EC-Council

WHY SECURITY AWARENESS TRAINING IS IMPORTANT FOR BUSINESSES IN 2023

EC-Council would like to thank **Ken Muir**, Chief Information Security Officer at LCM Security Inc., for authoring this whitepaper.

Abstract

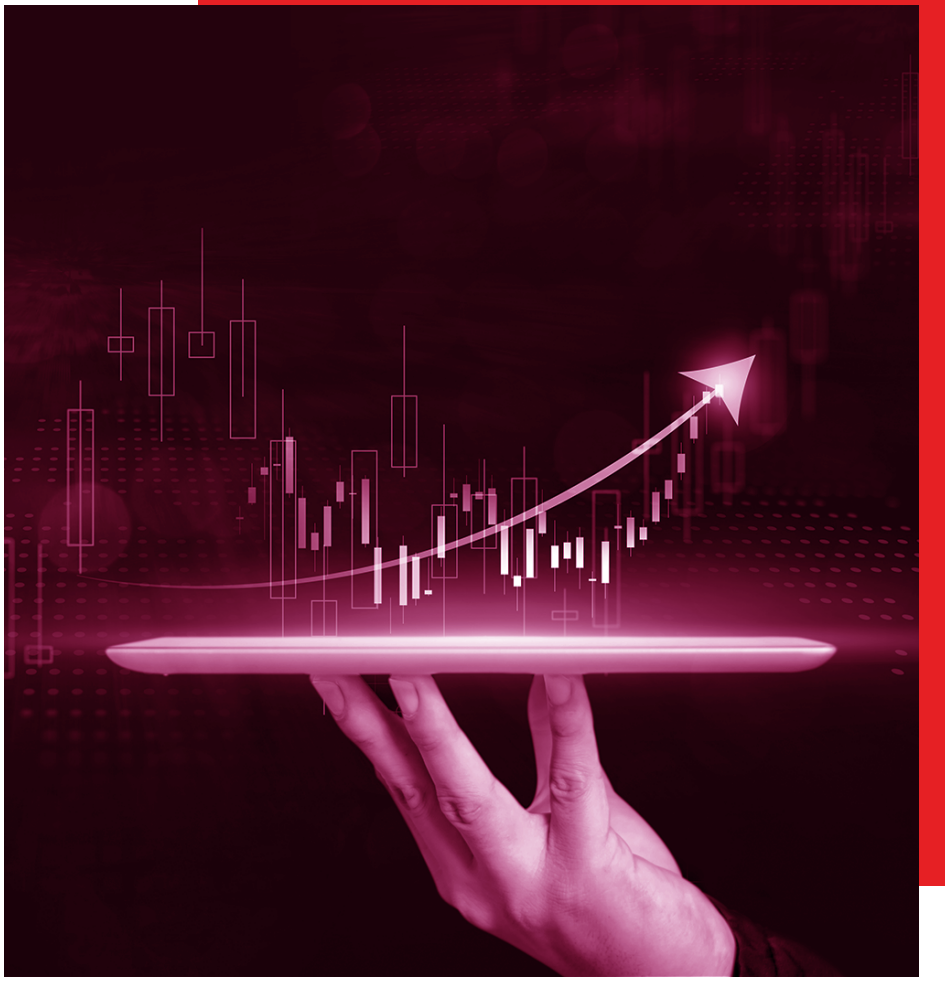
Enterprise security professionals are responsible for designing effective defense mechanisms for their organisations, but they often work in the background and rarely occupy center stage. A solid strategy is necessary to deal with incoming threats, and awareness is the first step in developing effective cyberdefenses. Data is easily accessible within many organisations, and when confronted with security risks, employees often do not know how to mitigate them. Security awareness training empowers employees to take corrective measures. This whitepaper discusses some of the threats **organisations** face and offers guidance on how to overcome the challenges associated with security awareness training to help mitigate those threats.

