Learn to Hack Cybersecurity Training

A complete guide to employee safety and best practices online.
Written and presented by: Derek Johnston

1. Introduction to Cybersecurity:

i) Overview of Cybersecurity

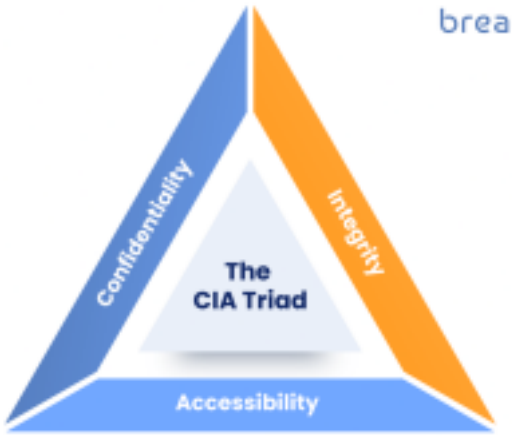
What is Cybersecurity?

Cybersecurity is the practice of protecting digital hardware, software, networks and data from unauthorized access, attacks, and damage. In today's digital age, cybersecurity is critical for safeguarding personal, organizational, and sensitive information. Due to the evolving nature of technology as well as its increasing accessibility, there has never been as much need for cybersecurity awareness as there is today.

For example, the US National Cyber Security Alliance found that 60% of small businesses went out of business within six months of a cyberattack, with less than half being able to reclaim data after being hacked. [1] In addition in Canada, 85% of companies were affected by successful attacks in one year.

Today, there are a wide range of practices, technologies, and measures designed to protect digital systems, networks, and data from unauthorized access, attacks, damage, or theft. Primarily, it involves safeguarding information and systems from a variety of threats, ensuring their confidentiality, integrity, and availability.

The CIA triad is a useful way to remember these concepts as part of a working whole. Just implementing measures to provide confidentiality alone is not enough, it is by combining many different layers (Defense in depth) that cyber attacks can be more effectively combated and prevented.



Looking at the triad at a closer level, we have:

1. Confidentiality - > ensuring that information is accessible only to those who are authorized to access it.

2. Integrity - > ensuring that information remains unaltered, accurate and reliable.

3. Availability - > ensuring that information and resources are accessible and usable by authorized users when needed.

The above triad can be used to effectively guide policies within an organization and is a useful framework for organizations to assess and implement security measures.

So what are the individual elements that make up the practice of cybersecurity?

Key components include:

• **Network Security**:
Protecting networks from unauthorized access, intrusion, and threats.

• **Endpoint Security:**
Securing individual devices such as computers, smartphones, and tablets with antivirus software, encryption, and regular updates.

• **Application Security:**

Ensuring that software and applications are developed, tested, and maintained well enough to prevent vulnerabilities and unauthorized access.

• **Data Security:**

Protecting sensitive data from unauthorized access or theft through encryption, access controls, data masking, and secure storage practices.

• **Identity and Access Management (IAM):**

Managing and controlling user access to systems and data to prevent unauthorized entry.

• **Cloud Security:**

Implementing security measures to protect data stored in cloud environments.

• **Incident Response:**

Developing plans and procedures to respond effectively to cybersecurity incidents.

• **Security Awareness and Training:**

Educating employees and users about cybersecurity best practices, potential threats, and their role in maintaining a secure environment.

• **Regulatory Compliance:**

Ensuring compliance with industry-specific regulations and standards related to cybersecurity, such as GDPR, HIPAA, and PCI DSS.

• **Security Monitoring and Analytics:**

Implementing tools and processes to continuously monitor networks, systems, and data for potential security threats or anomalies and use analytics to detect and respond to these threats.

Ultimately, Cybersecurity is a dynamic field that evolves with the changing threat landscape. Implementing a comprehensive cybersecurity strategy involves a combination of all components tailored to an organization's specific risk profile, industry, and technological infrastructure.

ii) Importance of Cybersecurity for Small Businesses:

In 2023, it was found that up to 36% more small businesses are being targeted in cyberattacks.

Moreover, 70% of small firms are not prepared for them (Hiscox Cyber Readiness Report). In a small business context, understanding and implementing basic cybersecurity measures are essential to safeguard sensitive information and maintain operational integrity.

Why is Cybersecurity important for small businesses?

1. Protection of Sensitive Data: Safeguarding customer information, financial data, and intellectual property.
Small businesses often store customer information, financial data, and proprietary knowledge. Protecting this information is critical to maintaining trust and credibility.

2. Preserving Reputation: Maintaining trust with customers and stakeholders by demonstrating a commitment to data security.

A data breach can damage the reputation of a small business, leading to loss of customer trust. Protecting data enhances reputation and builds confidence among customers and partners.

3. Financial Loss Mitigation: Cyber attacks can lead to significant financial losses for small businesses.

The costs associated with data breaches, including recovery, legal fees and potential fines, can be crippling. Implementing cybersecurity measures helps minimize these risks.

4. Business Continuity: Minimizing disruptions caused by cyber incidents, ensuring uninterrupted operations.

Implementing cybersecurity measures, such as backups and recovery plans, ensures business continuity even in the face of cyber threats.

5. Compliance and Legal Obligations: Small businesses are often subject to various regulations regarding data protection and privacy.

Implementing cybersecurity measures ensures compliance with these regulations, reducing the risk of legal repercussions and fines.

A strong cybersecurity foundation is essential for the protection and sustainability of a small business. By fostering a culture of awareness and vigilance amongst employees, businesses can significantly reduce the risk of cyber threats.

Common Cyber Threats for Small Businesses:

For small businesses, several common cybersecurity threats pose significant risks:

1) Phishing Attacks:

These are emails, messages, or websites that impersonate legitimate entities to trick users into revealing sensitive information or installing malware. Phishing attacks are often targeted and can lead to data breaches or financial losses.

2) Ransomware:

This is malicious software that encrypts a company's files or systems, rendering them inaccessible until a ransom is paid. Ransomware attacks can disrupt business operations and cause financial damage.

3) Insider Threats:

Risks posed by employees, contractors, or anyone with internal access to the company's systems. This could involve intentional actions (malicious intent) or unintentional mistakes that compromise security.

4) Weak Password and Credential Theft:

Poor password practices, such as using weak passwords or reusing them across multiple accounts, can lead to credential theft. Attackers might then use these credentials to gain unauthorized access to systems.

5) Unpatched Software and System Vulnerabilities:

Failure to update software or apply security patches leaves systems vulnerable to exploitation by cyber attackers who target known vulnerabilities.

