E-COMMERCE & DIGITAL SECURITY
Assignment-12

N Ravinder Reddy
Roll No: 2406CYS106

Unit 3 - DIGITAL DEVICES SECURITY

Assignment Questions.

Syllabus:

Device and Mobile Security: End Point device and Mobile phone security, Password policy, Security patch management, Data backup, Downloading and management of third-party software, and Device security policy.

Tools and Technologies for Cyber Security: Authentication tools, firewalls, intrusion detection systems, and antivirus and encryption software.

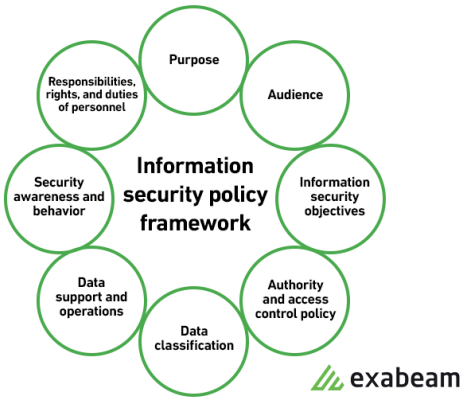
Cyber Security Best Practices: Cyber Security best practices, Significance of host firewall and Anti-virus, management host firewall and Anti-virus, Wi-Fi security, Configuration of basic security policy and permissions.

Device and Mobile Security:

1Q. Essay Question:

Explore the importance of device and mobile security in today's digital landscape. Discuss the various threats and vulnerabilities faced by mobile devices, including malware, phishing attacks, and data breaches. Explain the significance of implementing security measures such as encryption, biometric authentication, and secure boot processes to protect against these threats. Additionally, analyzes the role of user education and awareness in enhancing device security. Provide examples of best practices and case studies to illustrate effective strategies for mitigating risks to mobile and IoT devices.

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.



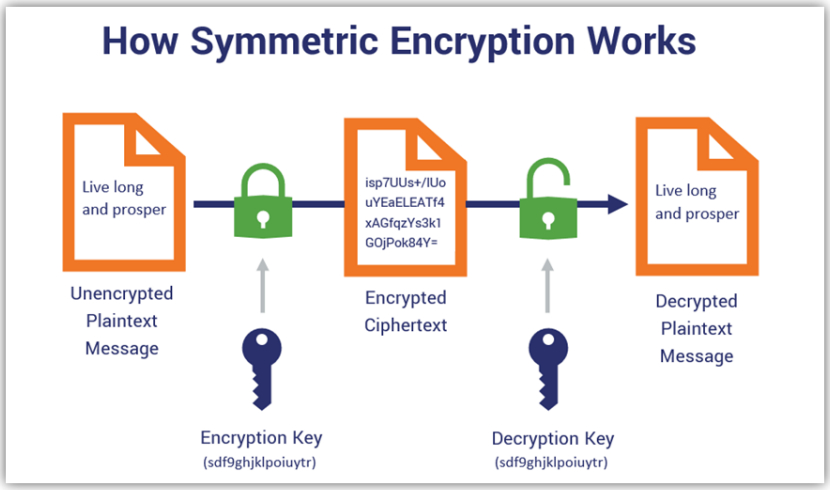
What is mobile security (wireless security)?

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.

Why is 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.

Incorporating security measures from the start ensures a comprehensive and robust approach to cyber security. By integrating security considerations into the design and development phases of a system or application, potential vulnerabilities can be identified and addressed early on, reducing the risk of cyber attacks.