Keywords: security awareness training, security awareness trends, security awareness, security threats, security issues

Contents

Why Security Awareness Training Is Important for Businesses in 2023

Cybersecurity is a major priority for organisations, and business owners tend to take a layered approach to implementing a strong security strategy. Despite putting in place security policies, procedures, awareness programs, and training solutions, however, malicious hackers continue to target systems and cause data breaches. Because security awareness training is treated as an optional module in many organisations, it is often overlooked. After a data breach occurs, senior executives may puzzle over what went wrong, missing the cause-and-effect connection with their failure to invest in cybersecurity strategies. Given the rapid rise in cyberattacks, every organization should raise cybersecurity awareness and establish programs to train employees in fundamental security principles and practices, as these processes are key to creating a solid cybersecurity defense strategy. Customers, partners, and employees must collectively contribute to the protection of confidential data and share responsibility for ensuring the integrity of those data.



The Top Security Issues Faced by Organisations

IT teams are not solely responsible for protecting data. Rather, executives, managers, and security leaders must empower all employees by teaching them how to prevent or mitigate common threats through safe data management and sharing practices. This section outlines the top security concerns and issues that organisations currently face.

Insider Threats

Insider threats have become one of the most significant challenges facing organisations today because of their potential to inflict severe damage that results in heavy costs. Insider attacks cost impacted organisations more money than those originating from external attackers, according to a report conducted by Ponemon Institute (Proofpoint, 2022). The average cost of an insider attack in 2021 was USD 15.38 million per incident, Ponemon researchers found, while the average cost of a security incident executed by external attackers was USD 4.24 million.

Insider threats are security risks that originate within targeted organisations. Malicious activities are typically conducted by users who have legitimate access to sensitive information. Current or former employees might sell the company's confidential data on the dark web. Malicious insiders might also steal hard drives or other hardware devices that contain encrypted data, change user access privileges on network accounts, or abuse their own credentials for personal motives. Insiders who unknowingly give out sensitive information to attackers are known as pawns. Others, called "turncloaks," sell company secrets to outsiders for profit. One prominent example of a turncloak is Dongfan "Greg" Chung, who sold trade secrets to the Chinese government over a 30-year period while employed as an engineer at Boeing. He faced charges of corporate espionage and ultimately was sentenced to prison for 15 years and 8 months (Associated Press, 2010.

Phishing Scams

Threat actors employ a variety of social engineering tactics to target unsuspecting employees at work. Phishing emails are the most common mechanisms for social engineering attacks. Often, they consist of scam emails sent in bulk to a large number of recipients. They sometimes target individuals with customized content—a tactic known as spear phishing. One form of spear phishing requires the target to open an attachment, which triggers a malicious action. Crafted to appear to be messages from legitimate business sources, phishing emails typically aim to trick recipients into divulging personal details or downloading malware to their systems.

Phishing schemes have become more prevalent during the COVID-19 pandemic, coinciding with employees switching to remote work. Attackers have taken advantage of new opportunities to target employees with phishing emails masquerading as information about making vaccination appointments, scheduling leave, and accessing company databases from home networks. Organisations are faced with a heightened need to bolster their identity management and security access frameworks to combat these types of phishing schemes.

Lack of Security Awareness Training

There are many security solutions available to organisations, but installing software is not enough. To substantially reduce their vulnerability to cyberthreats, organisations must provide proper cybersecurity awareness training for their employees, as humans are the weakest link in any cyberdefense strategy. Attackers frequently use psychological ploys to surpass cyberdefenses and infiltrate the most protected networks. At a minimum, cybersecurity training for employees should address the following topics:

- Phishing emails
- Malicious insider threats
- Attack vectors for malware, especially ransomware
- Password security best practices
- Security of physical devices (e.g., USB drives, Internet of Things devices)
- Wi-Fi security
- Remote work security

Legacy Equipment and Data Migration

Many companies store sensitive data in legacy equipment that is vulnerable to compromise. Because legacy hardware systems typically do not have advanced systems in place to tackle emerging security threats, they often become soft targets. Adding to the problem, many organisations still run some equipment using outdated operating systems, such as Windows XP and Windows 7, for which support and security updates have been discontinued. One analysis, for example, found that 83% of medical devices were running on operating systems that no longer received updates and were considered potentially lucrative attack targets (Alder, 2020).

