

Cybersecurity best practices for small and medium-sized enterprises (smes)



03/12/20023

Emre OTU - 2349586

Interactive Learning Skills and Communication – NV1600CA

Contents

[***Cybersecurity Best Practices for Small and Medium-Sized Enterprises (SMEs)*** 2](#_Toc152471336)

[Introduction 2](#_Toc152471337)

[Importance of the Data Protection Act and GDPR 2](#_Toc152471338)

[Cybersecurity Challenges and Solutions 2](#_Toc152471339)

[Lack of Awareness 2](#_Toc152471340)

[Finite financial sources 3](#_Toc152471341)

[Lack of cyber security specialist 3](#_Toc152471342)

[Complexity of systems and cyber security tools 3](#_Toc152471343)

[Effects of DoS and DDoS attacks 3](#_Toc152471344)

[Firewall and Anti Viruses 4](#_Toc152471345)

[Conclusion 4](#_Toc152471346)

[References 5](#_Toc152471347)

# Cybersecurity Best Practices for Small and Medium-Sized Enterprises (SMEs)

## Introduction

According to the National Cyber Security Centre (2020), cyber security is to protect devices, systems, and services from cyberattacks for individuals and organizations. Furthermore, SMEs must follow the Data Protection Act (2018) General Data Protection Regulation (GDPR) in order to protect the data of individuals and organizations. As the internet and its applications are part of modern life (NCSC), it has become increasingly popular to depend on computers. Furthermore, it even affects human society. Therefore, cybernetics and cyber security concepts are woven into the majority of institutions (Singer and Friedman, 2014). However, small, and medium-sized enterprises face issues with cyberattacks significantly as the result of not having sufficient resources, insufficient budget, poor security precautions, not having cyber security expertise, and other factors (LinkedIn, 2023). The purpose of this report is to examine the cyber security challenges with practical strategies to improve the cyber security posture of organizations, and cost-effective solutions to protect the system and data of organizations and individuals.

## **Importance of the Data Protection Act and GDPR**

Currently, one of the most threatening challenges for individuals and organizations is cyber-attacks as the prevalent adoption of the Internet of Things is gaining widespread popularity (Saleem, et al., 2017). In some way, organizations must protect their and their users’ data. Therefore, the Data Protection Act and General Data Protection Regulation (GDPR) came into force. The Data Protection Act (2018) sets rules about how businesses must collect and protect data. Cybersecurity applications are involved to protect organizations' or individual’s data. Businesses which deviate from compliance with the Data Protection Act are issued fines of up to £17.5 million or 4% of the business’s annual international revenue. It is decided the greater of two (ICO, 2022). As SMEs have finite financial resources, they must pay attention to this act. Otherwise, SMEs may be on the verge of bankruptcy or experience more substantial challenges. The basis of SMEs should consist of the Data Protection Act and GDPR for the purpose of escaping fines.

## Cybersecurity Challenges and Solutions

### Lack of Awareness

According to Rawindaran, et al. (2023), the lack of awareness and acknowledgement of the consequences of cybersecurity is one of the substantial hurdles for SMEs. Several approaches are available for hackers in order to attack the victim systems. These methods might be phishing, email phishing, CEO fraud, spear phishing and so forth (IBM, 2023). The purpose of these attacks is to deceive the target, who is usually a human, in order to acquire confidential data, such as passwords. They may create counterfeit emails and send them to employees. After accruing access credentials information, they obtain unauthorized access to the system (IBM). While they are in the system, they may have access to sensitive data. As SMEs should consider the Data Protection Act and GDPR, they may desire to hold seminars to raise awareness among employees regarding phishing methods. Furthermore, it is significantly cost-effective considering the fines notably for SMEs. There are approaching methods to define if it is forged. These are in search of grammar mistakes, incongruous sender addresses, unexpected attachments, appeal-sensitive data, abbreviated links, and so forth. They might not be obvious at first look. However, they can still be distinguished.

### Finite financial sources

In addition, the constrained budgetary allocation is one of the issues that SMEs face. According to the ENISA report (2021), devoted cyber security solutions, particularly professional firewalls and SIEM (Security information and event management), require substantial financial allocation. Furthermore, it demonstrates that many of the SMEs have not devoted extra security controls even though some of them have produced innovative solutions due to COVID-19. A piece of advice for SMEs would be to consider cyber security an investment to reduce the risk and protect the organization instead of frivolous cost.

### Lack of cyber security specialist

In order to manage the additional security controls, SMEs need to employ more cyber security expertise and personnel. Owing to the fact that securing the system requires specialized knowledge. Nevertheless, the SMEs might delegate several tasks or roles to individual cybersecurity specialists (ENSIA, 2021). This may result in reducing the specialist’s attention and make them prone to incur mistakes. Moreover, cyber security specialists may experience a challenge in implementing cybersecurity-related standards, such as ISO 27001:2013 Information Security Standard and the Federal Office for Information Security (BSI) IT-Grundschutz, due to being time-consuming. Following these standards helps SMEs to be secured in the cyber threat landscape as it continuously alters.

### Complexity of systems and cyber security tools

Additional challenges would be less technologically complex and difficult in using cyber tools (Kabanda, Tanner and Kent, 2018, pp.269-282). SMEs abstain from old and complex systems. However, according to the research bigger companies sustain old systems. The reason for that is SMEs have fewer assets to maintain than bigger companies which helps SMEs to face fewer cyber threads. Old systems are no longer supported, or it is difficult to gain knowledge of the system. Furthermore, some of the cyber tools might be hard to use too. SMEs should adopt tools and systems that are suitable for them as the cost is vital.