6) Lack of Security Awareness:

Employees who are not adequately trained in cybersecurity best practices can inadvertently click on malicious links, download infected files, or fall victim to social engineering attacks.

7) Third-party and Supply Chain Risks:
Small businesses often rely on third-party vendors for various services. Compromised vendors and supply chain partners can introduce security risks to the business.

iii) Basic Terminology and Concepts:

Now that we understand more about Cybersecurity and its importance for small businesses, let's visit some basic but key terminology and concepts.

-> Malware:
Malicious software designed to harm or exploit computers, networks, and devices. Types include viruses, worms, ransomware, trojans, and spyware.

One of the earliest known examples of malware was the 'Morris Worm' created by Robert Tappan Morris in 1988 which led to the development of computer emergency response teams or 'CERTS'.

-> Phishing:
A form of social engineering where attackers use deceptive emails, messages, or websites to trick individuals into revealing sensitive information or performing actions that compromise security.

-> Firewall:
A security barrier between a trusted internal network and untrusted external networks (like the internet) that monitors and controls incoming and outgoing network traffic based on predefined security rules.

-> Encryption:

The process of converting data into a code to prevent unauthorized access or interception. Encrypted data can only be accessed by those with the appropriate decryption key.

The largest encryption keys used in practice today are typically 4096 bits for asymmetric encryption algorithms like RSA or Diffie-Hellman.

-> Authentication:

The process of verifying the identity of users or systems attempting to access resources. This can involve passwords, biometrics, tokens, or multi-factor authentication (MFA).

-> Vulnerability:

Weaknesses or flaws in systems, software, or configurations that can be exploited by attackers to compromise security and gain unauthorized access.

CVSS (Common Vulnerability Scoring System) is a framework used to assess and communicate the severity of security vulnerabilities in software or systems.

-> Patch:

Software updates are released by vendors to fix security vulnerabilities or bugs in their software. Regularly applying patches helps mitigate known security risks.

-> Incident Response:

The process of responding to and managing cybersecurity incidents, including detecting, containing, eradicating, and recovering from security breaches.

-> Access Control:

Measures that restrict and manage user access to resources, ensuring that only authorized users have appropriate permissions.

-> Penetration Testing:

Ethical hacking techniques are used to identify vulnerabilities in systems and networks by simulating real-world cyberattacks.

-> Security Policy:

A set of rules, guidelines, and procedures established by an organization to ensure information security and guide employee behavior related to security.

-> Cyber Threat Intelligence:

Information about potential or current cybersecurity threats and risks obtained through monitoring, analysis, and research to help organizations prepare and respond effectively to threats.

-> Social Engineering:

Manipulating people to divulge confidential information through psychological tactics.

-> Denial of Service (DoS) Attacks:

Overloading systems and networks to disrupt service availability.

Understanding these basic terms and concepts provides a foundation for grasping the broader landscape of cybersecurity and is essential for anyone involved in securing systems, data, or networks.

For a more comprehensive glossary, you can refer to this glossary from SANS Institute: https://www.sans.org/security-resources/glossary-of-terms.

2. Cyber Threat Landscape:

The 'Cyber Threat Landscape' refers to the entire scope of possible threats that can impact individuals, organizations or specific industries at a particular time.

As new threats become known, the Cyber Threat Landscape adjusts accordingly.

For small businesses, it is important to create a cybersecurity strategy that is robust enough to deal with a changing Cyber Threat Landscape in order to be able to respond to and mitigate potential attacks effectively.

Part of this involves understanding and knowing about the various different types of malware that can infiltrate and cause damage to devices, networks and software that a company may be using.

i) Types of Cyber Threats:

Malware, short for '*malicious software*', refers to a broad category of software specifically designed to harm, disrupt, or gain unauthorized access to computers, networks, and devices.
Malware can take various forms and carry out different malicious activities, often without the knowledge or consent of the user.

Here are some common types of malware:

1) Viruses:
These are malicious programs that attach themselves to legitimate files and spread when those files are executed. Viruses can corrupt or delete data, or even take control of the infected system.

The 'ILOVEYOU' virus, also known as the Love Bug, is an example of a virus that exploited systems in May 2000 via email inboxes and the file 'LOVE-LETTER-FOR-YOU.txt.vbs'. When the (.vbs) file was opened, virus code was executed, spreading to address book contacts and overwriting other files on the system.

2) Worms:
This is self-replicating malware that spreads across networks without human intervention. Worms can exploit vulnerabilities to infect multiple devices.

The Morris Worm, created by Robert Tappan Morris in 1988, was one of the earliest and most well-known examples of a computer worm. It was created to gauge the size of the internet by exploiting vulnerabilities in Unix systems. Due to a flaw in the worm's code, it ended up spreading more aggressively than originally intended, causing system slowdowns and disruptions.

3) Trojans:

Trojans are a common and versatile form of malware used disguised as legitimate software to trick users into installing it. Once installed, trojans can steal data, create backdoors for attackers, spy on user activities and modify system settings.

The 'Zeus' Trojan also known as 'Zbot' is a notable example of a sophisticated banking Trojan that emerged around 2007. It was designed to steal sensitive financial information, particularly online banking credentials. Stolen information was then transmitted to command-and-control servers operated by cybercriminals.

4) Ransomware:
Malware that encrypts files or locks users out of their systems until a ransom is paid. This can severely disrupt operations and cause data loss.

'WannaCry' is a prominent example of Ransomware that also used worm techniques to spread and infect systems, emerging in May 2017. It targeted Windows operating systems, exploiting a vulnerability called EternalBlue. This exploit targeted a vulnerability in the Server Message Block (SMB) protocol. After spreading rapidly across networks, WannaCry encrypted files on a victim's computer and demanded a ransom in Bitcoin for decryption.

5) Spyware:
Malware designed to spy on users' activities, collecting sensitive information like keystrokes, login credentials, or browsing habits without their knowledge.

An example of spyware that was used to exploit systems by Gamma Group is 'FinFisher'. It can be deployed through various means, including phishing emails, fake software updates or exploiting software vulnerabilities. It was notorious for being used by governments and law enforcement agencies for surveillance purposes.

6) Adware:
Software that displays unwanted advertisements or redirects users to advertising websites. While not as harmful as other types, adware can be intrusive and impact system performance.

The 'Superfish' adware came pre-installed on certain Lenovo laptops between September 2014 and January 2015. It was intended for displaying targeted advertisements to users based on their

browsing habits. It worked by installing its own self-signed root certificate authority, enabling it to decrypt and read encrypted data passing through affected browsers. The discovery of Superfish on Lenovo laptops led to a public outcry and prompted the company to issue a removal.