Companies that do not upgrade their networks face operational and security risks. The speed gap between high-speed networks and low-performing devices creates security vulnerabilities, for example. Network taps and packet brokers can be helpful in managing network performance and security in environments where legacy systems are in use (Hartrup, 2019).

Natural Disasters

Bad weather can impact infrastructures, disrupt network operations, and disable security systems. Unpredictable environmental disasters such as floods, earthquakes, and fires create opportunities for threat actors to exploit. If servers go offline, for example, attackers might be able to steal data before systems recover, and the breach may never be noticed.

Weak Passwords

Weak passwords are a major issue when it comes to managing security risk. Despite widespread advice cautioning against the practice, many people still use easy-to-remember passwords that are easy for attackers to predict using brute-force methods. Any company committed to adopting a robust security policy must make sure its employees use strong passwords. Ideally, passwords should be both complex and long (i.e., at least 20 characters).

Ensuring security in password storage is just as important as creating strong passwords in the first place. Organisations can use identity and access management solutions on premises, while individuals working from home can use password manager programs for safe storage. Once a password is leaked and credentials are compromised, it may become difficult to regain access to the affected accounts.

Open Ports

Open ports create loopholes in security systems that external threat actors can exploit to access sensitive data. Sometimes attackers are not initially aware of these vulnerabilities but stumble upon them after gaining access to a system. Cybercriminals use footprinting to find as much technical information about a system as possible—such as running services and open ports—to gain unauthorized access to target system resources (Rahaman, 2022).

Lack of Asset Ownership

Often, organisations do not have a clear understanding of where their intellectual property assets are located within the company and its systems. Likewise, businesses may not be aware of which data are most vulnerable, sensitive, or at risk of being compromised. The process of identifying, discovering, and securing intellectual property assets is frequently neglected, resulting in a major security awareness concern.

Injection Attacks

In an injection attack, a hacker sends—or injects—malicious code to web applications and then attempts to gain control of an organisation's systems when the applications execute these files. The technology or framework being utilized makes a significant difference in how code injection vulnerabilities can be prevented. Although it is not the end user's role to mitigate injection attacks, it is nevertheless important for employees to be aware of the existence of this threat as part of a security awareness training program.

Network Misconfigurations

Network misconfigurations can lead to a number of undesirable outcomes, including gaining access to inactive user accounts, escalating user privileges, and hijacking administrator access controls. A network that has been improperly configured can cause disruptions to the flow of data within an organisation and impact internal and external communications. Attackers can take advantage of broken authentication measures and other misconfigurations, which can make administrator information completely visible to public users (Witts, 2022).

The Importance of Security Awareness Training

Security awareness training refers to the formal programs that organisations use to identify and mitigate cybersecurity risks. It involves building an awareness of threat vectors and training employees in the best ways to protect their data. The role of security awareness training is to help employees gain an understanding of the tools and tactics used for launching cyberattacks and to reinforce the need for personal accountability in ensuring the confidentiality of sensitive information in their organisations. Providing effective security awareness training during the employee onboarding process equips newcomers with the tools to handle a variety of threats and to uncover and remediate vulnerabilities in existing security systems before attackers exploit them (Mimecast, n.d.).

Organisations need security awareness training because human error is a contributing factor in 90% of data breaches, with phishing techniques the primary cause of nearly half of breaches (CybSafe, 2021). The people who operate and use technology and applications in organisations are the most vulnerable, since malicious attackers often find it easy to target them. Employees often know key details that attackers need to access sensitive information. A lack of security awareness training can spell disaster, as employees might not have the knowledge or tools to differentiate between official entities and potential threat actors.

