Introduction To Cyber Security – Individual Written Report

By Matt Hyde

1 Introduction

Computer systems are commonly used to store information and support organisational practices. As a result of this, cyber-attacks that can harm, alter or access computer systems and the information they store are happening at an increasing rate. Agrafiotis et al. (2018) finds that cyber-attacks can result in various types of organisational harm. This includes financial loss, a damaged reputation and physical harm to systems, information and people. For organisations in the UK, if personal, identifying data is stolen in an attack on your information systems, you could be fined for breaching the General Data Protection Regulations (GDPR) under the Data Protection Act (2018). With these issues in mind, it is imperative that organisations consider potential risks and implement organisational practices to mitigate cyber-attacks. This can be done by creating a security policy containing a clear set of rules and requirements which in practice, can protect the organisation from cyber-attacks. This paper will discuss research into the role of security policies in organisations, propose a security policy for a large retail chain and provide a critical review of the effectiveness of the proposed policy.

2 The role of security policies in organisations

The purpose of security policies within organisations is protect their employees, data and assets from security threats. For data and assets such as computer systems, Von Solms and Van Niekerk (2013) finds confidentiality, integrity and availability to be some of the critical properties of their security. Therefore, a security policy should aim to maintain these characteristics by enforcing organisational rules and procedures which prevent unauthorised access or modification to information systems and keeps them accessible when they are required by the organisation.

According to Flowerday and Tuyikeze (2016), before the security policy can be developed, a risk assessment must be performed to identify external and internal threats to the organisation that will need to be addressed within the policy. Jouini et al. (2014) classifies external threats as natural disasters and cyber-attacks from people outside the organisation, whereas internal threats are people within the organisation who maliciously or accidentally cause harm.

A security policy will aim to mitigate these threats by informing employees of the rules and procedures they must follow to maintain the organisation's security. For this to be effective, the policy must be written and structured so that it is easily comprehensible for anyone within the organisation. Höne and Eloff (2002a) finds that employees can be left confused and uninterested by overly-technical security policies, they also explain that a security policy should be a short document with simple language which clearly informs employees of their responsibilities and defines key terms the reader must know to understand the policy. This is supported by Goel and Chengalur-Smith (2010) who finds that being concise and easy to read are some of the key factors of a successful security policy. According to Höne and Eloff (2002b), security policies should provide an introduction and explanation of the policy's scope and objectives to help employees understand their organisation's intentions. This allows employees to appreciate the importance of the policy and it's role in protecting the organisation and themself from security threats.

The introduction to the document should be followed by policy statements which explain the rules and procedures to the employees. These statements minimise the risk and impact of threats

by informing employees of their responsibilities and the consequences of failing to comply with the policy. This is supported by Straub Jr (1990) where it was found that increasing employee awareness of security and potential punishments for policy breaches decreases the likelihood of computer misuse. Helping employees to understand their role in in handling data, using information systems and how to report policy breaches protects them from potentially facing disciplinary or legal action so long as they comply with the policy. The policy statements must cover the entire system, explaining the steps employees must take to ensure it's protection. According to Gollmann (2010), this should include things such as databases and web applications. Gollmann (2010) also explains that policies can ensure that people are only permitted to access specific systems and information necessary for their roles. This would support the confidentiality and integrity of an organisation's systems as it prevents the unauthorised viewing and modification of data.

The International Organisation for Standardisation/International Electrotechnical Commission (ISO/IEC) 27000 family of information security management standards should be considered during the development of a security policy. Disterer (2013) explains that the ISO/IEC 27001 standards provide security requirements that must be met to support information security, while ISO/IEC 27002 provides guidelines on achieving ISO/IEC 27001 compliance, and that compliance with these standards will improve an organisation's information security and reputation. Lopes et al. (2019) finds that ISO/IEC 27001 compliance supports organisations in achieving GDPR compliance as it covers much of the GDPR's requirements. Because of this, a security policy that is developed with considerations for ISO/IEC 27001 compliance will increase an organisation's security and decrease the risk of breaching GDPR and potentially facing serious legal issues.

Employees must feel motivated to comply with the security policy if it is to be effective. Hu et al. (2012) explains that the top management of an organisation can increase compliance by explaining and encouraging the security policy throughout the organisation and creating a culture where employees believe in the importance of maintaining security. This is supported by Alotaibi et al. (2016) where it was found that management providing regular employee security training covering the content of the policy can increase compliance and the overall organisational security. Siponen et al. (2010) supports increasing employee awareness through training but also finds that stating the disciplinary actions that will be taken against employees that fail to follow the policy increases compliance. Siponen et al. (2010) explains that clearly communicating to employees how they will be caught and punished for breaching the policy, motivates them to make sure that they comply.

As organisations develop and grow, their security needs change over time. Because of this, a security policy must be regularly reviewed and updated to ensure that it reflects the organisation's needs and that it identifies and responds to the latest security threats. Changes to the policy will then need to be communicated to staff through updated security training. This is supported by Knapp et al. (2009) where it is found that security policy development is an iterative process where many versions of the policy are created over time and regular reviews are necessary to make sure that the policy is still relevant.