Additional cyber threats that are good to be aware of include:

-> Phishing and social engineering

-> Supply Chain Attacks

-> Insider Threats

-> IoT (Internet of Things) Vulnerabilities

-> Nation-State Attacks

-> Zero-day Exploits

-> AI and Machine Learning threats

Malware can enter systems through various means, including email attachments, malicious websites, software downloads from untrusted sources, infected USB drives, or exploiting software vulnerabilities. Its impact can range from minor annoyances to severe disruptions, data breaches, and financial losses.

Protecting against malware involves using reputable antivirus and antimalware software, keeping systems and software updated with the latest security patches, practicing safe browsing habits, being cautious with email attachments and downloads, and regularly backing up important data to mitigate the potential damage caused by malware infections.

ii) Common Attack Vectors:

An attack vector is a way for an attacker to break into a network or system. Common ones include credential theft, vulnerability exploits and social engineering. A key aspect to information security is minimizing the available attack vector wherever possible to make life harder for the hacker.

Due to the complexity of modern digital systems, eliminating all attack vevectors,s usually not viable. Nonetheless, for a small business who is equipped with practical understanding of the threats and how to mitigate them, they have a good chance of reducing the attack vector considerably to make infiltration a lot less of an issue.

Below are some of the most common attack vectors including suggestions for mitigating or reducing their possible impact.

1. Compromised credentials

-> Mitigating this attack vector is crucial to prevent attackers from leveraging stolen or compromised usernames and passwords to gain unauthorized access.

Mitigate with:

• Multi-factor authentication

• Regularly update and enforce strong password policies

• Implement account lockout and intrusion detection

• Limit privileges and access

• Establish incident response plans

2. Vulnerability exploits

-> Security flaws or weaknesses in software, hardware or other systems that are unknown to the vendor or developers and have no available patches or fixes at the time they are discovered.

Mitigate with:

• Vulnerability management

• Patch management and timely updates

• Network segmentation and least privilege

• Implement defense-in-depth strategies

• Behavioral analytics and anomaly detection

3. Open ports

-> Ports help computers and servers associate network traffic with a given application or process. E.g. HTTP = port 80, HTTPS = port 443.

Mitigate with:

• regular scanning and maintenance of open ports on systems, close unnecessary ports and services

• implement strong firewall rules and access controls to restrict access to open ports

4. Phishing

-> is a type of attack where attackers use deceptive tactics to trick individuals into disclosing sensitive information such as login credentials, financial details or personal information.

Mitigate with:

• Employee training

• Email filtering

• Multi-factor authentication

• Browser protection and security tools

• Continuous monitoring and response

5. Insecure Encryption

-> Poorly encrypted or unencrypted data can potentially be viewed by anyone who has access to the same network.

Mitigate with:

• Strong encryption algorithms and protocols such as AES, RSA or Elliptic Curve Cryptography

• Secure key management

• Regular Security Audits and Assessments

• Regular Updates and Patching

6. Account takeover

-> To take over a user's account, there are many different options available to an attacker. They can steal user credentials via a phishing email, carry out a brute force attack or purchase them on the dark web. In web browsers, session cookies can be intercepted to replay a session and impersonate a user.

Mitigate with:

• Multi-factor authentication

• Regular password changes

• Account lockout policies

• IP Whitelisting and Geolocation Restrictions

• Encryption and secure protocols

7. Insider threats

-> Proximity is power and when it comes to insider threats, the story is no different. Here, a known and trusted user exploits their position to distribute confidential data or helps an attacker do the same. These kinds of events can be both intentional or accidental.

Mitigate with:

• Employee education and awareness

• Access control and least privilege

• Monitoring and auditing

• Segmentation of networks

• Background checks and vetting

8. Email attachments

-> Due to the ease of use in setting up, email attachments are one of the most prolific attack vectors to be aware of. After a user opens a file that has been sent, malicious code can execute and disrupt a system or multiple systems with ease.

Mitigate with:

• Robust email filtering that detects and blocks emails with suspicious files

• Educate users

• Use antivirus and anti-malware

• Regular backups of important data

• Implement authentication protocols such as DMARC, SPF and DKIM

When it comes to potential cybersecurity attacks, working to reduce the available attack vectors that a hacker can employ is a key aspect to improving security whilst reducing risk for an organization.

iii) Understanding Vulnerabilities:

Vulnerabilities are a critical aspect of cybersecurity to be mindful of due to their importance in an attackers' workflow for infiltration into a system. After an attacker has successfully delivered a weaponized bundle to a victim through email, the web or USB, their next step is to exploit a

vulnerability and execute code on the relevant system. By doing this, they will then have the necessary access to carry out further tasks such as installation malware, elevating privileges, moving laterally through the network or performing more reconnaissance.

The Cyber Kill Chain provides a great framework for the full seven steps that an attacker may take beginning with reconnaissance before moving onto:

- Weaponization
- Delivery
- Exploitation
- Installation
- Command & Control (C2)
- Actions on objectives

Without vulnerabilities residing on target systems, networks, software or hardware, hackers would be unable to exploit them and infiltrate their target. Because of this, understanding the
potential dangers and working to update and patch new vulnerabilities as they become known is a critical aspect to having a proactive and effective cybersecurity posture.

Vulnerabilities can exist in many different shapes and forms. Below are the main types to be aware of:

- **Software vulnerabilities:**

- bugs, coding errors or design flaws in software applications or OS's
- can include buffer overflows, SQL injection or insecure deserialization

- **Hardware vulnerabilities:**

-weaknesses in computer hardware devices that can be exploited such as security flaws in CPUs or hardware misconfigurations

- **Network vulnerabilities:**

-weaknesses in network infrastructure or protocols that could be exploited for unauthorized access, data interception or denial-of-service attacks
-e.g. open ports, unsecured protocols or misconfigured firewalls

- **Human factor vulnerabilities:**

-social engineering, phishing attacks or lack of security awareness among employees can be

exploited by attacks to gain unauthorized access to systems or sensitive information ● **Zero-day vulnerabilities:**

-newly discovered vulnerabilities that are not yet known to the vendor or have no available patches or fixes

-often exploited before they're mitigated

- **Physical security vulnerabilities:**

-weaknesses in physical security measures such as unsecured access points or lack of surveillance, that could allow unauthorized access to premises or hardware ● **Supply chain vulnerabilities:**

-weaknesses introduced through third-party software, components or services

To address the problem of vulnerabilities, organizations can carry out vulnerability assessments, using various tools and techniques to identify, prioritize and mitigate these weaknesses.