1. Data Security:
   - Definition: Data security involves protecting digital data from unauthorized access, use, or disclosure, consistent with an organization's risk strategy. It also includes safeguarding data from disruption, modification, or destruction.
   - Significance:
     - Confidentiality: Encryption ensures that sensitive data remains confidential even if unauthorized parties gain access.
     - Integrity: Measures like secure boot processes prevent unauthorized modifications to system files.
     - Availability: Proper security practices prevent disruptions that could lead to data unavailability.
   - Best Practices:
     - Encryption: Encrypt data at rest (e.g., using AES-256) and during transmission (e.g., TLS/SSL).
     - Access Controls: Limit access based on roles and permissions.
     - Regular Backups: Ensure data availability by backing up critical information.
   - Example Case Study:
     - Equifax Data Breach (2017): A lack of proper security controls led to unauthorized access, exposing sensitive data of 147 million consumers[1].
2. Biometric Authentication:
   - Definition: Biometric authentication uses unique physical or behavioral traits (e.g., fingerprints, facial recognition) for user identification.
   - Significance:
     - Strong Authentication: Biometrics provide robust authentication, reducing reliance on easily compromised passwords.
     - User Convenience: Users find biometrics more convenient than remembering complex passwords.
   - Best Practices:
     - Multi-Factor Authentication (MFA): Combine biometrics with other factors (e.g., PIN or token).
     - Liveness Detection: Prevent spoofing by verifying that the biometric sample is from a live person.
   - Example Case Study:

- Apple's Face ID: Face recognition on iPhones combines security and user convenience[2].

3. Secure Boot Processes:
   - Definition: Secure boot ensures that only trusted software components load during system startup.
   - Significance:
     - Preventing Malware: Secure boot prevents unauthorized or malicious code execution.
     - Chain of Trust: Establishes a secure chain from firmware to OS.
   - Best Practices:
     - Signed Bootloaders: Use cryptographically signed bootloaders.
     - Hardware Root of Trust: Leverage hardware-based security modules (e.g., TPM).
   - Example Case Study:
     - UEFI Secure Boot: Modern PCs use UEFI firmware with secure boot to prevent rootkits[3].
4. User Education and Awareness:
   - Role:
     - Educated users make informed decisions, reducing the likelihood of falling victim to social engineering attacks.
     - Awareness campaigns foster a security-conscious culture.
   - Best Practices:
     - Phishing Training: Regularly train users to recognize phishing emails.
     - Security Policies: Communicate security policies and best practices.
   - Example Case Study:
     - Google's Phishing Quiz: An interactive quiz educates users about phishing techniques.

Tools and Technologies for Cyber Security:

1Q. Case Study Question:

Select a recent cyberattack incident and analyze the tools and technologies that were utilized by the attackers. Describe the attack vector, the tools employed (e.g., malware, penetration testing frameworks, exploit kits), and the techniques used to exploit vulnerabilities. Evaluate the effectiveness of the defensive measures in place at the targeted organization and assess the lessons learned from the incident. Based on your analysis, propose recommendations for enhancing the organization's cybersecurity posture, including the adoption of specific tools and technologies to prevent similar attacks in the future.

Ans:

1. ICBC Financial Services ransomware attack

Date: November 2023

Impact: Disruption of the US Treasury market

In November, a subsidiary of the Industrial and Commercial Bank of China (ICBC), the ICBC Financial Services, experienced a ransomware attack that disrupted some operating systems, including those used to clear US Treasury trades and repo financing. As a result of this disruption, the brokerage was unable to settle trades for other market players and temporarily owed BNY Mellon $9 billion.

This not only highlights the growing payment interruption risk that financial institutions face due to cybersecurity incidents — it also reflects the increasing scale of such incidents. Because financial systems and business operations are increasingly interconnected, the impact of a cyber attack is rarely limited to the target organization. Instead, it has a ripple effect that can affect organizations and economies across the world.

The attack on ICBC Financial Services, for example, disrupted the US Treasury market, which plays a crucial role in global finance.

Key learning

Cyber attacks like this are expected to increase as threat actors continue to target important financial institutions and infrastructure in major economies. If successful, an attack on one organization can impact partners, suppliers, and customers across the globe.

This emphasizes the importance of supply chain risk management. Supply chain risk management involves identifying and assessing threats throughout the supply chain and developing mitigation strategies to protect the integrity, trustworthiness, and authenticity of products and services within that chain. Having a defined process in place can help your organization minimize the likelihood and magnitude of these risks to the supply chain.

