https://doi.org/10.34074/rere.00506

Conceptual Article

Improving Cyber-Security Education and Awareness Programs for Small Teams in Enterprises

Thao Le Y Nguyen, Senaka Amarakeerthi, and Barry Dowdeswell

AUCKLAND INTERNATIONAL CAMPUS

ABSTRACT

In the contemporary digital landscape, small teams within enterprises are often targeted by cyber-criminals who seek to breach their security and access sensitive information. This article examines a range of strategies and resources to support cyber-security education and awareness programs that are tailored to the needs of small teams within enterprises. The aim is to empower individuals and teams to recognize and respond effectively to cyber-threats. After briefly explaining what cyber-security is and the type of threats a team may encounter, the article explores education strategies discussed in the current literature. The authors then present examples of resources they have identified or developed during this research. This includes an analysis of an ISO standard that presents an example risk-assessment plan as well as an interview sheet we developed for performing an initial assessment of a teams cyber-security awareness level. Strategies for educating teams about how to address typical cyber-security situations a team may encounter, such as email phishing scams, are then explored in the context of an example training plan that can be used to facilitate interactive and engaging learning. The article concludes that teams often face unique challenges, including limited resources, varying levels of technical expertise, and the ever-present risk of underestimating cyber-threats. Promoting a proactive cyber-security culture within a small team by using resources organised into an systematic program is a crucial step in building a resilient and security-aware workforce.

Keywords:Cyber-Security Awareness, Education, Team Development, Resources, and Small-to-Medium Enterprises.

INTRODUCTION

Technology has long been a key driver and enabler of modern business practice. Besides offering advantages, online technologies now present many new challenges: one is the risk of cyber-attack. A cyber-attack is an intentional effort by an outside entity to expose or steal information and often to disable or destroy an organisation's digital infrastructure (IBM, 2021). A typical example is a Ransomware exploit, a cyber-attack that encrypts computer files and sometimes locks the computer, rendering it completely unusable until a ransom payment is made (Park et al., 2022). In an era where the risk of on-line threats like this are always present, the necessity for robust cyber-security measures has never been more critical.

While the focus of cyber-security education has traditionally been on large corporations, smaller groups within Small to Medium Enterprises (SMEs) often face unique challenges. Alahmari and Duncan (2020) explain that SMEs typically employ 250 or less staff. In the United Kingdom (UK) in 2020, there were over 5.6 million SMEs, employing over 16 million staff. These organisations make a significant contribution to a national economy: in 2018, UK SMEs had a turnover in excess of £1,994 billion.

Being Secure

In the past, companies understood that "Being Secure" meant keeping accounting records, intellectual property, and client information safe behind locked doors within their business premises. There, it could only be accessed by their staff. The first Time-Sharing computer systems that allowed users to manage and exchange information remotely were not available until 1964 (Kemeny & Kurtz, 1968). Hildebrandt et al. (1980) discuss the later emergence of the first fully self-contained in-house computer systems that became available in the 1970s. These allowed organisations to store and manage data on their own computers within their own premises. This on-going digitisation of information required organisations to consider how to prevent criminals accessing their valuable intellectual property while inside their buildings (Härting et al., 2022). After that, the introduction of Remote Networking, the Personal Computer, and the Internet meant that information technology became more affordable and available to a wider segment of society, including criminals (Aieshwaryaa, 2022; Smith et al., 2004). This meant that the threat of cyber-crime, executed remotely to breach their security and steal valuable information, was a reality that could no longer be ignored.

Building a cyber-secure company environment

Riggs et al. (2023) explain that building a company environment that is cyber-secure is a complex task, typically involving two distinct aspects.

The first aspect involves the electronic infrastructure needed to protect the computers. This is accomplished by configuring intrusion-control software and hardware devices such as electronic firewalls (Blansit, 2009). Figure 1 shows a Netgate SG-1100 firewall that is commonly used to protect SMEs (Netgate, 2025). Firewalls are electronic gateways that implement rules to enable authorised users to access the information being stored in the companies computers while restricting access by outside unauthorised systems connected to the internet. While it is important for all staff to have a basic understanding of the purpose and need for such equipment, they do not have to be able to configure such devices themselves. For smaller organisations, that is often a task contracted to specialised outside cyber-security consultants.