Vulnerability assessments serve several key purposes:

1. Identification of weaknesses
2. Risk prioritization based on severity and likelihood of exploitation
3. Compliance and regulatory requirements
4. Enhanced security posture
5. Patch management
6. Third-party risk management
7. Incident response planning
8. Business continuity and resilience

Today, there are also useful practical and open-source frameworks available to help with the defensive aspects of vulnerabilities including:

- CVSS Scoring System: https://www.first.org/cvss/calculator/3.1
- OWASP Top 10: https://owasp.org/www-project-top-ten/

3. Social Engineering Awareness:

i) What is Social Engineering?

Social engineering is a technique used by cyber attackers to manipulate individuals into divulging sensitive information, performing certain actions, or granting access to systems or data.

Unlike traditional hacking methods that exploit technical vulnerabilities, social engineering targets human psychology and behavior to deceive and exploit individuals.

Due to the key element of human error, Social Engineering can show up in a variety of different shapes and sizes. It is often said that humans are the biggest vulnerability to be mindful of due to our sometimes unpredictable nature and there are many scams that can be built around how people think and act.

Some interesting statistics to do with social engineering:

• 98% of Cyber Attacks involve some form of social engineering

• 84% of organizations fell victim to a phishing attack in 2022

• social engineering attacks cost companies $130,000 on average

• just 56% of companies provide security awareness training

Research tells us that social engineering will be one of the most prominent challenges in the current decade. Due to the rise and increased intensity of these types of attacks, the need for novel detection techniques and cyber security educational programs are needed.

ii) Common Social Engineering Techniques

We'll now look at some common social engineering techniques in more detail so we can better understand how to recognize and respond to them.

1. Phishing

Phishing is a key technique to be mindful of. This is due to how prevalent it is as well as the number of different types of phishing techniques that hackers can employ. Typically it is carried out by email (though it can be done via phone calls (vishing), text messages (smishing) or instant messaging also). This is where malicious actors impersonate legitimate entities to deceive individuals into divulging sensitive information, such as usernames, passwords, financial details, or personal information.

According to the Anti-Phishing Working Group (APWG), the number of phishing attacks

worldwide has been consistently high, with millions of attacks reported each month. Certain sectors such as finance, healthcare, technology and retail are commonly targeted due to the high value of the data they possess.

Key elements of phishing attacks include:

• Deceptive communication

• Malicious links or attachments

• Exploitation of trust

2. Pretexting

This is a form of social engineering where an attacker fabricates a scenario or pretext to manipulate individuals. It involves creating a false or misleading narrative to gain someone's trust or cooperation.

Key elements include:

• Fictitious story

• Establishing trust

• Request for information or actions

3. Baiting

A technique used in cyber attacks where attackers entice individuals into performing specific actions by offering something appealing or enticing. It involves luring victims into a trap by promising something in exchange for information or access.

Key elements include:

• Offering tempting 'bait'

• Manipulating curiosity or greed

4. Tailgating

This refers to an unauthorized individual gaining entry to a restricted area by closely following an authorized person. Tailgating is the reason why 'mantraps' are employed as physical access controls in necessary locations.

Key elements include:

• Exploiting trust

• Unauthorized entry

5. Quid Pro Quo

In Latin this translates to 'something for something'. In cybersecurity this is where an attacker offers something of value or benefit in exchange for sensitive information or access.

Key elements include:

• Offering something of value

• Exploiting reciprocity

6. Impersonation

This is a tactic where an attacker masquerades as a legitimate entity to deceive individuals into divulging sensitive information or performing certain actions.

Key elements include:

• False identity

• Deceptive communication

• Gaining trust

For better results, many attackers will look to combine elements of multiple techniques listed above in order to better deceive and exploit their target.

iii) Recognizing and Responding to Social Engineering Attacks

As we've touched upon, social engineering is a major threat because it exploits an element that can't be managed as reliably as other technological-based aspects: humans. In fact, these exploits have a history that predates the rise of the internet and even computers. It is much easier to hack a human than it is to hack into software or hardware.

Many of the effective ways to respond to social engineering attacks relate to being aware of various situations where influence is being imposed on us.

It is often effective to ask probing questions to ascertain the legitimacy of a situation or communication. Below are some key questions to consider depending on the

source.

1. Source verification:

-> does the sender's email address match the claimed sender?

-> are there any unusual characters or misspellings in the domain?

2. Urgency and tone:

-> is the message creating a sense of urgency or panic?

-> does it pressure for immediate action or threaten consequences?

3. Request for information:

-> is the request for sensitive data, login credentials, or financial information unusual or unexpected?

-> is there a valid reason provided for the request?

4. Attachments or links:

-> are there unexpected attachments or suspicious links?

-> have these been verified as safe or legitimate?

Asking these types of questions and fostering a culture of skepticism can help individuals and organizations recognize social engineering attacks and respond appropriately, reducing the risks of falling victim to these deceptive tactics.

4. Safe Browsing Practices:

i) Web Browsing Security Best Practices

When it comes to web browsing security, one of the first things to be mindful of is the actual browser itself. Today, there are a wide array of browsers available each with their own pros and cons when it comes to security.

Below is a quick summary of the most secure browsers as of 2023:

- Firefox - highly flexible and easy to use
- Tor - best for privacy and maintaining maximum anonymity

- Brave - very fast speeds with ad and tracker blocking
- Pale Moon - highly customizable and open-source
- DuckDuckGo - privacy focused mobile browser for Android and iOS

After selecting a secure browser there are additional practices that can be implemented to help maintain a secure online experience.

These include:

• Keep software updated

• Install security extensions/add-ons

• Enable automatic updates

• Use strong passwords

• Enable two-factor authentication

• Stay cautious of links and downloads

• Beware of phishing

• Use HTTPS

• Regularly clear browser data (e.g. history, cookies and cache)

• Be wary of public Wi-Fi

• Enable pop-up blockers

• Backup your data

When thinking about web security for small businesses, considering cybersecurity practices is especially important as many companies may appear to be attractive targets to hackers online, even if in reality, the company is fairly small.

Ultimately web security is vital for small businesses for several reasons including: protection of customer data, business continuity, compliance, protection of intellectual property and preservation of reputation.

ii) Identifying Secure Websites and URLs

When using the internet it is fairly simple to get led astray if one isn't educated about the ins and outs of secure website browsing.

One example of this is visiting a web browser that isn't using https.

Https (port 443) is simply encrypted http (hypertext transfer protocol, port: 80), utilizing TLS (Transport Layer Security) to encrypt connections to other authenticated peers over a network.

Earlier, less secure versions of the protocol were called Secure Sockets Layer (SSL), but the principle remained the same - encrypt connections using https instead of http to ensure that data is unreadable and secure from eavesdroppers.