2. MGM Resorts phishing attack

Date: September 2023

Impact: Over $100 million in financial losses

After detecting a cyber attack that disrupted its operations in late September 2023, MGM Resorts International shut down its systems to contain the damage. It then reported that it would take a $100 million hit to its third-quarter results, as it worked to restore its systems. The casino giant also expected to incur a one-time cost of approximately $10 million related to the attack.

It appears that the hackers used a social engineering technique known as vishing. After finding an employee's information on LinkedIn, the hackers

impersonated the employee in a call to MGM's IT help desk to obtain credentials to access and infect the systems.

Key learning

Social engineering attacks are expected to increase in sophistication and frequency due to AI, which enables threat actors to create more convincing and legitimate sounding phishing emails, deepfakes, vishing calls, and more.

Organizations that extensively use AI and automation to enhance their cybersecurity capabilities will be best positioned to defend against this weaponized use of AI by cybercriminals. In a study by Capgemini Research Institute, 69% of executives said that AI is necessary to effectively respond to cyberattacks and results in higher efficiency for cybersecurity analysts.

3. Boeing ransomware attack

Date: October 2023

Impact: 43GB data leak

In October 2023, Boeing, one of the world's largest defense and space contractors, suffered a cyber attack that impacted its parts and distribution business. This attack was traced to a vulnerability in Citrix's software, known as Citrix Bleed, that was exploited by the ransomware group LockBit 3.0. LockBit later leaked more than 43 gigabytes of data allegedly stolen from Boeing's system when the aerospace company refused to pay the demanded ransom.

Exploitation of CitrixBleed impacted other major organizations as well, including the U.S. branch of ICBC and logistics firm DP World. The majority of affected systems were reported to be located in North America. It's estimated that US organizations hit by LockBit paid as much as $90 million in ransom between 2020 and mid-2023.
As a result of the incident at Boeing, the Cybersecurity and Infrastructure Security Agency (CISA), the FBI, and Australian Cyber Security Center issued a cybersecurity advisory urging organizations to patch against the actively exploited flaw immediately if they haven't done so already.

Key learning

In October, Citrix posted a security bulletin rating the bug a 9.4 out of 10 on the CVSS severity scale. However, in November, thousands of instances where the tool was used were still vulnerable to the issue, including nearly 2,000 in North America alone. There was widespread exploitation of the Citrix vulnerability in unpatched software services throughout both private and public networks as a result.

Managing exposure to discovered vulnerabilities is a key aspect of vulnerability management, alongside discovering, categorizing, and prioritizing vulnerabilities and analyzing the root cause of vulnerabilities. Having a robust vulnerability management program can help an organization develop a comprehensive understanding of its risk profile, understand what controls need to be implemented for risk mitigation, and prevent repeat vulnerabilities.

4. The British Library ransomware attack

Date: October 2023

Impact: Major disruptions to systems and operations and 600GB data leak

The UK's largest library was hit by a cyber attack on the last weekend of October. While the British Library took immediate action to isolate and protect its network, its online systems and services were massively disrupted, its website went down, and it initially lost access to even basic communication tools such as email.

On January 15, it began a phased return of certain key services, starting with the restoration of a reference-only version of its main catalog. However, the disruption to some of its operations is expected to persist for months, possibly until next fall or even longer.

In total, the cost of recovering the British Library's IT systems is estimated to be as high as £7 million, which represents about 40% of its unallocated cash reserves.

Key learning

To help prevent lengthy and costly recoveries in the event of a successful ransomware attack, organizations must update their cyber resiliency measures, including putting a disaster recovery plan in place.

Having a disaster recovery plan in place that is well-designed and regularly maintained can help organizations minimize downtime, reduce financial losses, protect critical data, and provide peace of mind for employees.