The Benefits of a Security Awareness Training Program

1. Data Breach Prevention

Data breaches can have catastrophic consequences for affected organisations, and quantifying the number of data breaches before and after security awareness training is one way to measure such a program's effectiveness. The average cost of a data breach in 2021 rose to USD 4.24 million (IBM, 2021). Organizations that operate in highly regulated sectors, such as healthcare, banking, and insurance, may incur high fines and penalties from compliance bodies for violating provisions of laws and standards like the General Data Privacy Regulation (GDPR, Payment Card Industry Data Security Standard (PCI DSS, and the Health Insurance Portability and Accountability Act. Customers may initiate lawsuits if their sensitive personal information is exposed to the public. Suspension of operations and revenue losses are other impacts of data breaches. However, the most devastating consequence is typically damage to business reputation, which may be tarnished for a long time and possibly never fully restored. A data breach massively impacts return on investment, and failure to respond to threats in a timely way speaks volumes about an organization's security strategies.

2. Reinforcement of a Cybersecurity Culture

Employees are often the first line of defense against cyberattacks. In many cases, attackers target the people behind the technology rather than the technology itself. Situational awareness training, building a culture of security values, and learning about the best practices for safeguarding data are key to keeping employees protected. Promoting a cybersecurity culture in organisations will help employees develop a mindset that prioritizes best security practices and makes them second nature, instead of regarding security as a set of tedious procedures and IT policies contained in rarely read manuals. A culture of security also makes it easier for employees to maintain a work–life balance, as it reduces instances of having to work odd hours responding to data breach emergencies.

3. Enterprise Security Solutions Maintenance

Businesses often consider investing in technological tools and defenses to improve their security policies and practices. However, without proper feedback and performance reviews, it can become difficult to decide which direction to take. Updating software, configuring firewalls, and addressing security issues in a timely way can help companies build a robust security solution. To take full advantage of technology, enterprises require cooperation across all business units. All employees must be on the same page and able to contribute insights about security workflows through participation in vulnerability assessments. To prevent downtimes or delays in business operations, it is mandatory to regularly upgrade enterprise security solutions. However, security awareness training is necessary as the first step in establishing a security software maintenance plan.

4. Customer Loyalty Boost

When choosing services or making investment decisions, organisations look for a reputation that reflects trustworthiness. Client prospects typically check the security credentials of vendors before they decide to convert to their product offerings. Often, one of the first things they check is how the organization ensures its cyberdefenses in connection with managing customers' personal data: Which security measures are in place? Which technological solutions are in use? What are employees' levels of IT security knowledge?

The same is true for individuals. In a consumer survey conducted in 2017, 88% of participants said the extent of their willingness to share personal information was predicated on how much they trusted a given company (PwC, 2017. Many organisations throughout the world are not doing enough when it comes to their cybersecurity practices. Security awareness training and assessments can help bolster an organization's cybersecurity defenses, which ultimately builds customer trust and increases recommendations and referrals.