Figure 1: A typical Netgate SME firewall appliance

The second aspect discussed by Reggs et al. is more important to the majority of employees. How they act responsibly, day-by-day, not falling prey to cyber-attacks through their actions, is a behavior that has to become both a personal habit and part of their organisational culture. Hence, implementing cyber-security education for these users aims to build awareness, foster good practices, and empower employees to recognize and respond to potential threats when they encounter them (Al-Daeef et al., 2017).

Hence choosing or creating a cost-effective program that is appropriate for small, resource-challenged teams is not simple. Many larger companies outsource their cyber-security training programs to specialist organisations. However, that may not be financially viable for all SMEs (Annarelli et al., 2021). By emphasizing ongoing education, practical engagement, and regular updates to the curriculum, organizations can cultivate a culture of cyber-security awareness and resilience.

The rest of the article focuses on recommendations from the current literature on how to address the challenges

faced by small teams. It then proposes simple guidelines for best practices, as outlined in the literature, to facilitate cyber-security education and awareness (Romansky & Noninska, 2020). It considers examples of training material that utilize interactive and practical exercises. The goal is to create an engaging, sustainable, and cost-effective learning environment (Chidukwani et al., 2022). Teams must also learn how to adapt to changes in the cyber-security threat landscape by participating in on-going education (Hatzivasilis et al., 2020).

LITERATURE REVIEW

In their 2018 State of Cyber Security in SMEs study, Bada and Nurse (2019) identified three main challenges faced by small organisations:

- Not having the in-house expertise needed to mitigate cyber-risk.
- Information Technology (IT) budget constraints.
- A general lack of understanding about how to protect against cyber-attacks.

The authors emphasise that enhancing awareness of cyber-threats should be a critical part of training programs, since it will encourage organisations to find ways to address these three issues. Making sure that employees understand company cyber-security guidelines should be a key part of both the on-boarding of new staff and the regular up-skilling of all team members. Hight (2005, page 2) comments that "As a human is generally considered the weakest link in a computer system, professional training is now becoming a necessity". This implies that companies also need to determine when it is appropriate to bring in outside resources to augment their own training initiatives.

Al-Daeef et al. (2017) explain that well-designed user training methods can effectively enhance awareness and security behaviors. The authors describe a typical criminal tactic called Phishing (NIST, 2025), a type of social engineering where cyber-criminals try to deceive users into sharing sensitive information. This can happen when they inadvertently or deliberately follow links on external web sites, in emails, or other documents they receive. This exploit can connect their computers to malicious external web sites. Once connected, the software on these sites can inject viruses or other "trojan" software entities into the user's computer system. This creates a gateway via that computer into the rest of the companies network. When cyber-criminals gain access in this way, they can explore and mine information undetected by staff, sometimes for extended periods of time. Akhgar et al. (2014) present examples of such long-term intrusions and the consequences of this sort of criminal activity.

Techniques for enhancing cyber-security awareness

Mistakes made by individuals related to their use of technologies are not always solved just by adding more technology (Orlikowski & Gash, 1994). Education is usually more effective when delivered by appropriate awareness training programs since there are limitations to how well technology can alleviate the consequences of user's mistakes. Gundu (2019) found that SMEs need to understand more about possible vulnerabilities rather than understanding how to implement security tools. This encourages them to better perform relevant self-assessment of the risks to their particular situation.

Hight (2005) proposes a range of strategies. First, training sessions need to be conducted frequently using company-approved material that includes information about the latest cyber-threats, how to recognize them, and how to adopt best practice using representative examples from historical cases. These sessions can be interactive with quizzes, games, and real-life scenario simulations.

Moreover, organizations should send simulated phishing emails to test employee's vigilance and response. This activity helps reinforce learning and provides practical experience in identifying suspicious communications. Secondly, establish and promote clear communication channels where associates can ask questions about potential threats, best practice, and report suspicious activities without fear of reprisal. Thirdly, use a variety of engaging content such as short videos, infographics, campaign events, and interactive modules to make learning about cyber-security more interesting and less tedious. Finally, organizations are recommended to provide continuous updates on new and emerging threats. This could include the use of newsletters, intranet posts, or brief informational videos to keep everyone informed (Bada & Nurse, 2019).

Bada and Nurse (2019, page 4) further explain that "It is well recognized that an individual's knowledge skills and understanding of cyber-security, as well as their experiences, perceptions, attitudes, and beliefs, are the main influences on their behavior". The authors explain that there is a set of key issues that users should focus on. These include teaching people how to identify phishing emails and malicious links by using real-world examples. Practitioners also need to provide instructions to help users learn how to respond appropriately when a security incident occurs. Other aspects such as secure passwords practices, safe browsing, correct data handling outside the organisation, and the appropriate use of mobile devices are initiatives which promote the user's goal to gain knowledge and behave well (Santa, 2010).

