Overcoming the Challenges of SMEs and Research Organization's Cyber Security Management: The Case of Smart Innovation Norway

A.M. Belay[*], S.Reardon[**], M.Lerario[*], H. Tuiskula[*]

[*]Smart Innovation Norway
Håkon Melbergs Vei 16, 1783 Halden, Norway
**DNV AS
Veritasveien 1, 1363, Høvik, Norway

ABSTRACT

The paper investigates the cybersecurity management systems of SMEs and research institutes. It identified the key aspects of cyber security management and explored the sources and types of cybersecurity challenges with their associated risks and mitigation methods. Smart Innovation Norway (research organization) was considered as a case and the authors analyzed user data collected from its five different departments during six months. For the analysis purpose, various statistical methods and visualization dashboards were used. In the analysis, the authors extracted usage data from the organization's Microsoft tenant using the dedicated tools for compliance and security. The result from the analysis showed a total compliance score for Smart Innovation Norway (SIN) of 85%. This score is based on ISO 27001 controls. We also investigated the main reasons for improvement to achieve the required compliance level. The research analyzed the impact of IT awareness before and after training and compared the compliance score of SIN with similar-sized organizations using Microsoft 365 portals. The result comprises a business impact assessment and the bow tie method which includes mitigation actions and preventive measures. Furthermore, the paper lays a foundation and has implications for managing cyber security not only for the SME and research organization but also for startups that have limited resources.

Keywords: Cybersecurity system, compliance, risk, mitigation, SMEs, research, framework, innovation

1 INTRODUCTION

Using the right approach to manage cyber security and information systems helps to protect an organization's systems and networks. This would be possible by properly planning and carrying out appropriate and proactive security measures at different levels of the organization. Indeed, these need disruptive solutions and a structured framework to prevent critical information from being damaged, stolen, or in some cases compromised.

This paper investigated and discussed the key aspects of cyber and information security for better data management in a research organization for the purpose of making safe an organization's data, clients' and employees' information, or any type of stored information from cyberattacks or a security breach.

2 LITERATURE REVIEW

The general literature in connection to the thematic areas of the research is summarized in table 1 below and the key aspects are discussed in section 3.

Key aspects of cyber and information security	**Authors**
Definitions of cyber and information security	[1], [2], [3]
Business and cybersecurity impact	[8], [9]
Organizational cyber and information security culture	[4], [6], [7]
Protection, risk management, and mitigation	[5] [12]
Intellectual property and the General Data Protection Regulation GDPR	[10], [11]

3 KEY ASPECTS OF CYBER SECURITY MANAGEMENT

3.1 Key definition and concepts of information and cyber security

The proliferation of security terms has led to some confusion on what is meant by, and the differences between information and cyber security. The International Standards Organisation definition of information security Management systems (ISMS) i.e., as ISO/IEC 27001 formally specified, the Information Security Management System is a governance arrangement comprising a structured suite of activities with which to manage information risks called 'information security risks in the standard[1]. The classification of the sensitivity of the data is a key component in the standard whereby the level of protection and its associated safeguards are identified and prioritized[2].

Although Cyber security is claimed and has become an increasingly important topic in modern organizations[3], it is perhaps less well defined as there is no universally agreed definition of the term. For example, the Cybersecurity & Infrastructure Security Agency (CISA) in the United States defines cybersecurity as: Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring

[1] https://www.iso27001security.com/html/27001.html

[2] https://eits.uga.edu/access_and_security/infosec/pols_regs/policies/dcps/

[3] https://webstore.iec.ch/preview/info_iec62443-2-1%7Bed1.0%7Den.pdf

confidentiality, integrity, and availability of information[4]. This definition relies on the 'three pillars of cyber security' namely confidentiality, integrity, and availability but this does not take into account the needs of industrial control systems (industry 4.0 cyber-physical) where safety is the priority. (IEC 62443 Industrial Automation and Control Systems Security Management System).

Another definition of Cyber Security, which is a little more wide-ranging is "Cyber security is the application of technologies, processes, and controls to protect systems, networks, programs, devices and data from cyber-attacks"[5].

Other broader approaches and industrial models of Cybersecurity have also been discussed which include Safety, Reliability, and Productivity (SRP) and Reliability, Availability, Maintainability, Safety, Environment, and Security (RAMSES). However, it is important to note that the order of the terms does not imply a hierarchical aspect of importance rather the organization should base its decisions on what is most important to it and the data it holds. For example, an industrial control system is unlikely to contain 'confidential' data as regulated by various privacy laws so efforts to secure the system would focus on the integrity of the data and its availability.