5. Ripple Effect

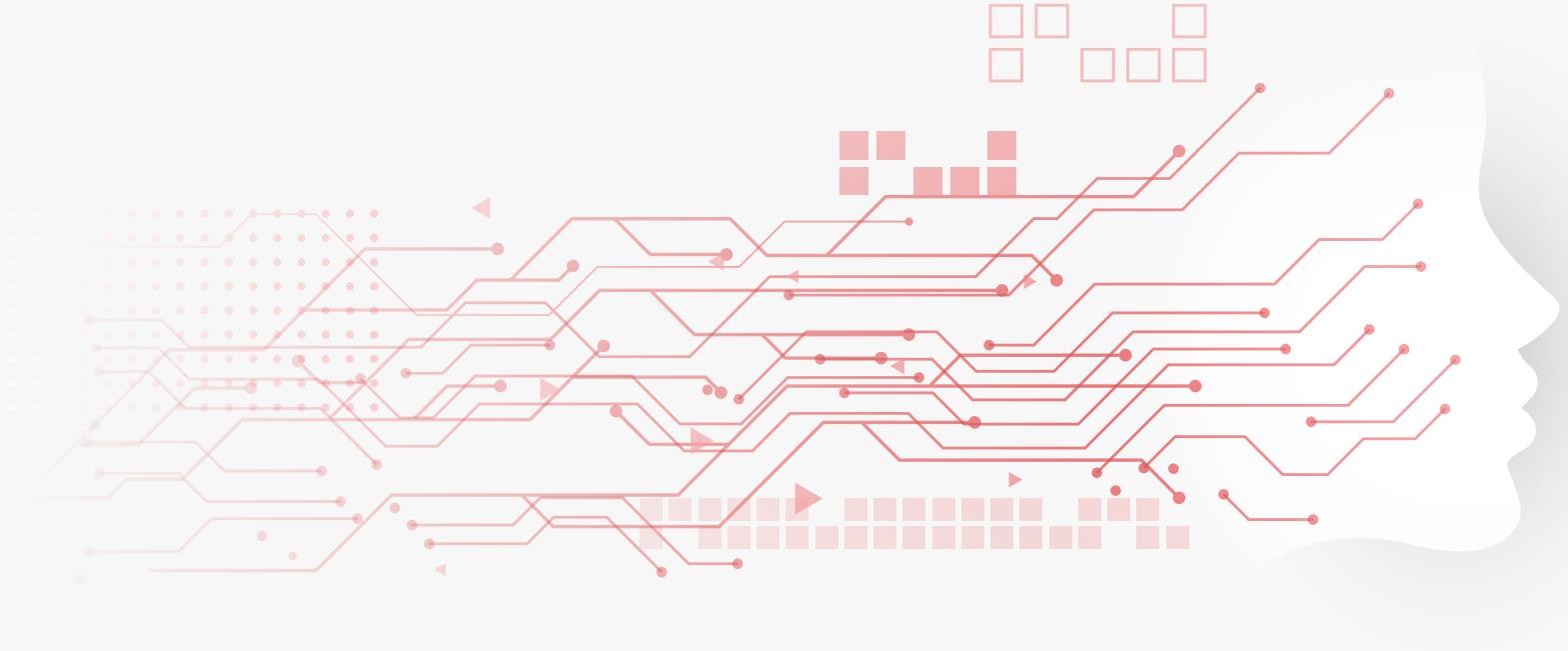
The benefits of security awareness training are not limited to employees and businesses but extend to everyone around them. All suppliers, third-party vendors, and other associated businesses enjoy benefits when an organization with which they are affiliated incorporates awareness training programs into its cybersecurity strategy. Threat actors are notoriously creative in devising new malicious attacks that affect organisations worldwide. Companies that implement security training and policies improve their own defenses and, in so doing, make other organisations less susceptible to threats. For instance, conducting a supply chain attack typically involves exploiting security vulnerabilities in a third-party vendor, supplier, contractor, or subcontractor to gain unauthorized access to an organization's IT environment. Security training helps an organization become more resilient to such attacks, increasing customer and partner trust.

6. Productivity Gains

It is well documented that happy people are productive people (Bellet et al., 2019. Cybersecurity awareness training helps increase happiness by reducing the stress and worry that often accompanies the handling of unforeseen incidents. It prepares employees to manage existing threats more easily and to be alert to potential future attacks. For the organization, the net result can be a marked improvement in productivity.

7. Compliance Assurance

Enterprises are mandated to achieve compliance with laws and governmental regulations, but such compliance can be very challenging to achieve if employees are uneducated about security risk factors and what they can do to help keep organisations' systems and data safe. There are also sets of industry standards established by nonprofit organisations that are generally accepted. Failure to comply with legally required or widespread industry-specific standards can result in the imposition of heavy penalties and fines, along with reputational damage. Common enterprise security standards include the GDPR, the PCI DSS, and the standards established by the International Organization for Standardization and the National Institute of Standards and Technology (Kirvan & Granneman, 2021).



Security Awareness Training Trends

The technology landscape is constantly evolving, and the same is true of the threat landscape. Security awareness training programs are based on threat trends, and organisations devise response strategies based on the expected impact of trending threats. Nobody can predict with certainty the disruptions that might happen as the digital age progresses, but the following overview of trends provides some insight into the current focus of security awareness training.