Organizations should be encouraged to create an environment where security is a shared responsibility while fostering a culture of security awareness. Those key strategies could be implemented to include ensuring that leadership priorities and active participation in cyber-security initiatives remain a key focus. This sets a tone of seriousness and commitment throughout the organization.

Key considerations for developing an effective cyber-security training program

The examples discussed in this section emphasised that promoting and maintaining excellent personal cyber-security behavior is the most important goal for any cyber-security education program. Daswani and Elbayadi (2021) highlight three issues that need to be considered when creating cyber-security training activities:

- The cyber-security threat landscape is changing daily. At the same time, a company's infrastructure is probably being enhanced with new equipment and software upgrades. New mobile devices, including small Internet Of Things (IoT) electronic devices (Gazis, 2021), which include security monitoring and building access control equipment, are also software devices which are attack targets for cyber-criminals.

- The number of outside connections and the volume of data moving in and out of an organisation is likely to be changing regularly. New Cloud services, including on-line accounting, travel-booking, and payroll systems are often changed as a company's needs evolve.

- Malware introduced into software during normal upgrades, including malicious macros in applications, is a serious issue. The company's cyber-security management plan should require regular updates to anti-virus software on all computers and ensuring that subscriptions remain up-to-date.

This section has emphasised that developing a cyber-security education program for an organisation is not a one-time task. Once established, it must be re-evaluated at regular intervals as both the technology platforms and the profile of staff employed evolves as the SME grows.

GUIDELINES FOR CREATING AND IMPLEMENTING A SME CYBER-SECURITY EDUCATION PROGRAM

It is important to develop, trial, and then enhance custom content for individual SME teams, since no two organisations will present the same opportunities, called a "Threat-Attack Surfaces", to cyber-criminals (Matkowsky, 2023). This implies that there is a need to understand and review potential cyber-threats and vulnerabilities that the team is most likely to encounter in their daily activities. This section summarises a range of strategies from the literature presented in the previous section as well as identifying other resources that are available from the internet. Teams can use these ideas to stimulate their thinking and then to craft their own cyber-security education programs.

Planning and up-skilling of the cyber-security lead team

A group of company staff can be co-opted to form a Cyber-Security Management Implementation team. They should have a range of skills, but do not necessarily need to be highly-technical computer experts. They are primarily representative of the typical company staff members. Working through example Cyber-Security plans and policy documents available from on-line sources will help them to formulate questions and define topics they need to investigate further. Security awareness programs should primarily be designed to influence users' behavior and understanding levels, giving them confidence to manage their particular situation (Wilson, Hash, et al., 2003).

One of the most fundamental, well-established, and internationally-recognised set of guidelines is the *Framework for Improving Critical Infrastructure Cybersecurity* (NIST, 2018) published by the National Institute of Standards and Technology (NIST). The document explains that its role is to provide a set of industry standards for best-practice cyber-security programs that are applicable to private sector needs and are both "voluntary" and "risk-based" (page 1).

The NIST guidelines stress that any framework an organisation implements must be both flexible and incorporate practices that are "repeatable". By this, they mean that a chosen response to a threat works reliably and is applicable in other circumstances whenever a similar threat is encountered. A proposed plan should provide a framework to achieve aims that NIST recommends (NIST, 2018, page 6):

- Describe the current cyber-security "posture" or state of the organisation.
- Define what the target state is that the organisation wants to achieve and establish. This implies that the team should have well-defined aims for how cyber-secure they want to be. It is understood that no organisation will ever be 100% safe from attack however there should be a well-defined understanding of what "secure-enough" means for their organisation.
- That there are mechanisms in place to identify and prioritise opportunities for improvement.
- That it will be possible to assess progress towards the goals that are being established.
- That teams should be able to communicate to internal and external stakeholders the team's understanding of cyber-security risks.

In summary, any framework or program should facilitate five key activities: identifying threats, protecting infrastructure and data, detecting intrusions, practices for responding, and processes for recovering.