In cybersecurity, an attack vector refers to the specific pathways or methods that cybercriminals employ to breach a computer system, network, or application's security. These vectors serve as the entry points into valuable data, making them a priority for cybersecurity professionals to address.

An attack vector is the method or combination of methods that cybercriminals use to breach or infiltrate a victim's network.

Adversaries typically develop an arsenal of attack vectors that they routinely use to carry out their attacks. Over time and with repeated use, these attack vectors can become virtual “calling cards” for cybercriminals or organized eCrime gangs, making it possible for threat intelligence analysts, cybersecurity service providers, law enforcement, and government agencies to assign an identity to different adversaries.

Recognizing and tracking an adversary’s attack vectors can help organizations better defend against existing or upcoming targeted attacks. In addition, knowing who is behind an attack — determined in part by their use of a signature attack vector — can help the organization understand the adversaries’ capabilities and take steps to protect the business and its assets in the future.

Attack vector vs attack surface vs threat vector vs threat actor
What is an attack surface?

An attack surface is the sum of all possible security risk exposures in an organization’s environment. Put another way, it is the collective of all potential vulnerabilities (known and unknown) and controls across all hardware, software, network components, and people.

Attack surfaces can be categorized into three basic types:

1. Digital attack surface: Encompasses the entire network and software environment of an organization. It can include applications, code, ports, and other entry and exit points.
2. Physical attack surface: All of an organization’s infrastructure such as desktop systems, laptops, mobile devices, servers, access gates, telco infrastructure, and even electrical feeds.
3. Social engineering attack surface: Attacks that exploit the human mind, used often in phishing, pretexting (smishing), vishing (voicemail), and other manipulative techniques to mislead the human

What is a threat vector?

Threat vector is a term used to describe the method a cybercriminal uses to gain initial access to a victim network or infrastructure. Threat vector is often used interchangeably with attack vector.

What is a threat actor?

A threat actor, also known as a malicious actor or digital adversary, is any person or organization that intentionally causes harm in the digital sphere. They exploit weaknesses in computers, networks, and systems to carry out disruptive attacks on individuals or organizations.

The term “threat actor” includes cybercriminals, but it is much broader. Ideologues such as hacktivists (hacker activists), terrorists, insiders, and even internet trolls are all considered threat actors.

How to secure attack vectors

There is a wide range of attack vectors, each of which exploits a specific vulnerability, be it a person, unpatched software, misconfigured service, or a weak password. There is no single defense mechanism that will protect the organization from all attack types. Further, it is important to recognize that many attack vectors target people, which means that most security tools, no matter how advanced, will be of limited use in protecting the organization from such techniques.

The mix of digital and personal attack vectors is why it is so important for organizations to take a comprehensive approach to security and incorporate a mix of preventative, defensive, proactive, and reactive security measures to best protect the organization and its assets. Here we share a list of best practices for developing and deploying a comprehensive security strategy:

1. Develop a robust employee cybersecurity training program.

Employees are on the front line of your security. Make sure they follow good hygiene practices — such as using strong password protection, connecting only to secure Wi-Fi, and being on constant lookout for phishing attacks — on all of their devices. Provide comprehensive and regular security awareness training sessions to ensure they understand the evolving threat landscape and are taking the necessary steps to protect themselves and the company from all forms of cyber risk.

2. Track the operating system configuration and keep all software patched and up to date.

Hackers are constantly looking for holes and backdoors to exploit. By vigilantly updating your systems, you’ll minimize your exposure to known risks and limit attack vectors that utilize misconfigurations and other IT vulnerabilities as a pathway.

3. Prioritize Cloud Protection

Adversaries are aggressively targeting cloud infrastructure. The number of observed cloud exploitation cases grew and adversaries are using a broad array of TTPs (e.g., misconfigurations, credential theft, etc.) to compromise critical business data and applications in the cloud. Stopping cloud breaches requires agentless capabilities to protect against misconfiguration, control plane and identity-based attacks, combined with runtime security that protects cloud workloads.