### Effects of DoS and DDoS attacks

DoS (Denial of Service Attack) and DDoS (Distributed Denial of Service Attack) attacks should be considered by SMEs. Those attacks aim to increase the internet traffic to make the system, machine, or network unavailable for some period of time. As SMEs are facing issues with having a finite budget, having less secured and ineffective systems, lack of cyber security awareness, and insufficient amount of cyber security expertise, they may want to use third-party applications to set up their cloud system (Sharifi, et al., 2019, pp. 1-4). This makes SMEs vulnerable to DoS and DDoS attacks. Additionally, this makes exploring budget-friendly solutions more challenging. SMEs may still want to use third-party applications. Given the circumstances, they should ensure the application they are planning to use is secured.

### Firewall and Anti Viruses

Furthermore, SMEs should consider using anti-viruses and firewalls in order to secure their systems. Antivirus assists computers to scan for malware in order to protect the data from unauthorized disclosure or the system being hacked. According to NCSC (National Cyber Security Centre), every single computer and laptop should enable anti-virus in order to protect from malware. Additionally, antiviruses can detect applications with potential security vulnerabilities, and back up the data and system folders which is also vital for SMEs to protect their data. Antiviruses are sufficient for securing the system from installed or installed applications. However, SMEs should also secure their systems when they are online. The most advantageous selection for that is to use firewalls. Firewalls are to secure computers from cyber-attacks, extraneous network data, and additionally block access from malicious websites (CISA, 2023). Furthermore, the Cybersecurity & Infrastructure Security Agency contributes two diverse types of firewalls which are hardware and software. Hardware one is situated between the computer and the internet. Some of the internet service providers may supply incorporated routers. Software one should be activated by SMEs too. Software firewalls filter websites to be defined by recognized and trustworthy sources. SMEs should consider employing cyber security experts to maintain firewalls as they might be challenging (CISA).

## Conclusion

In conclusion, SMEs should define solutions to protect individuals' and organization’s data in the cyber threat landscape. There are laws in order to guide SMEs in instructing how the data should be stored and secured. These are essential for SMEs as if they deviate from compliance with the Data Protection Act are issued fines of up to £17.5 million or 4% of the business’s annual international revenue. This may result in encountering bankruptcy. Furthermore, SMEs should exercise due diligence to define solutions for other cyber security challenges, such as finite financial sources, insufficient cyber security expertise, lack of awareness, DoS and DDoS attacks and forth. Finite financial sources and insufficient cyber security expertise are the most vital challenges for SMEs. SMEs may want to use firewalls and antiviruses in order to secure their system and data. Firewalls can protect SMEs from DoS and DDoS attacks as well. However, with insufficient cyber security expertise, it might be hard to maintain the aforementioned solution. Furthermore, some of the tools and systems that are used by SMEs may be challenging too. Therefore, it is vital for SMEs to have sufficient cybersecurity expertise. Additionally, SMEs may desire to hold seminars to raise awareness among employees regarding phishing methods in order to reduce the lack of awareness which might be a cost-effective manner. To summarize briefly, SMEs should define cost-effective solutions, increase the awareness of employees, use firewalls and antivirus, employ cyber security specialists, and abstain from complex systems and tools in order to be safe in the cyber threat landscape.

## References

Cybersecurity & Infrastructure Security Agency (2023). *Understanding Firewalls for Home and Small Office Use*. Available at: https://www.cisa.gov/news-events/news/understanding-firewalls-home-and-small-office-use.

ENISA (2021). *Cybersecurity for SMEs - Challenges and Recommendations*. [online] ENISA. Available at: <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes>.

GOV.UK (2018). *Data Protection Act*. [online] Gov.uk. Available at: <https://www.gov.uk/data-protection.>

IBM (2023). *What is phishing? | IBM*. [online] www.ibm.com. Available at: <https://www.ibm.com/topics/phishing.>

ICO (Information Commissioner's Office) 2022, 'Enforcement of this code', UK GDPR Guidance and Resources, Available at: <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/data-sharing-a-code-of-practice/enforcement-of-this-code/>

Kabanda, S., Tanner, M. and Kent, C., 2018. Exploring SME cybersecurity practices in developing countries. *Journal of Organizational Computing and Electronic Commerce*, *28*(3), pp.269-282.

National Cyber Security Centre (2020). Cyber Security Small Business Guide. Available at: <https://www.ncsc.gov.uk/files/NCSC_A5_Small_Business_Guide_v4_OCT20.pdf>.

National Cyber Security Centre (2020). *What is cyber security?* [online] ncsc.gov.uk. Available at: <https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security>.

Rawindaran, N., Ambikesh Jayal, Prakash, E. and Chaminda Hewage (2023). Perspective of small and medium enterprise (SME’s) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales. *International journal of information management data insights*, 3(2), pp.100191–100191. doi:<https://doi.org/10.1016/j.jjimei.2023.100191>.

Saleem, J., Adebisi, B., Ande, R. and Hammoudeh, M., 2017, July. A state of the art survey-Impact of cyber attacks on SME's. In *Proceedings of the international conference on future networks and distributed systems*.

Sharifi, A.Z., Zaheer, H., Azizi, M.F. and Faizi, J., 2019, December. Detection and prevention of distributed denial of service attacks in SMEs: the case of CloudPlus. In *2019 Sixteenth International Conference on Wireless and Optical Communication Networks (WOCN)* (pp. 1-4). IEEE.

Singer, P.W. and Friedman, A., 2014. *Cybersecurity: What everyone needs to know*. oup usa.

www.linkedin.com. (2023). *Cybersecurity for Small and Medium-sized Enterprises (SMEs): Challenges and Solutions*. [online] Available at: <https://www.linkedin.com/pulse/cybersecurity-small-medium-sized-enterprises-smes-challenges/>.