Initial team surveys

Once the initial concepts have been understood by the people tasked with designing the program, one starting point for engaging with other staff is a brief survey that can be used in individual interviews. This can help to gauge employees' existing knowledge and identify potential gaps. Figure 2 is an example of an interview form the authors developed for use in future surveys and case studies, based on recommendations found in the literature review.

Figure 2: Example Survey form for use during one-on-one or department interviews.

Cyber-Security in our Organisation

Department name: _____ Name: _____

Date of interview: _____

No.	Question	Comment	Compliance
1.	What do you know about Cyber-Security?		
2.	Is Cyber-Security important when you handle business information?		
3.	Do you know who to contact if you have questions about our Cyber-Security practices and policies?		
4.	Have you read our Cyber-Security Policies and Guidelines?		
5.	What sort of information do we need to protect?		
6.	Do you know how to protect the data you work it?		
7.	Do you know who to report a Cyber-Security incident or concern to?		
8.	Have you ever downloaded or installed software on your work computer?		
9.	Should you upload business information to on-line platforms such as YouTube, Facebook, or Instagram?		
10.	Do you have any suggestions or comments about how we could become more secure here?		

The form is designed to guide a one-on-one or small team discussion without appearing to be a test. Instead, it is intended to help the team assess their overall level of knowledge by aggregating the results elicited from all participants. The first two questions are general and are designed to establish an environment where questions can be asked freely. The next three questions gauge how well supported and informed staff feel about the information, resources, and training provided to them currently. Question 5 asks if they know what are the most critical resources that they need to protect. Once these concepts have been socialised, practical examples and concerns are elicited in the remaining questions.

Understanding the types of potential cyber-threats

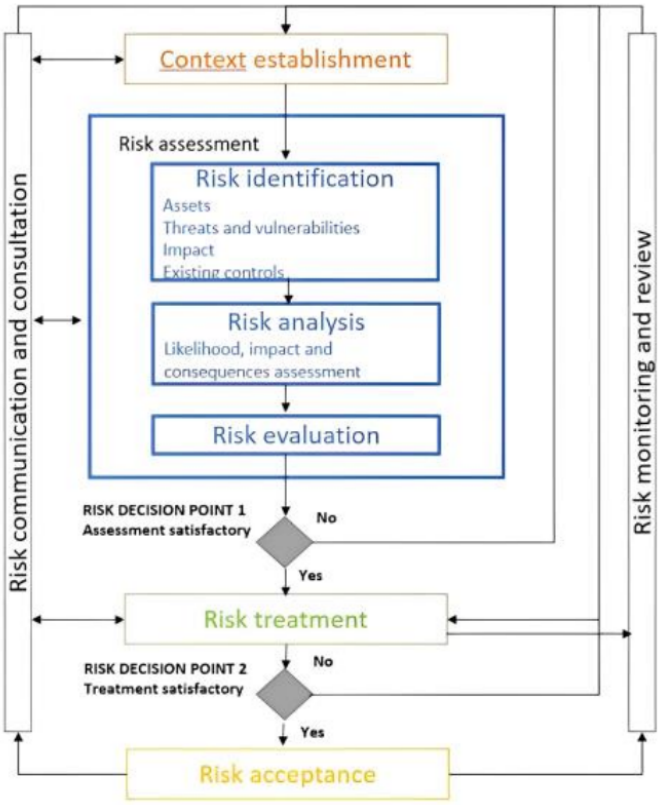
Studying examples of current cyber-threats trains the team to learn how to identify vulnerabilities in their own behavior and systems. A typical example of a serious cyber-threat that the team should understand is a *Ransomware Attack* (Park et al., 2022). The name embodies two important aspects of the threat: the purpose of the attack is to extort a payment from an organisation by holding their data and computers "to ransom" and it is executed by software called "Ransom Malware" (Kramer & Bradfield, 2010). The attackers use this type of software to encrypt important files in the target computers and then lock-down the computers, rendering them completely inaccessible and unusable. The cyber-criminals then promise to decrypt the data and release their hold on the computers in exchange for a ransom payment. Unless the situation is resolved, the information loss is either temporary or in some cases, permanent. The attack causes disruption to the companies operations and financial losses due to work not being completed or the inability to bill customers. NIST(NIST, 2018) provides an example plan that includes guidelines for protecting companies from ransomware attacks. Like many other public resources, it is freely downloadable from the NIST site (Souppaya et al., 2025).