In a web browser, you can be sure that you're visiting a page that is using https instead of http by the padlock symbol to the left of the url as seen in the image above.

While being sure to use https is one way that we can stay more secure while browsing the web, it shouldn't be the only way as attackers can often forge CA certificates (Central Authority), to make it appear as if a link is trustworthy when it isn't.
Other safe browsing practices small businesses should look to implement and practice include:
• Stick to reputable websites and avoid clicking on links from unknown sources. • Regularly update your web browser, operating system, and plugins to patch vulnerabilities. • Use a Virtual Private Network (VPN) for an added layer of security, especially on public networks.
• Enable Safe Browsing Mode: Most browsers offer a safe browsing mode that helps block malicious websites and scripts.
• Check File Extensions: Be cautious with file extensions; avoid downloading executable files from untrusted sources.
• Use Trusted Platforms: When making online payments, use reputable and secure platforms. • Enable Browser Security Warnings: Allow browsers to display warnings about potential security risks or unsafe websites
• Review Privacy Settings: Regularly review and adjust privacy settings on social media and other online platforms.

iii) Risks of Unsafe Browsing

The unfortunate fact about web browsing is that dangers lurk around every virtual corner.

This video explains how simple it can be to connect to a rogue network when an attacker is on the loose:
https://www.youtube.com/watch?v=1OVTmrXGHyU.

As explained in the video, if you are connecting to a public network, it is recommended to:
i) turn off file sharing apps like air-drop
ii) don't work with sensitive data
iii) check that you're using a https connection from the web browser URL

Below are some key concerns about growing threats in the realm of web browsing and cybersecurity:

a) A growing number of phishing attempts involve web browsing with users directed to fraudulent sites through links in emails or search engine results

b) There are thousands of new malicious websites created every day aiming to steal data, distribute malware or carry out cyber attacks

c) Reports suggest that browser vulnerabilities account for a significant percentage of overall security vulnerabilities

d) With the rise of mobile browsing, threats targeting these devices such as phishing attacks, malicious apps and mobile specific vulnerabilities have increased e) User awareness of cybersecurity risks related to web browsing remains a concern, with many individuals still susceptible to falling for phishing scams or visiting malicious sites

5. Password Security:

i) Importance of Strong Passwords

In 2021, more than 80% of confirmed breaches were related to stolen, weak or reused

passwords. Additionally, in 2022, over 24 billion passwords were exposed by hackers. All this to say that even in today's modern times, passwords are a fundamental security risk that we all should be aware of due to the number of accounts that we all have and use regularly on the internet.

In cybersecurity, strong passwords play a critical role for a number of reasons:

1. **Protection against unauthorized access:**

-strong passwords act as a frontline defense, preventing unauthorized individuals or cyber attackers from gaining access to sensitive accounts, systems, or data

2. **Prevention of credential guessing:**

-weak or easily guessable passwords are a common target for hackers who use automated tools to guess passwords based on common words, phrases, or patterns

3. **Security across multiple accounts:**

-using unique and strong passwords for each account ensures that if one account is compromised, others remain secure

4. **Defense against dictionary attacks and credential stuffing:**

-strong passwords that don’t contain recognizable words or phrases are resistant to these attacks where hackers use pre-compiled dictionaries of commonly used passwords and words or leverage stolen credentials from a breach to gain unauthorized access to other accounts **5. Resilience against phishing and social engineering:**

-strong passwords add an extra layer of security against phishing attempts where attackers try to trick individuals into revealing their passwords through deceptive means

6. **Compliance and best practices:**

-strong password practices align with industry standards, compliance regulations, and best practices recommended by cybersecurity experts, ensuring adherence to security guidelines

By encouraging the use of strong, unique passwords, implementing password management practices, such as regular password updates, multi-factor authentication, and avoiding password reuse, an organization can significantly strengthen their cybersecurity posture.

ii) Creating and Managing Secure Passwords

So what makes a secure password?

Demonstration using: https://www.passwordmonster.com/.

Using the above link to test, we can see that if a password is only lower-case and a few characters, it can be broken in a number of seconds or even milliseconds.

Once we get to 8 characters, the time to crack rises. Nonetheless, the best situation is where we have a password of 14 characters (very strong) including a mixture of numbers, special characters, upper and lowercase.

Passphrases have been proven to be the best choice when it comes to passwords. Passphrases are easy to remember. Unlike traditional passwords, passphrases, composed of multiple words or a combination of words and characters, strike a harmonious balance between complexity and memorability. Their inherent length and unpredictability make them a formidable defense against brute force attacks, significantly raising the bar for unauthorized access attempts.

Alongside length and complexity other factors to consider when creating secure passwords are:

- Avoid predictable patterns (e.g. 'password123', 'qwerty')
- Unpredictability (for example containing names or birthdays)
- Randomness
- Avoid reusing passwords across multiple accounts
- Avoid dictionary words
- Regular updates (especially for critical accounts)
- Use a password manager (for example LastPass or Bitwarden)
- Two-factor authentication (2FA)

Alongside creating a secure password that isn't easily hacked, it is also important to consider usability and the ability to remember the password. Balancing complexity and memorability is key to creating strong, secure passwords.

iii) Multi-factor Authentication (MFA) Usage

As mentioned previously, implementing 2FA or 'MFA' (Multi-factor authentication), helps to provide more security when logging into accounts by adding an additional layer requiring a second form of verification alongside the password.

According to Microsoft, enabling MFA can block over 99.9% of account compromise attacks and as such, its adoption across various industries has been on the rise due to its effectiveness in preventing unauthorized access. Various regulatory bodies and industry standards such as PCI DSS and NIST recommend or require the use of MFA to enhance security.

It is especially useful when implemented for remote access users who may be working from and accessing accounts in riskier environments or situations (for example working off a public wifi).

MFA solutions can come in a wide variety of shapes and sizes working either as part of an authentication application such as Microsoft or Google authenticator or from a physical input device.

Some examples of physical MFA solutions include:

- Security keys (USB)

-> YubiKeys

-> Google Titan Security Keys

- Smart cards

-> physical cards embedded with integrated circuits that store credentials and require users to insert them into a card reader for authentication

-> commonly used for access control

- Token-based authentication

-> physical tokens often known as hardware tokens or key fobs that generate one-time passwords (OTPs) that users input during login

- Biometric cards

-> these cards combine a physical card with biometric authentication capabilities such as a fingerprint or palm vein recognition to verify a user's identity

- Wearable device

-> some smartwatches or fitness trackers can act as an authentication factor by generating authentication codes or providing proximity-based authentication

- Bluetooth or NFC devices

-> authentication based on proximity to a trusted device or system

Multi-factor authentication solutions often require a mix of the following

aspects: a) Something you have (e.g. the physical device)

b) Something you know (a password)

c) Something you are (biometrics)

Overall multi-factor authentication solutions are great for providing enhanced security in a straightforward way.