4. Continuously monitor the environment for malicious activity and indicators of attack (IOAs).

Enable an endpoint detection and response (EDR) system to monitor all endpoints, capturing raw events for automatic detection of malicious activity not identified by prevention methods.

5. Integrate threat intelligence into the security strategy.

Monitor systems in real time and keep up with the latest threat intelligence to identify the adversary universe that may be targeting your organization. Data on a threat actor's next move is crucial to proactively tailoring your defenses and preempting future attacks.

6. Protect against identity-based attacks

Enable full, real-time visibility into the AD, both on-premises and in the cloud, and identify shadow administrators, stale accounts, shared credentials, and other AD attack paths.

Harden AD security and reduce risks by monitoring authentication traffic and user behavior and enforce robust security policies to proactively detect anomalies.

Enable continuous monitoring for credential weakness, access deviations, and password compromises with dynamic risk scores for every user and service account.

7. Extend multi factor authentication (MFA) security

Protect unmanaged endpoints with risk-based conditional access and extend multifactor authentication (MFA) protection to legacy applications and tools using proprietary analytics on user behavior and authentication traffic.

Enforce consistent risk-based policies to automatically block, allow, audit, or step up authentication for every identity.

8. Create a baseline of user activity

Centralize user activity and behavior across all relevant data logs, including access, authentication, and endpoint.

Leverage this data to create a baseline of activity for each individual user, user group, function, title, and device that can help identify unusual or suspicious activity.

Assign a customized risk score to each user and endpoint to provide additional context to the cybersecurity team.

9. Leverage behavior analytics and AI to identify threats

Leverage analytics and AI-enabled tools to monitor behavior for users and devices in real time.

Cross reference alerts with the risk score to provide additional context into the event and prioritize response efforts.

10. Practice makes perfect

Execute red team/blue team exercises. While technology is clearly critical in the fight to detect and stop intrusions, security teams are the crucial link in the chain to stop breaches. For security teams, practice makes perfect. Encourage an environment that routinely performs tabletop exercise and red/blue teaming to identify gaps and eliminate weaknesses in your cybersecurity practices and response. And security teams shouldn't be the only ones practicing — initiate user-awareness programs to combat the continued threat of phishing and related social engineering techniques.

Identifying Attack Vectors with CrowdStrike

At CrowdStrike, we believe that a key part of preventing and defending against cyberattacks is understanding the adversaries who may target your organization and the attack vectors they rely on.

We offer robust actor profiling services so we can identify the adversaries that may target our clients, as well as their capabilities and intentions. This allows us to develop customized strategies with our customers to protect their data and assets most at risk and strengthen defenses in the areas most often exploited by threat actors.

As part of our Human Intelligence (HUMINT) offerings, we developed the CrowdStrike Adversary Universe to help organizations better understand the humans behind these attacks and the methods they use.

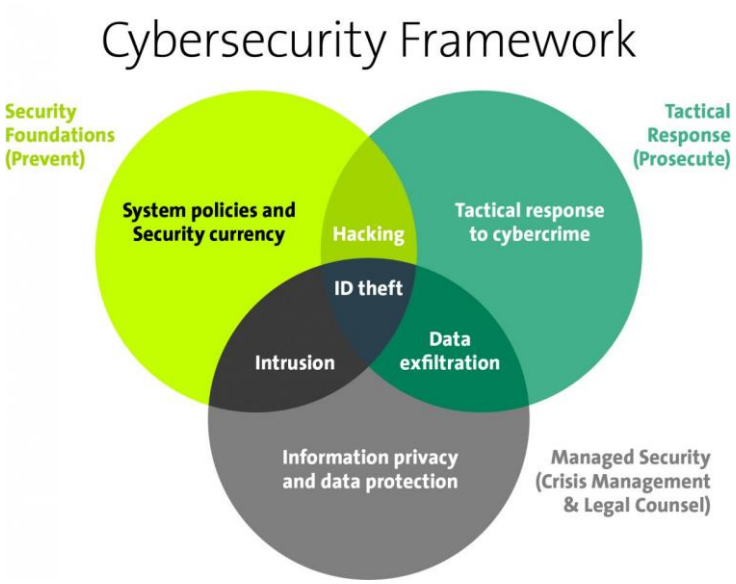
Cyber Security Best Practices:

1Q. Policy Development Question:

Imagine you are tasked with developing a comprehensive cyber security policy for a medium-sized organization. Outline the key components that should be included in the policy, such as access control, data protection, incident response, and employee training. Discuss the importance of each component and provide examples of specific policies or procedures that could be implemented to mitigate cyber security risks. Additionally, address the challenges of policy enforcement and compliance monitoring within the organization. Finally, propose strategies for ensuring the ongoing effectiveness of the cyber security policy in the face of evolving threats and technologies.

Ans:

Six steps to Building a Cyber Security Policy for small and mediumsized Enterprises Developing a robust cyber security policy is crucial to protect your business's valuable data, maintain customer trust, and ensure business continuity. This article outlines six key steps for SMEs to create an effective cyber security policy that mitigates risks and safeguards their operations.



1. Assess your vulnerabilities through regular IT auditing Start by conducting a thorough assessment of your business's unique cybersecurity vulnerabilities. Regular IT system audits identify potential entry points for cyberattacks, such as outdated software, weak passwords, or inadequate employee training. Consider the types of data you handle, including customer and supply chain information, financial records, and intellectual property. Understanding your vulnerabilities will guide your policy development and help prioritize security measures.

2. Set clear goals and objectives Establish clear goals and objectives for your cyber security policy. Define what you aim to achieve, such as protecting sensitive data, ensuring regulatory compliance, and minimising business

disruptions. Ensure that your policy aligns with industry best practices and relevant compliance standards, such as the General Data Protection Regulation (GDPR). Setting specific objectives provides a framework for policy implementation and evaluation.

3. Define roles and responsibilities Clearly define the roles and responsibilities for each employee regarding cyber security within your business. Identify who will be responsible for policy development, implementation, monitoring, and incident response. Assign specific individuals or teams to oversee cyber security tasks and establish reporting protocols to ensure accountability. Clearly defining roles helps ensure that everyone understands their responsibilities and ensures your business fosters a culture of cyber security awareness.

4. Establish best practices Develop best practices that address the specific vulnerabilities you identified during the assessment and audit stage. This may include enforcing strong password policies, implementing multi-factor authentication, regularly updating software and systems, and securing network infrastructure. Employee education surrounding safe browsing habits, phishing awareness, and social engineering tactics. Implement measures to protect against malware, including firewalls, antivirus software, and intrusion detection systems.

Figure 2. Cyber security approach as set out in the guidelines

5. Employee training and awareness One of the most critical elements of a cyber security policy is employee training and awareness. Conduct regular training sessions to educate employees about the importance of cyber security, common threats, and best practices. Emphasise the significance of identifying and reporting potential security incidents promptly. Encourage a culture of cyber security awareness by promoting ongoing education and providing resources such as posters, newsletters, and awareness campaigns.

6. Incident response and recovery Develop a cyber response plan that outlines the steps to be taken in the event of a cyber security incident. This plan should include procedures for containing and mitigating the incident, notifying relevant parties, preserving evidence, and initiating recovery

processes. Regularly test and update your plan, using ‘playbooks’ to ensure its effectiveness. Building a cyber security policy is a proactive step that SMEs must take to protect their operations, customers, supply chain and reputation. By assessing vulnerabilities, setting clear goals, defining roles, implementing security controls, training employees, and preparing for incident response and recovery, SMEs can establish a strong foundation for cyber security. Remember that cyber security is an ongoing concern, and regular review and updates to your policy are essential to keep up with evolving threats. If you need support with any of the points raised in this article, please get in touch with one of our engineers. We’re happy to have a conversation about how you can better protect your business