Conducting a risk assessment

Teams should follow international guidelines when conducting a risk assessment of their organisation. The ISO/IEC Standard 27005 (ISO, 2022) outlines a detailed model recommended by Sánchez-García et al. (2023). Figure 3 was extracted from the standard, which outlines the assessment steps that begin with an initial identification of the context in which the risk could occur. An example of a risk context is the way the company staff interact via the internet with their clients, suppliers, and other parties. Is information received in electronic files, uploaded to the companies computers, and then accessed? Part of the assessment includes understanding what malicious content could be carried in those files (Melaku, 2023)

The next steps after a risk context is identified is to find specific situations or environments within the organisation where that risk could cause damage. The team should consider assets, vulnerabilities, and what

Figure 3: ISO/IEC 27005 Risk Assessment Model



the impact of a successful cyber-attack could be. The next step involves a deeper analysis of each aspect uncovered, leading to an evaluation of the risk that can be documented as something to address.

Note that the process is cyclic: not all aspects will necessarily be understood in the first pass. Sánchez-García et al. (2023) caution that it is important to plan sub-steps of risk assessment and identify real metrics for accurate risk assessment calculations. For example, what would it cost to recover or replace a damaged asset? The end result of this analysis should be a set of recommendations for how the risk should be mitigated.

During risk assessment, the SME should ask when or if the risk is such that they should seek outside expert help to mitigate it. Building some parts of an effective management program may require specialised outside technical advice. This can be a worthwhile investment to ensure that the technical aspects of the potential threats can be identified and explained to people in ways they can understand Annarelli et al. (2021) and Landoll (2021).

Employing team building activities and resources

To ensure that training is effective, other interactive and engaging learning methods can be employed. Two examples are sending custom emails that test each user's ability to recognise a phishing attempt (NIST, 2025) and the use of targeted posters and shared self-learning resources.

Posters and other media are also reported to be an effective way of socialising cyber-security practices. Figure 4 shows two typical examples. The poster on the left from Westchester University encourages vigilance by students and staff against phishing attacks, where an intruder tries to gain access to a system by deceiving a user into clicking

Figure 4: Examples of Cyber-Security Awareness Posters that can be displayed in organisations.

on content that can compromise their system (WCUPA, 2024). The second poster from the Australian consultants Caniphish is one of a set of free Cyber-Security Awareness posters they make available to organisations (Caniphish, 2025).

Activities can also include conducting random simulated phishing attacks and other practices to improve users' experiences. These activities will help associates recognize and respond to any incidents independently. Besides that, the trainer team can incorporate gamified elements such as quizzes, crosswords, and rewards to make learning more engaging and enjoyable. Moreover, organizations could design posters which explain relevant issues that users may encounter at work such as receiving phishing emails, how to create strong passwords, and the correct way to use secured websites. These posters highlight those things that users need to do or keep in mind when they perform their daily tasks. It is important that employees continue to remember, visualize, and follow cyber-security best practice.

Monitoring compliance

Monitoring the level compliance achieved by the staff is a critical aspect of maintaining a robust cyber-security posture. Once the program has been implemented, processes must be put in place to monitor compliance and effectiveness. Larger organisations employ automated tracking systems that are designed to capture key information regarding program activity (e.g., courses, dates, audience, costs, and sources). The tracking system can also capture this data at a small-team level, so that it can be used to provide enterprise-wide analysis and reporting regarding awareness, training, and education initiatives (Wilson, Hash, et al., 2003).

Formal evaluation and feedback mechanisms are critical components of any security awareness, training, and education program. Continuous improvement cannot occur without a good sense of how the existing program is working. In addition, the feedback mechanisms must be designed to address objectives initially established for the program. A feedback strategy needs to incorporate elements that will address quality, scope, deployment method (e.g., web-based, onsite, offsite), level of difficulty, ease of use, the duration of sessions, relevancy, currency, and suggestions for modification (Wilson, Hash, et al., 2003).

Continuous improvement is an on-going process that focuses on creating a level of security awareness and excellence to achieve a pervasive security presence in the organization. The processes that deliver awareness, training, and education to the workforce should be integrated thoroughly into the overall business strategy. A mature security awareness and training program defines a set of metrics for this area, and automated systems should be in place to support the capture of quantitative data and the delivery of management information to accountable parties on a regular, predefined cycle. Finally, in this stage, agencies have incorporated into their awareness and training program formal mechanisms for ongoing research in areas of technology advancement, good practices, and benchmarking opportunities.