Overall, security policies support organisations in protecting themselves from security threats and legal issues by clearly communicating rules and procedures to employees through regular training. Developing an understanding of what the organisation requires of them allows employees to effectively perform their responsibilities and avoid the negative repercussions of breaching the policy.

3 Bespoke security policy for Barts Marvelous Mart

Purpose

We rely on computer systems and electronic information to organise our business. This can only be achieved if we protect their:

- **Confidentiality**: ensuring that only authorised people can view our systems and information
- **Integrity**: ensuring that only authorised people can alter our systems and information
- **Availability**: ensuring that our systems and information are accessible when they are needed

There are many threats outside and within the organisation that can put our systems, information and employees at risk.

Failing to protect against these threats can result in business, financial and legal problems for the organisation and its employees.

The purpose of this policy is to explain the procedures in place to reduce the risk and impact of threats, and the consequences for employees failing to comply with the policy.

Objectives

The objectives of this policy are to:

- implement procedures that protect the organisation's systems, information and employees
- ensure that the organisation meets it's legal obligations towards protecting personal information
- inform employees of their responsibility in protecting systems and information
- explain the consequences of breaching the policy

Scope

The policy must be strictly followed throughout the organisation.

Security training will be provided to all employees to ensure that they understand potential threats, the policy and their responsibilities.

Failing to comply with the policy will result in disciplinary action proportionate to the severity of the policy breach.

Compliance

The Chief Information Security Officer (CISO) will be responsible for monitoring employee compliance with the policy.

If you believe that you or another employee may have breached the policy, you are responsible for reporting the breach to the CISO.

Breaching the policy or failing to report a breach may result in you being required to complete addition training, receiving a warning, losing your job or facing legal action.

Review

To keep the policy relevant and informative, it will be reviewed and updated annually.

The employee security training shall be updated and provided to all employees annually.

Definitions

- **Networks**: connected computers that send information to each other
- **Anti-virus software**: computer programs that scan computers for anything harmful
- **Firewall**: monitors networks and prevents unauthorised computers connecting to or sending information to the network
- **Backups**: copies of computer systems and information that can replace the main systems and information if they're damaged or lost

Policy Statements

1. Risk assessment

Before each review of the policy, a risk assessment will be performed by the CISO to identify risks that the policy will aim to mitigate.

2. Passwords

Employees must create a password with a minimum of ten characters with at least one uppercase letter, number and symbol.

Employees must update their password at least once every six months.

An employee's new password must not be the same as any of their previous ten.

Employees must not share their passwords with anyone else.

Employees must not create or display a note containing their work password.

Employees may use approved password manager services to store their work password.

3. Computer use

Computers within the organisation will only be able to access websites and applications approved by the CISO.

Employees must only access computers or information systems with their own login credentials.

When accessing work devices, employees will be required to prove their identities with multi-factor authentication.

Records of computer use will be maintained and monitored to identify computer misuse.

Employees must logout of computer devices before they leave them unattended.

4. Email use

Emails received on work email addresses will be scanned and blocked if it is suspected that they are illegitimate.

Employee email addresses must not be used for non-work related purposes.

5. Access control

The CISO will be responsible for determining the systems and information different employees will be required to access and update for their role.

The CISO will be responsible for granting and removing access and update privileges to employees as to maintain the confidentiality and integrity of our systems and information.

Employees must not attempt to access or update any systems or information without permission.

Employee access and update privileges must be immediately updated or removed when an employee changes role or leaves the organisation.

6. Anti-virus software

Approved anti-virus software will be installed on all devices within the organisation.

Automatic anti-virus scans will be performed daily on all devices within the organisation to identify anything malicious.

If the anti-virus software alerts an employee, they must follow it's instructions and report it to the CISO.

7. Firewalls

Firewalls will be used to monitor the organisation's network and prevent anything from entering it without authorisation.

8. Backups

Backups of the organisation's systems and information must be automatically updated daily.

Backups must be stored in a separate site and network so they are unaffected by any damage to the main system.

In the event of the organisation's systems or information being damaged or lost, the latest backup must be used to replace them to keep the organisation's systems and information available for our business needs.

9. Database security

All databases within the organisation must be encrypted to ensure that they can only be viewed by authorised people.

All databases must be designed to prevent people accessing, updating or deleting data without authorisation.

10. Physical security

High-security areas within the outlets and distribution facility will be identified and locked behind finger-print scanners.

The CISO will be responsible for determining which high-security areas need to be accessed by different employee roles.

Employees must not attempt to access high-security areas without permission.

Employee physical access privileges must be immediately updated or removed when an employee changes role or leaves the organisation.

11. Suppliers

Before we conduct business or share information with new suppliers, an investigation into their information security must be conducted and approved of by the CISO.

12. General data protection regulations

Personal information stored within our systems must be handled in accordance with the General Data Protection Regulations (2016) under the Data Protection Act (2018).