6. Email Security and Phishing Awareness:

i) Email Security Best Practices

While we have many more options for communication using technology today when compared with older times, email is still the predominant method used by organizations to reach people. For small businesses especially, it can be an effective way to build a connection with prospective clients or customers and as such we need to be vigilant when thinking about email from a security context.

Below are some email security best practices that can help safeguard against various email-related threats:

1. **Use Strong, Unique Passwords:**

Employ strong, complex passwords for email accounts and avoid using the same password across multiple accounts. Consider using a password manager to generate and manage complex passwords securely.

2. **Enable Multi-Factor Authentication (MFA):**

Implement multi-factor authentication whenever possible. MFA adds an extra layer of security by requiring an additional form of verification, such as a code sent to a mobile device, alongside the password.

3. **Be Cautious with Email Links and Attachments:**

Avoid clicking on suspicious links or downloading attachments from unknown or unexpected sources. Verify the sender's credibility before interacting with links or attachments.

4. Verify Email Addresses and Domains:

Check the sender's email address and ensure it matches the legitimate domain of the organization. Be wary of email addresses that seem altered, misspelled, or unfamiliar.

5. Use Email Filtering and Anti-Malware Software:

Employ robust email filtering and anti-malware software to detect and block phishing attempts, spam, malicious attachments, and malware-laden emails.

6. Encrypt Sensitive Information:

When sending sensitive or confidential information via email, use encryption tools or secure file-sharing methods to protect the data from unauthorized access.

7. Regularly Backup Email Data:

Backup critical email data regularly to protect against data loss in case of a security incident or email account compromise.

8. Establish Email Policies and Procedures:

Develop and enforce clear email security policies and procedures within the organization to guide employees on safe email practices, handling sensitive information, and reporting suspicious emails.

Implementing these best practices helps strengthen email security, mitigate risks associated with various email threats, and reduce the likelihood of falling victim to email-related attacks.

ii) Identifying Phishing Emails

As we are talking about email security, of course a major hacking technique that we need to be mindful of is phishing.

As we've already touched upon, phishing is commonly used by hackers as part of social engineering. It can be used during the initial reconnaissance phase of the Cyber Kill Chain to harvest information but also during the delivery stage where a potential weaponized file for download has been attached.

To best understand how to identify phishing emails and the varying contexts at play, first we need

to understand the general process used.

This video from microsoft gives us a good brief overview of phishing: https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44.

How does Phishing work?

1) Attackers initiate a phishing attack by crafting deceptive emails, messages or websites that come from legitimate and trusted sources.

2) Phishing messages often create a sense of urgency or importance to prompt immediate action from the recipient.

3) Messages often contain links to fake websites or malicious attachments (e.g. a document with a virus inside). Clicking on the provided links might lead victims to counterfeit websites that closely resemble real ones, prompting them to enter sensitive information.

4) Victims who interact with these deceptive messages might unknowingly provide sensitive information such as usernames, passwords, credit card numbers, social security numbers or other personal details.

5) Once individuals provide their information, attackers can exploit it for various malicious purposes, such as unauthorized access to accounts, identity theft, financial fraud, or selling the information on the dark web.

Types of Phishing:

Due to the varying nature of businesses and people, there are actually multiple different types of phishing techniques that can be employed by a hacker depending on the situation and their goals.

These include:

• **Generic phishing:** sending mass emails pretending to be from reputable organizations to lure as many people as possible into clicking malicious links, downloading malware or divulging

confidential information

• **Spear phishing:** a targeted form of phishing where cybercriminals personalize their messages to specific individuals or organizations with the aim of deceiving the recipient into taking specific actions

• **Business email compromise (BEC):** a sophisticated email scam that targets businesses or individuals performing financial transactions

• **Vishing (Voice Phishing):** attackers use phone calls or voice messages to deceive individuals into divulging personal or financial information

• **Smishing (SMS Phishing):** the sending of deceptive test messages to mobile phone users, often containing links or requests to call a particular number

• **Email spoofing:** forging the sender's email address to appear as if it is coming from a different source

• **Whaling:** a specific form of spear phishing that targets high-profile individuals or executives within an organization

• **Search Engine Phishing:** manipulating search engine results to lead users to malicious or fraudulent websites

Identifying phishing emails involves recognizing certain telltale signs and being cautious while assessing the legitimacy of an email. Below are some tips to keep in mind:

- Check the sender's email address
- Examine the salutation and tone
- Look for spelling and grammar errors
- Inspect links and URLs (e.g. by hovering over them to see the actual URL) ● Beware of attachments (especially if they prompt you to enable macros or run scripts) ● Check for requests for personal information
- Verify urgent requests or threats
- Trust your instincts

By remaining vigilant and adopting these practices, individuals can better identify and protect themselves from falling victim to phishing attempts.

iii) Reporting Suspicious Emails and Phishing Attempts

As scam emails are currently one of the most common threats in cybersecurity, it is useful to know how to go about reporting instances where you may be a victim to an attempted email hack.

ActionFraud in the UK is just one example of an organization that deals with cases and accepts reports from individuals. Submitting a report doesn't take long and no personal information is collected.

Once submitted, Action Fraud will forward reports to the National Fraud Intelligence Bureau (NFIB) for collation and analysis. This enables crucial intelligence to be gathered and preventative action to be taken.

In the US, alongside reports for identity theft and more, email fraud can be reported to the Federal Trade Commission via: https://reportfraud.ftc.gov/#/.

The steps that are recommended to follow if you have fallen for a phishing scheme are:

1. Alert others
2. Limit the damage
3. Follow your company's procedures
4. Notify customers
5. Report it

Organizations such as the Anti-Phishing Working Group (APWG) and the Internet Crime Complaint Center (IC3) are also specialist organizations that accept reports of phishing incidents.

It is good to remember that reporting suspicious emails and phishing attempts not only protects you but also contributes to the collective effort to combat cyber threats and protect others from

falling victim to similar attacks.

7. Safe Data Handling:

i) Understanding Data Sensitivity

In cybersecurity, data sensitivity refers to the level of confidentiality or criticality of information. It determines how sensitive certain data is and dictates the level of protection and controls necessary to safeguard it from unauthorized access, disclosure or modification.