Enterprises should consider their IT budgets when planning, based on factors such as business size, business growth expectations, business performance expectations, the emerging business landscape, and the state of their current infrastructure. Alexandra Borgeaud, who is a research expert covering cyber-security and tech in Latin America, published on the Statista website that "On average, companies worldwide allocate at least 12 percent of their IT budget to information security. The highest share was distributed in 2020, at 12.8 percent. By 2020, companies allocated approximately 12.7 percent of their IT budget to IT security" (Borgeaud, 2023b, page 10) . Moreover, the article highlighted that "In 2025, small and mid-sized businesses (SMEs) were forecast to spend 29.8 billion U.S. dollars on managed security services. Overall, SMEs were expected to spend 90 billion U.S. dollars on cyber-security in 2025, up from 57 billion U.S. dollars in 2020. The regions with the highest anticipated spend are North America, the Asia

Pacific region, and Western Europe" (Borgeaud, 2023a, page 20)

CONCLUSIONS

The increasing complexity and frequency of cyber-threats necessitates robust cyber-security education and awareness programs, especially for small teams within enterprises. These teams often face unique challenges, including limited resources, varying levels of technical expertise, and the ever-present risk of underestimating cyber-threats.

This article has outlined several strategies to enhance cyber-security education and awareness for small groups. By developing tailored training modules, employing interactive and engaging learning methods, and continuously updating content to reflect emerging threats, organizations can equip their small teams with the skills and knowledge necessary to identify and respond to cyber-threats effectively. Furthermore, promoting a proactive security culture, enabling behavior change in cyber-security implementing practical security measures, and addressing resource constraints are crucial steps in building a resilient and security-aware workforce.

By focusing on these strategic areas, enterprises can significantly improve their cyber-security posture, ensuring that even the smallest teams are prepared to defend against cyber- adversaries. This proactive approach not only safeguards sensitive information but also enhances the overall resilience and security of the organization.

REFERENCES

Aieshwaryaa, N. (2022). Cyber Crime and Criminals: An Overview. *Issue 6 Indian JL & Legal Rsch*, *4*, 1.

Akhgar, B., Staniforth, A., & Bosco, F. (2014). *Cyber Crime and Cyber Terrorism Investigator's Handbook* (1st). Syngress Publishing.

Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. *2020 international conference on cyber situational awareness, data analytics and assessment (CyberSA)*, 1–5. https://doi.org/0.1109/CyberSA49311.2020.9139638

Al-Daeef, M. M., Basir, N., & Saudi, M. M. (2017). Security awareness training: A review. *Proceedings of the World Congress on Engineering WCE 2017, London*, *1*, 5–7.

Annarelli, A., Colabianchi, S., Nonino, F., & Palombi, G. (2021). The effectiveness of outsourcing cybersecurity practices: a study of the Italian context. *Proceedings of the Future Technologies Conference*, 17–31. https://doi.org/10.1007/978-3-030-89912-7_2

Bada, M., & Nurse, J. R. (2019). Developing cybersecurity education and awareness programmes for small-and medium-sized enterprises (SMEs). *Information & Computer Security*, *27*(3), 93–410. https://doi.org/10.1108/ICS-07-2018-0080

Blansit, D. (2009). Firewalls: basic principles and some implications. *Journal of Electronic Resources in Medical Libraries*, *6*(3), 260–269. https://doi.org/10.1080/15424060903167377

Borgeaud, A. (2023a). Small and mid-sized business (SMB) cyber security spending forecast worldwide for 2025, by category. https://www.statista.com/statistics/1245710/cyber-security-spending-category-forecast-smb/

Borgeaud, A. (2023b). What percentage of your employer's IT budget is allocated to information security? https://www.statista.com/statistics/1319677/companies-it-budget-allocated-to-security-worldwide/

Caniphish. (2025). Caniphish Free Cyber Security Awareness Posters. https://caniphish.com/free-cyber-security-awareness-posters

Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. *IEEE Access*, *10*, 85701–85719. https://doi.org/10.1109/ACCESS.2022.3197899

Daswani, N., & Elbayadi, M. (2021). The Seven Habits of Highly Effective Security. In *Big breaches: Cybersecurity lessons for everyone* (pp. 195–232). Springer. https://doi.org/10.1007/978-1-4842-6655-7_9

Gazis, A. (2021). What is IoT? The Internet of Things explained. *Academia Letters*, *2*. https://doi.org/10.20935/AL1003

Gundu, T. (2019). Acknowledging and reducing the knowing and doing gap in employee cybersecurity compliance. *ICCWS 2019 14th International conference on Cyber Warfare and Security*, 94–102.

