such suspicious activities.

To prevent a watering hole attack, it is advised to conceal your online activities. For this, use a VPN and also make use of your browser's private browsing feature. A VPN delivers a secure connection to another network over the Internet. It acts as a shield for your browsing activity. NordVPN is a good example of a VPN.

Although we had a look at several ways to prevent the different types of cyberattacks we discussed, let's summarize and look at a few personal tips which you can adopt to avoid a cyberattack on the whole.

Change your passwords regularly and use strong alphanumeric passwords which are difficult to crack. Refrain from using too complicated passwords that you would tend to forget. Do not use the same password twice.

Update both your operating system and applications regularly. This is a primary prevention method for any cyber attack. This will remove vulnerabilities that hackers tend to exploit. Use trusted and legitimate Anti-virus protection software.

Use a firewall and other network security tools such as Intrusion prevention systems, Access control, Application security, etc.

Avoid opening emails from unknown senders. Scrutinize the emails you receive for loopholes and significant errors.

Make use of a VPN. This makes sure that it encrypts the traffic between the VPN server and your device.

Regularly back up your data. According to many security professionals, it is ideal to have three copies of your data on two different media types and another copy in an off-site location (cloud storage). Hence, even in the course of a cyber attack, you can erase your system's data and restore it with a recently performed backup.

Employees should be aware of cybersecurity principles. They must know the various types of cyberattacks and ways to tackle them.

Use Two-Factor or Multi-Factor Authentication. With two-factor authentication, it requires users to provide two different authentication factors to verify themselves. When you are asked for over two additional authentication methods apart from your username and password, we term it as multi-factor authentication. This proves to be a vital step to secure your account.

Secure your Wi-Fi networks and avoid using public Wi-Fi without using a VPN.

Safeguard your mobile, as mobiles are also a cyberattack target. Install apps from only legitimate and trusted sources, make sure to keep your device updated.

These are the tips you must implement to protect your systems and networks from a cyber attack.

Evolution of Cyber Security:

The evolution of cyber security can be traced back to the early days of computing when security measures were minimal, and the internet was a relatively small network. In the early 90s, firewalls were the common method of protecting networks and data from cyber-attacks. Now, this field of cyber security has a wide range of technologies:

Intrusion detection systems

Threat intelligence

Security information and event management (SIEM)

Cyber Security Best Practices:

QUESTION 1:

Security threats are constantly evolving, and compliance requirements are becoming increasingly complex. Organizations must create a comprehensive information security policy to cover both challenges. An information security policy makes it possible to coordinate and enforce a security program and communicate security measures to third parties and external auditors.

To be effective, an information security policy should:

Cover end-to-end security processes across the organization

Be enforceable and practical

Be regularly updated in response to business needs and evolving threats

Be focused on the business goals of your organization

The importance of an information security policy

Information security policies can have the following benefits for an organization:

Facilitates data integrity, availability, and confidentiality —ffective information security policies standardize rules and processes that protect against vectors threatening data integrity, availability, and confidentiality.

Protects sensitive data — Information security policies prioritize the protection of intellectual property and sensitive data such as personally identifiable information (PII).

Minimizes the risk of security incidents — An information security policy helps organizations define procedures for identifying and mitigating vulnerabilities and risks. It also details quick responses to minimize damage during a security incident.

Executes security programs across the organization — Information security policies provide the framework for operationalizing procedures.

Provides a clear security statement to third parties — Information security policies summarize the organization's security posture and explain how the organization protects IT resources and assets. They facilitate quick response to third-party requests for information by customers, partners, and auditors.

Helps comply with regulatory requirements — Creating an information security policy can help organizations identify security gaps related to regulatory requirements and address them.

12 Elements of an Information Security Policy

A security policy can be as broad as you want it to be, from everything related to IT security and the security of related physical assets, but enforceable in its full scope. The following list offers some important considerations when developing an information security policy.

1. Purpose

First state the purpose of the policy, which may be to:

Create an overall approach to information security., especially as touches standards, security requirements, and best practices adopted by the organization.

Detect and preempt information security breaches such as misuse of networks, data, applications, and computer systems.

Maintain the reputation of the organization, and uphold ethical and legal responsibilities and applicable governance.

Respect employee and customer rights, including how to react to inquiries and complaints about non-compliance.

2. Audience

Define the audience to whom the information security policy applies. You may also specify which audiences are out of the scope of the policy (for example, staff in another business unit which manages security separately may not be in the scope of the policy).

3. Information security objectives

Guide your management team to agree on well-defined objectives for strategy and security. Information security focuses on three main objectives:

Confidentiality — Only authenticated and authorized individuals can access data and information assets.

Integrity — Data should be intact, accurate and complete, and IT systems must be kept operational.

Availability — Users should be able to access information or systems when needed.

4. Authority and access control policy

Hierarchical pattern — A senior manager may have the authority to decide what data can be shared and with whom. The security policy may have different terms for a senior manager vs. a junior employee or contractor. The policy should outline the level of authority over data and IT systems for each organizational role.