The various types of data can be classified into the following categories:

• Public data = data that poses no risk or harm if disclosed
• Internal data = data that may not contain highly sensitive information
• Confidential data = sensitive information that requires protection from unauthorized access or disclosure
• Restricted / highly confidential data = data that, if exposed, could cause severe harm to individuals or organizations

By understanding the sensitivity of data in question, organizations can better prioritize their security efforts.

We'll now take a look at some of the various options and implementation methods that are out there for small businesses when it comes to protecting and securing data.

Regular Data Backups:
• Choose reliable backup solutions that fit the business's needs. E.g. Cloud-based services, external hard drives of network-attached storage (NAS).
• Automate backup processes to minimize the risk of data loss.
• Test backups to ensure data can be restored successfully.

Data Encryption:

• Identify sensitive data. Personal information, financial data, and intellectual property often need encryption.

• Use encryption tools. Implement encryption tools for data at rest and in transit. •
Secure encryption keys. Store keys securely, restricting access to authorized personnel.

Update and Patch Systems:

• Establish a patch management process. This includes operating systems, applications and firmware.

• Automate updates wherever possible to ensure systems receive timely patches and fixes for known vulnerabilities.

• Prioritize critical updates to address known vulnerabilities that could be exploited by attackers.

Access Controls:

• Implement user access policies. Define user access levels and permissions based on job roles and responsibilities. Use the principle of least privilege to grant access only to necessary resources.

• Use authentication measures. Implement strong authentication methods like MFA to verify user identities before granting access to sensitive data or systems.

• Regularly review access rights to ensure that privileges align with current job roles and responsibilities.

Regular Security Audits:

• Schedule routine audits to evaluate the effectiveness of security measures and identify vulnerabilities.

• Engage external experts to conduct comprehensive security audits and assessments for an unbiased evaluation.

• Act on findings. Implement corrective actions based on audit findings to address identified vulnerabilities and improve overall security posture.

ii) Understanding Personally Identifiable Information (PII)

What is (PII)?

(PII) Stands for Personally Identifiable Information and refers to any data that could potentially

identify a specific individual. This includes information such as:

◦ A person's name

◦ Address

◦ Phone number

◦ Email address

◦ Social security number

◦ Biometric records

◦ Financial information

In cybersecurity it is crucial to protect PII as its exposure can lead to identity theft, fraud or other privacy breaches. The term has been used for several decades in the context of privacy and data protection. One of the early and significant legislative steps in the US was the Privacy Act of 1974, which addressed the handling and protection of PII by federal agencies.

In today's data rich world, where we increasingly rely on IT at work or at home, the quantity of PII shared with organizations has increased. This is an attractive situation for hackers who can try and obtain this data to then use as part of a further cyberattack.

PII can be direct or indirect. The former includes identifiers unique to a person (for example a passport number). Indirect PII relates to more general personal details like race or place of birth. Protecting customer PII is a key factor to being compliant in the realm of information governance. The sensitive information that PII includes can have severe consequences for a business and its customers or employees if compromised.

All of the following factors are reasons why protecting PII is a good idea for small businesses:

• Legal Compliance

• Trust and Reputation

• Financial Impact

• Business Continuity

• Competitive Edge

Since (PII) first gained prominence alongside laws and regulations, nearly five decades ago, 'PII' has become increasingly prevalent in the context of privacy laws globally. For example, in relation to the EU's General Data Protection Regulation (GDPR), introduced in 2018.

GDPR emphasizes the protection of personal data, which includes any information relating to an identified or identifiable natural person, aligning closely with the concept of PII.

iii) Understanding PCI DSS

Just like (PII), PCI DSS is a critical category of information that small businesses should factor into their cybersecurity procedures in order to operate in an ethical and compliant manner.

PCI DSS stands for Payment Card Industry Data Security Standard, which was first introduced in December 2004.

The standard was developed by major credit card companies including Visa, MasterCard and American Express, to improve payment card account data whilst facilitating the broad adoption of consistent data security measures globally.

As of version 4.0 (March 2022), principle requirements include the following:

• **Build and maintain a secure network and systems**
-install and maintain network security controls
-apply secure configurations to all system components
• **Protect account data**
-protect stored account data
-protect cardholder data with strong cryptography during transmission over open, public networks
• **Maintain a vulnerability management program**
-protect all systems and networks from malicious software
-develop and maintain secure systems and software
• **Implement strong access control measures**
-restrict access to system components and cardholder data by business need to know
-identify users and authenticate access to system components
-restrict physical access to cardholder data
• **Regularly monitor and test networks**
-log and monitor all access to system components and cardholder data
-test security of systems and networks regularly

• **Maintain an information security policy**

-support information security with organizational policies and programs

The standards and requirements set forth by PCI DSS are primarily to ensure that businesses which process, store or transmit credit card information do so in a secure environment, helping to reduce the risk of data breaches and fraud.

Non-compliance with PCI DSS can result in fines, penalties or restrictions on card processing capabilities.

For more information on PCI DSS including downloadable standards, you can visit: https://www.pcisecuritystandards.org/document_library/?category=pcidss&document=pci_dss

8. Incident Reporting:

i) Importance of Incident Reporting

When Cybersecurity events happen, they are often unexpected. To be better prepared for future events and to learn from them, incident reporting is a key aspect that can be implemented when seeking to improve an organization's Cybersecurity posture.

Incident Reporting acts as the first major part of an Incident Management process as part of a Risk assessment. It refers to the formal process of identifying and documenting and escalating security incidents within an organization. It is a critical part of incident response, allowing organizations to identify, assess, and address cybersecurity events quickly and effectively.

Reports can include data such as who was involved, what happened, when it happened, where it happened, what caused it to happen, and any other relevant details. Any documents created can be referred to later on for Incident Handling and further planning or communications. Over time, incidents can be tracked to identify patterns which can be used for deeper analysis.
Having an effective incident reporting process is crucial for several reasons:

1. Timely response

-it aids in containing the incident, mitigating its impact and preventing further damage or data loss

2. Understanding the threat landscape

-analyzing incidents helps in understanding attack patterns, trends and vulnerabilities enabling proactive measures to be taken

3. Risk mitigation and prevention

-through the documentation of incidents and their causes, organizations can identify weaknesses in their security posture to help prevent similar incidents from happening again

4. Compliance and legal obligations

-complying with regulations is essential for many industries to avoid legal repercussions and maintain regulatory compliance

5. Resource allocation and improvement

-understanding the nature and frequency of incidents helps guide investment decisions in security measures

6. Communication and transparency

-both internal and external communication can help maintain trust with stakeholders, customers and partners

Overall, incident reporting is critical for maintaining cybersecurity resilience, minimizing the impact of incidents, and continuously improving an organization's ability to detect, respond to, and recover from cyber threats.

ii) Incident Reporting Process & Procedures

To aid in the process of incident reporting, it is often helpful to refer to established and reputable defensive frameworks already in place and widely used in the industry.