4 Self-reflective review of the bespoke security policy

The security policy is brief, uses simple language that can be easily followed by employees and defines key terms that the employees must understand. According to Höne and Eloff (2002a), this will make the policy more effective as it will be more engaging and understandable for employees. This will help to reduce the risk of accidental insider threat as the policy will be better understood and practised throughout the organisation.

Several common areas of information security standards outlined by Höne and Eloff (2002b) are included in the policy. The policy begins by defining it's purpose which explains why the organisation needs to protect it's assets, informs the employee that they have a role in protecting these assets and that there are consequences for failing to do so. The objectives give a clear explanation of the policy's intention and the scope clarifies that the policy needs to be practised throughout the organisation. Clearly communicating this key information to employees should decrease insider threat as Pahnila et al. (2007) finds that policies containing high quality information have higher employee compliance.

The policy's statements are designed to briefly and explicitly explain what is required of the employees, by using unambiguous language such as "employees must". This was done to reduce the risk of employees misinterpreting the policy and accidentally exposing the organisation to threats by failing to correctly follow the rules and procedures. This is supported by Buthelezi et al. (2016) where it is found that more implicit policies are ambiguous and difficult to follow.

The organisation will have computer systems involved in their web systems and warehouse operations, and databases storing information critical for the business. Because of this, the policy covers areas of security highlighted by Gollmann (2010) such as, access control, firewalls and database security to prevent insiders from accessing or altering the organisation's systems and information without authorisation.

According to Siponen et al. (2010), informing employees of the consequences of breaching the policy will increase compliance. This is supported by Straub Jr (1990) who also finds that increasing employee awareness of how breaches will be discovered increases compliance. In the policy, the potential disciplinary actions for breaching the policy are discussed and the monitoring of employee use of computer systems are mentioned. This will encourage employees to follow the policy and deter potential malicious insiders by highlighting how non-compliance will be discovered and punished.

The policy enforces annual security training for all staff. Alotaibi et al. (2016) finds that employees need regular training to improve their understanding and compliance with the security policy. The training will increase the overall organisational compliance with the policy and reduce the chance of accidental insider threat by educating employees about their responsibilities.

The policy requires an annual review where a risk assessment is performed and used to update the policy before updating and delivering employee security training. This allows the organisation to regularly identify new threats and areas of weakness in the current policy and update them so that they cannot be exploited by insiders. This is supported by Knapp et al. (2009) where it is found that regular policy reviews keep them relevant and effective over time.

5 Conclusion

In conclusion, security policies exist to protect organisations and their employees from threats such as cyber-attacks. A bespoke security policy for Bart's Marvelous Mart has been created and reviewed following research into academic studies of security policies. The review finds that the policy will reduce insider threat as the language and structure of the document is easy to understand, the scope and consequences of breaching the policy are clear and there are plans to update the policy and employee training to maintain their effectiveness over time.

References

Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S., and Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, 4(1):tyy006.

Alotaibi, M., Furnell, S., and Clarke, N. (2016). Information security policies: A review of challenges and influencing factors. In *2016 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 352–358. IEEE.

Buthelezi, M. P., Van Der Poll, J. A., and Ochola, E. O. (2016). Ambiguity as a barrier to information security policy compliance: A content analysis. In *2016 International Conference on Computational Science and Computational Intelligence (CSCI)*, pages 1360–1367. IEEE.

Disterer, G. (2013). Iso/iec 27000, 27001 and 27002 for information security management. *Journal of Information Security*, 4(2).

Flowerday, S. V. and Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *computers & security*, 61:169–183.

Goel, S. and Chengalur-Smith, I. N. (2010). Metrics for characterizing the form of security policies. *The Journal of Strategic Information Systems*, 19(4):281–295.

Gollmann, D. (2010). Computer security. *Wiley Interdisciplinary Reviews: Computational Statistics*, 2(5):544–554.

Höne, K. and Eloff, J. (2002a). What makes an effective information security policy? *Network security*, 2002(6):14–16.

Höne, K. and Eloff, J. H. P. (2002b). Information security policy—what do international information security standards say? *Computers & security*, 21(5):402–409.

Hu, Q., Dinev, T., Hart, P., and Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, 43(4):615–660.

Jouini, M., Rabai, L. B. A., and Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, 32:489–496.

Knapp, K. J., Morris Jr, R. F., Marshall, T. E., and Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & security*, 28(7):493–508.

Lopes, I. M., Guarda, T., and Oliveira, P. (2019). How iso 27001 can help achieve gdpr compliance. In *2019 14th Iberian Conference on Information Systems and Technologies (CISTI)*, pages 1–6. IEEE.

Pahnila, S., Siponen, M., and Mahmood, A. (2007). Employees' behavior towards is security policy compliance. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*, pages 156b–156b. IEEE.

Siponen, M., Pahnila, S., and Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer*, 43(2):64–71.

Straub Jr, D. W. (1990). Effective is security: An empirical study. *Information systems research*, 1(3):255–276.

Von Solms, R. and Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, 38:97–102.