Rise of Ransomware

Ransomware is plaguing organisations today, and it is very difficult to crack down on the cybercriminals behind such attacks. Consequently, educating employees on ransomware attacks and how to defend against them is among the top security awareness trends in 2022. Ransomware attacks use sophisticated techniques, including encryption of stolen confidential data. After attackers acquire information, they often sell it on illegal markets at exorbitant rates or charge companies huge sums in exchange for not erasing it or leaking it online. Ransomware attacks not only cause economic impacts on organisations but also threaten their reputations and credibility. As using virtual private networks does not provide sufficient protection against such attacks, organisations are shifting toward the use of zero-trust network access to control remote access to sensitive information.

Widespread Implementation of Multifactor Authentication

Although companies are educating employees on crafting strong passwords for user accounts, the use of multifactor authentication (MFA as an additional safeguard is becoming the norm. MFA requires users to verify their identity by entering a one-time code, usually sent to a phone number or email account on record. There is a time limit set for using the code before it expires. MFA is a helpful layer of defense because the code may only be used once, and a new code must be generated for the next login. However, there are more- and less-secure methods of MFA. Some experts advise using application-based MFA (e.g., Google Authenticator or Microsoft Authenticator over the SMS-based method (Cimpanu, 2020).

Proliferation of Artificial Intelligence

It is now common for organisations to adopt artificial intelligence (AI solutions for security awareness, training, and defense. Designing plans for file backup and incident response or recovery is core to enterprise cybersecurity strategies. organisations often use AI software and automation tools to analyze massive volumes of data, gain insights from previous attack patterns, and replace manual labor. AI saves countless hours and helps companies become more productive and efficient. AI security systems are often used to streamline business operations and change the way data is managed online. Businesses invest in automation software with the expectation of mitigating the cost of data breaches and recovering from losses more quickly.

Increase in Cloud Attacks

With remote work becoming the new normal in the wake of the COVID-19 pandemic, organisations are relying on various cloud-based infrastructures and services to communicate and collaborate with employees. However, relying on cloud technologies is proving risky, as cloud services are not always optimized for security. Cloud vendors suffer from vulnerabilities in their products that attackers can exploit. Misconfigurations in cloud settings are among the leading causes of data breaches (Ermetic, 2020). Cloud migration is another potential problem area. These issues can be addressed in security awareness training at organisations that are shifting operations to the cloud.

Imposition of Data Privacy Regulatory Frameworks

Data privacy is an important component of modern security awareness training programs due to the recent issuance of a number of new regulations and guidelines by authorities and industry bodies. To achieve compliance, organisations must follow best data privacy procedures and practices. Identifying and remediating areas of data privacy weakness is now a top priority for many organisations. Data privacy and protection frameworks—including the EU's GDPR, the California Consumer Privacy Act, and Brazil's General Data Protection Law—are making it mandatory for organisations to exercise control over personal data. Some data privacy guidelines address the need to remove data from systems to reduce the risk of data abundance, which can lead to leaks. organisations that fail to implement these guidelines may ultimately jeopardize their reputation and incur financial losses due to data breaches.

Emphasis on Security Awareness Empowerment

Security awareness training vendors are emphasizing efficient practices as organisations seek to empower their employees to respond effectively to the changing technological landscape. The pandemic triggered the emergence of new data-driven solutions to help employees develop the skills needed to operate within frameworks designed specifically to secure them and their organizations from the latest threats. Many new security awareness training programs currently under development are aimed lowering cybersecurity risks associated with remote work (usecure, n.d.).

How to Approach Security Awareness Training

Security awareness training is designed to help employees be alert to the latest threats and take appropriate defensive steps. Cybersecurity threats are constantly changing, as attackers seek to target employees in novel ways and in areas where awareness is likely to be low. Many new employees are not well informed of security procedures and risks during the onboarding process and are therefore highly susceptible to threats. It is critical for organizations to inform their new staff on the greatest cybersecurity risks and to train them in responsible data-handling practices. Innocent mistakes can lead to severe consequences. Security awareness training helps ensure that employees do not carelessly divulge any vital details that could set them up for an attack and possibly jeopardize the entire organization. The following are some of the best approaches to security awareness training.