The NIST Cybersecurity Framework (CSF) is one such example and is a set of guidelines, standards and best practices created by the National Institute of Standards and Technology. It offers a voluntary framework designed to help organizations manage and improve their cybersecurity risk management processes.

The procedures listed below outline the steps and actions to be carried out when a security incident takes place within an organization's systems, networks or infrastructure. Based on the NIST framework described above, each is crucial for effectively managing and mitigating the impact of incidents.

1. **Identify**

-> develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data and capabilities

2. **Protect**

-> develop and implement appropriate safeguards to ensure delivery of critical services

3. **Detect**

-> develop and implement appropriate activities to identify the occurrence of a cybersecurity event

4. **Respond**

-> develop and implement appropriate activities to take action regarding a detected cybersecurity incident

5. **Recover**

-> develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or service that were impaired due to a cybersecurity incident

When it comes to incident reporting, we are really talking about the later stages of the NIST Cybersecurity Framework (Respond and Recover), however it is good to understand the broader context that this covers. Often when incidents happen, a RCA (root-cause-analysis) approach will need to be taken and that includes identifying the key systems and services which were affected as well as how best to protect them in the future.

Alongside identification and documentation of any security incidents that have happened, during incident reporting, relevant stakeholders will need to be contacted also. This can be on an internal basis as with the IT security team, incident response team, management or legal department but also potentially externally if regulatory authorities or law enforcement agencies need to be contacted. This will depend on the severity and the nature of the incident. It is important to stick to the facts and not jump to conclusions when capturing data so that post-incident analysis is as accurate as possible.
When it comes to the incident reporting process, details will vary depending on the institution

however, once again, following a framework can be helpful to keep us on track.

Below are recommended steps for writing a good incident report:

i) Document the details:
-this should include the date and time of the incident, affected systems or networks, who was involved and any initial observations

ii) Describe the incident:
-this should include the timeline of events with actions broken down plus the highlighting of any suspicious activities or anomalies plus evidence gathered

For example, when an event happens data generated can be gathered and collated from: • log files
• transcribed or written notes
• recordings
• email transcripts
• screenshots

iii) Analyze the incident:
-identifying the root cause of the incident is key to understanding how it occurred and what steps can be taken for prevention in the future

Once the required information has been collated, a full report can be written for later review by relevant stakeholders. Below are some key components for an example report that can be included:

- Introduction and executive summary
- Incident description
- Impact analysis
- Response actions
- Investigation and analysis
- Lessons learned
- Conclusion and follow-up

- Appendices and supporting documentation

Writing a good cybersecurity incident report requires clarity, accuracy and completeness of information. It should serve as a comprehensive record of the incident, its impact, the response taken, and measures to prevent similar incidents in the future.

10. Continuous Learning:

i) Continuous learning and building a culture of cybersecurity

Due to the fast paced and ever-evolving nature of today's technological world, it is important to be mindful of continuous learning in order to keep up and be able to build a culture of cybersecurity within an organization.

Currently there is a notable skills gap which is affecting the entire digital economy. Cybersecurity Ventures predicts that there will be 3.5 million unfilled cybersecurity jobs globally by 2025, indicating a persistent shortage. As remote work becomes more normal and infrastructures more distributed, the need for professionals who have up-to-date security skills and knowledge will continue to accelerate.

Organizations can aim to foster a culture of continuous learning and cybersecurity by implementing several strategies including the ones below:

- Training and awareness programs
- Leadership support and communication
- Encourage accountability and responsibility
- Promote collaboration and information sharing
- Create a positive security culture
- Continuous assessments and feedback

All in all, continuous learning is a vital aspect of personal and professional development, allowing individuals to adapt, grow and thrive in a rapidly changing world. It should be thought of as a

lifelong process and journey that goes beyond formal education.

ii) Ongoing Training Opportunities

Through the internet and the open-source world there are countless opportunities for learning and growth in the world of Cybersecurity today.

These include:

- Certification programs
- Online courses and platforms
- Cybersecurity bootcamps
- Workshops and conferences
- Webinars and virtual training sessions
- Capture the flag (CTF) competitions
- Professional associations and communities
- In-house training and mentorship.

Continuously pursuing these training opportunities allows cybersecurity professionals to stay updated with the latest threats, technologies and best practices, enabling them to effectively protect organizations against evolving threats.

For relevant links to training providers please see the resources section at the end of this document.

iii) Staying Updated on Emerging Threats

Just as developing new skills as a part of continuous learning is an ongoing process, for cybersecurity professionals, so too is staying updated on new emerging threats. This aspect is especially important to do if you work in the defensive side of the industry such as a SOC analyst, threat hunter or incident responder.

There are many different sources and resources out there which can help one to stay updated.

Below is a list of some of them:

- Security News:

- The Hacker News

- Krebs on Security

- Dark Reading

- ZDNet Security

- Security Blogs:

- Schneier on Security

- Troy Hunt's Blog

- Naked Security by Sophos

- Security Podcasts:

- Darknet Diaries

- Smashing Security

- Smashing Security

- Security Communities:

- Stack Exchange's Information Security

- OWASP

- ISSA

Resources:

1. https://www.edapp.com/top-10-cyber-security-training-for-employees/
2. https://www.itgovernance.co.uk/staff-awareness
3. https://www.esecurityplanet.com/products/cybersecurity-training/
4. https://csrc.nist.gov/Projects/cybersecurity-framework/Filters#/csf/filters 5. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html 6. https://www.sans.org/security-resources/glossary-of-terms/
7. https://www.nist.gov/cyberframework

References:

- https://www.hiscoxgroup.com/cyber-readiness
- https://www.safetydetectives.com/blog/which-is-the-most-secure-web-browser-to-use-in/#:~:text=I%20found%20Firefox%20to%20be%20the%20most%20secure.&text=Firefox%2

0also%20includes%20excellent%20anti,web%20browser%20on%20my%20list

- https://resources.digitalshadows.com/whitepapers-and-reports/account-takeover-in-202 2
- https://lp-cdn.lastpass.com/lporcamedia/document-library/lastpass/pdf/en/LastPass-Enterprise-The-Password-Expose-Ebook-v2.pdf
- https://www.proofpoint.com/uk/security-awareness/post/risky-business-unsafe-web-browsing
- https://firewalltimes.com/social-engineering-statistics/