Network security policy — Critical patching and other threat mitigation policies are approved and enforced. Users are only able to access company networks and servers via unique logins that demand

authentication, including passwords, biometrics, ID cards, or tokens. You should monitor all systems and record all login attempts.

5. Data classification

The policy should classify data into categories, which may include "top secret," "secret," "confidential," and "public." The objectives for classifying data are:

To understand which systems and which operations and applications touch on the most sensitive and controlled data, to properly design security controls for that hardware and software (see 6.)

To ensure that sensitive data cannot be accessed by individuals with lower clearance levels

To protect highly important data, and avoid needless security measures for unimportant data

6. Data support and operations

Data protection regulations — systems that store personal data, or other sensitive data — must be protected according to organizational standards, best practices, industry compliance standards, and relevant regulations. Most security standards require, at a minimum, encryption, a firewall, and anti-malware protection.

Data backup — Encrypt data backup according to industry best practices, both in motion and at rest. Securely store backup media, or move backup to secure cloud storage.

Movement of data — Only transfer data via secure protocols. Encrypt any information copied to portable devices or transmitted across a public network.

7. Security awareness and behavior

Share IT security policies with your staff. Conduct training sessions to inform employees of your security procedures and mechanisms, including data protection measures, access protection measures, and sensitive data classification.

Social engineering — Place a special emphasis on the dangers of social engineering attacks (such as phishing emails or informational requests via phone calls). Make all employees responsible for noticing, preventing, and reporting such attacks.

Clean desk policy — Secure laptops with a cable lock. Shred sensitive documents that are no longer needed. Keep printer areas clean so documents do not fall into the wrong hands.

Work with HR to define how the internet should be restricted both on work premises and for remote employees using organizational assets. Do you allow YouTube, social media websites, etc.? Block unwanted websites using a proxy.

8. Encryption policy

Encryption involves encoding data to keep it inaccessible to or hidden from unauthorized parties. It helps protect data stored at rest and in transit between locations and ensure that sensitive, private, and proprietary data remains private. It can also improve the security of client-server communication. An encryption policy helps organizations define:

The devices and media the organization must encrypt

When encryption is mandatory

The minimum standards applicable to the chosen encryption software

9. Data backup policy

A data backup policy defines rules and procedures for making backup copies of data. It is an integral component of overall data protection, business continuity, and disaster recovery strategy. Here are key functions of a data backup policy:

Identifies all information the organization needs to back up

Determines the frequency of backups, for example, when to perform an initial full backup and when to run incremental backups

Defines a storage location holding backup data

Lists all roles in charge of backup processes, for example, a backup administrator and members of the IT team

10. Responsibilities, rights, and duties of personnel

Appoint staff to carry out user access reviews, education, change management, incident management, implementation, and periodic updates of the security policy. Responsibilities should be clearly defined as part of the security policy.

11. System hardening benchmarks

The information security policy should reference security benchmarks the organization will use to harden mission-critical systems, such as the Center for Information Security (CIS) benchmarks for Linux, Windows Server, AWS, and Kubernetes.

12. References to regulations and compliance standards

The information security policy should reference regulations and compliance standards that impact the organization, such as the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), Payment Card Industry Data Security Standard (PCI DSS), the Sarbanes-Oxley Act (SOX), and the Health Insurance Portability and Accountability Act (HIPAA).

best practices for successful information security policies

Information and data classification — helps an organization understand the value of its data, determine whether the data is at risk, and implement controls to mitigate risks

Developers, security, and IT operations — should work together to meet compliance and security requirements. Lack of cooperation between departments may lead to configuration errors. Teams that work together in a DevSecOps model can coordinate risk assessment and identification throughout the software development lifecycle to reduce risks.

Security incident response plan — helps initiate appropriate remediation actions during security incidents. A security incident strategy provides a guideline, which includes initial threat response, priorities identification, and appropriate fixes.

SaaS and cloud policy — provides the organization with clear cloud and SaaS adoption guidelines, which can provide the foundation for a unified cloud ecosystem and standards of configuration, especially for development environments. This policy can help mitigate ineffective complications and poor use of cloud resources.

Acceptable use policies (AUPs) — helps prevent data breaches that occur through misuse of company resources. Transparent AUPs help keep all personnel in line with the proper use of company technology resources.

Identity and access management (IAM) regulations — let IT administrators authorize systems and applications to the right individuals and let employees know how to use and create passwords in a secure way. A simple password policy can reduce identity and access risks.

Data security policy — outlines the technical operations of the organization and acceptable use standards in accordance with all applicable governance and compliance regulations.

Privacy regulations — government-enforced regulations such as GDPR and CCPA protect the privacy of end users. Organizations that don't protect the privacy of their users risk fines and penalties, and in some cases court action.

Personal and mobile devices — Nowadays, most organizations have moved business processes to the cloud. Companies that permit employees to access company software assets from any location from any device risk introducing vulnerabilities through personal devices such as laptops and smartphones.

Creating a policy for proper security of personal devices can help prevent exposure to threats via employee-owned assets.