1 Divide Learning into Shorter Sessions

Participants in training programs may not be able to maintain their focus for more than 20 minutes per session. It is therefore a good practice to offer security awareness training in a modular fashion, as providing content in small chunks can make learning more effective. These lessons can be followed with practice sessions and simulations to evaluate employees' knowledge retention and ability to apply what they have learned. A classic example of this approach is phishing email simulations, in which (fake) malicious emails are sent to employees to gauge how they respond to them. Employees who understood the antiphishing concepts presented during their security awareness training should be equipped to take the appropriate course of action.

2 Focus on the Most Important Risks

When designing a security awareness training plan, it is important to focus on the most significant risks first. organisations usually conduct a vulnerability assessment to identify, categorize, and assign priority levels to risks in terms of their scope, financial repercussions, effect on mission-critical functions, and so on. Once the most important risks are clear, a proper threat remediation protocol can be incorporated. Security awareness training should align with an organization's overall goals, policies, procedures, and workforce culture (LiFars, 2020).

Conclusion

For organisations that are focusing on specific risks, it is important to start by educating employees on the importance of the role they play in protecting their organization's data and systems, regardless of their job function. Running phishing simulations, conducting vulnerability assessment tests, and creating personalized content for security training and education are key to improving defense systems, and making updates should prioritize feedback on implementation. When employees are equipped with the right knowledge, organisations are less likely to be hacked and can worry less about massive data breaches.

References

Alder, S. (2020, March 12). 83% of medical devices run on outdated operating systems. ***HIPAA Journal.*** **https://www.hipaajournal.com/83-of-medical-devices-run-on-outdated-operating-systems/**

Associated Press. (2010, February 8). Chinese-born engineer gets 15 years for spying. ***NBC News.*** **https://www.nbcnews.com/id/wbna35300466**

Bellet, C., De Neve, J., & Ward, G. (2019). ***Does employee happiness have an impact on productivity?*** (Saïd Business School Research Paper Series, WP 2019-13). Saïd Business School. **https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3470734**

Cimpanu, C. (2020, November 11). Microsoft urges users to stop using call & SMS-based multi-factor authentication. ***ZDNet***. **https://www.zdnet.com/article/microsoft-urges-users-to-stop-using-phone-based-multi-factor-authentication/**

CybSafe. (2020, February 7). ***Human error to blame for 9 in 10 UK cyber data breaches in 2019*** [Press release]. **https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/**

Ermetic. (2020, June 3). ***Ermetic reports nearly 80% of companies experienced a cloud data breach in past 18 months*** [Press release]. **https://www.businesswire.com/news/home/20200603005175/en/Ermetic-Reports-80-Companies-Experienced-Cloud-Data**

Hartrup, A. (2019, June 24). The role of network taps in today's hybrid data center environment. ***Data Center Knowledge***. **https://www.datacenterknowledge.com/security/what-weve-learned-12-months-colonial-pipeline-attack**

LiFars. (2020, August 20). ***5 ways to improve security awareness training***. **https://lifars.com/2020/08/5-ways-to-improve-awareness-training/**

Mimecast. (n.d.). ***What is security awareness training and why is it important?*** **https://www.mimecast.com/content/what-is-security-awareness-training/**

Ponemon Institute. (2022). ***2022 cost of insider threats: Global report***. Proofpoint. **https://www.proofpoint.com/us/resources/threat-reports/cost-of-insider-threats**

PwC. (2017). ***Consumer intelligence series: Protect.me***. **https://www.fisglobal.com/-/media/fisglobal/worldpay/docs/insights/consumer-intelligence-series-protectme.pdf**

Rahaman, M. (2022, April 22). Ethical hacking | Footprinting. ***GeeksforGeeks***. **https://www.geeksforgeeks.org/ethical-hacking-footprinting/**

usecure. (n.d.). ***12 essential security awareness training topics for 2022***. **https://blog.usecure.io/12-security-awareness-topics-you-need-to-know-in-2020**

Witts, J. (2022, April 26). The top 5 biggest cyber security threats that small businesses face and how to stop them. ***ExpertInsights***. **https://expertinsights.com/insights/the-top-5-biggest-cyber-security-threats-that-small-businesses-face-and-how-to-stop-them/**

EC-Council

www.eccouncil.org