Härting, R.-C., Bühler, L., Winter, K., & Gugel, A. (2022). The threat of industrial espionage for SME in the age of digitalization. *Procedia Computer Science*, *207*, 2940–2949. https://doi.org/10.1016/j.procs.2022.09.352

Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., Hildebrandt, T., Tsakirakis, G., Oikonomou, F., Leftheriotis, G., et al. (2020). Modern aspects of cyber-security training and continuous adaptation of programmes to trainees. *Applied Sciences*, *10*(16), 5702. https://doi.org/10.3390/app10165702

Hight, S. D. (2005). The importance of a security, education, training and awareness program. *Security*, *27601*, 1–5.

Hildebrandt, B. W., Lusak, R. J., & Bright, L. R. (1980). In-House Computers: Fact or Fiction. *Journal of the American Bar Association Journal (ABAJ)*, (10), 1217–1223. Retrieved September 4, 2025, from https://www.jstor.org/stable/20746773

IBM. (2021). What is a Cyber-Attack? IBM Think. https://www.ibm.com/think/topics/cyber-attack

ISO. (2022). ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks. https://www.iso.org/standard/80585.html

Kemeny, J. G., & Kurtz, T. E. (1968). Dartmouth time-sharing. *Science*, *162*(3850), 223–228. https://doi.org/10.1126/science.162.3850.223

Kramer, S., & Bradfield, J. C. (2010). A general definition of malware. *Journal in computer virology*, *6*(2), 105–114. https://doi.org/10.1007/s11416-009-0137-1

Landoll, D. (2021). *The security risk assessment handbook: A complete guide for performing security risk assessments*. CRC press.

Matkowsky, J. (2023). Threat Intelligence-Driven Attack Surface Management. *The SANS Institute*, *8*, 12.

Melaku, H. M. (2023). Context-based and adaptive cybersecurity risk management framework. *Risks*, *11*(6), 101. https://doi.org/10.3390/risks11060101

Netgate. (2025). Netgate SG1100 Firewall Specifications. https://shop.netgate.com/products/1100-pfsense

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. *NIST Publications CWSP*, *4162018*(7).

NIST. (2025). Definition of Phishing. https://csrc.nist.gov/glossary/term/phishing/

Orlikowski, W. J., & Gash, D. C. (1994). Technological Frames: Making Sense of Information Technology in Organizations. *ACM Transactions on Information Systems*, *12*(2).

Park, J. H., Singh, S. K., Salim, M. M., Azzaoui, A. E., & Park, J. H. (2022). Ransomware-based cyber attacks: A comprehensive survey. *Journal of Internet Technology*, *23*(7), 1557–1564. https://doi.org/10.53106/160792642022122307010

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., Vuda, K. V., & Sarwat, A. I. (2023). Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. *Sensors*, *23*(8), 4060. https://doi.org/10.3390/s23084060

Romansky, R. P., & Noninska, I. S. (2020). Challenges of the digital age for privacy and personal data protection. *Mathematical Biosciences and Engineering*, *17*(5), 5288–5303. https://doi.org/10.3934/mbe.2020286

Sánchez-García, I. D., Mejía, J., & San Feliu Gilabert, T. (2023). Cybersecurity Risk Assessment: A Systematic Mapping Review, Proposal, and Validation. *Applied Sciences*, *13*(1). https://doi.org/10.3390/app13010395

Santa, I. (2010). A users' guide: how to raise information security awareness. *ENISA: Heraklion, Greece*, 1–140.

Smith, R., Grabosky, P., & Urbas, G. (2004). Cyber criminals on trial. *Criminal Justice Matters*, *58*(1), 22–23.

Souppaya, M., Fisher, W., Scarfone, K., & Barker, W. C. (2025). Ransomware Risk Management: A Cybersecurity Framework 2.0 Community Profile. https://nvlpubs.nist.gov/nistpubs/ir/2025/NIST.IR.8374r1.ipd.pdf

WCUPA. (2024). WCUPA Westchester Information Security Resources for Staff and Students. https://www.wcupa.edu/infoServices/security/ITSecurityAwareness.aspx/

Wilson, M., Hash, J., et al. (2003). Building an information technology security awareness and training program. *NIST Special publication*, *800*(50), 1–39.