In general, Cybersecurity is more likely to be understood as all activities taken to ensure that the functioning of an organization can continue both by resisting compromise and recovering after an unwanted event. In this regard, many organizations consider the implementation of a security management system as a "one-off exercise". In reality, the most effective organizations embrace the concept of 'continuous monitoring and improvement' as a key concept in many of the ISO standards.

A distinction also needs to be drawn between compliance or certification with a standard, whether the information or cyber security. This distinction is particularly relevant to SMEs and research organizations that may lack the resources to acquire a recognized certification. Some organizations choose certification when it is a requirement from their clients and it can be a market differentiator. By achieving compliance an organization can confidently state that they welcome an audit by their client. Also relevant is whether compliance with a standard actually achieves the objective of being safe and secure. For example, as an analogy, consider the case of a person wearing only a swimsuit and riding a motorcycle. They are wearing a crash helmets and also wearing gloves. They are compliant with the law but are they secure? This would give insight that security has to be considered in the context of the organization's operations.

3.2 Impacts of Information and cybersecurity in business and research

It is beyond the resources of most SMEs to have a consistent and effective level of security across all of their activities. Therefore a business impact assessment (BIA) should be conducted to identify all the processes that, if they are adversely affected, would cause the organization to fail. Once this has been done, the security measures and recovery actions to ensure survival can be prioritized for the identified processes. Examples of this could be contractual penalties, irrecoverable reputational damage, or products/services with high margins.

3.3 The role of organizational security culture

A fundamental requirement for any organization from a sole trader to a multi-national is that it has a 'security culture. This means that everyone has an understanding of the need to protect their assets and displays a healthy cynicism toward everyday events. The responsibility for this culture has to be owned and championed by the most senior people and permeate from the top to the very bottom. In a global business context with extensive communication, it should not be assumed that the standards and ethics in a country will be observed by others as this is certainly not the case.

3.4 The relevance of protection, risk management, and mitigation

Total cyber or information security does NOT exist. Best efforts should be made but it is widely accepted that it is just a question of when you are breached and not if. It is common practice to deploy a number of risk controls that create multiple layers of security and these can be technical, policy-driven, or physical. This is known as 'defense in depth'. What is often not realized is that there is a need for controls to be planned for after an incident occurs. The purpose of these controls is to minimize the impact after the preventative controls have failed. A very effective method of designing and visualizing these controls is to use the 'bow tie' method. Taking the shape of a 'bow tie' the left-hand side shows the controls deployed to prevent the unwanted event e.g a data breach. The right-hand side shows the various outcomes and how they can be minimized. These might be public relations statements or technical measures to avoid your whole network collapsing.

Calculating risk can take two distinct forms. Quantitative is data-driven whereas qualitative is more based on experience and intuition. The method chosen really depends on the business itself and the context in which it operates but a hybrid method using multiple techniques is commonly used. The objective of assessing risk is to determine what risks need mitigating, what can be accepted, what can be transferred e.g insurance, and finally what cannot be accepted.

3.5 The values of understanding intellectual property and the General Data Protection Regulation GDPR

Intellectual property is arguably the most valuable asset an organization owns and protecting it should be a priority. Many organizations rely on patents, trademarks, and trade secrets with a remedy for misuse to be settled in a court of law. This may work well in a country with an established and independent judiciary but these actions are very expensive and time-consuming. Obtaining legal relief in different jurisdictions around the world can just be impossible. Therefore careful consideration should be given

[4] https://www.cisa.gov/uscert/ncas/tips/ST04-001

[5] https://www.itgovernance.co.uk/what-is-cybersecurity

to the most effective way to avoid a loss of the intellectual property before relying on the legal system.

4 METHODOLOGY, CASE DESCRIPTION, AND DATA SOURCE

4.1 Methodology

The research employed mixed methods which include a review and a case study of an SME focusing on research and innovation. The data is collected from the case organization repository, information shared within and external sources, and the information gathered from internal cyber security awareness training (a comparative study of the change before and after the training) is considered and analyzed.

4.2 Case Description

SIN is a research organization with five interconnected innovation platforms including energy, Applied AI, smart city and communities, venture, and communication. SIN's completed and ongoing projects cover different thematic areas of which in which, and most of the projects are directly and indirectly connected to the energy. By considering SIN as a case organization, different types of data are collected from its 5 different departments during a year. For the analysis, various statistical methods and visualization dashboards are used.

Data Sources: The five departments forming a unique innovation platform of SIN are used as the main source of data (figure 1). The majority of the information is based on national and international projects of SIN and the day-to-day activities and operations of the organization.

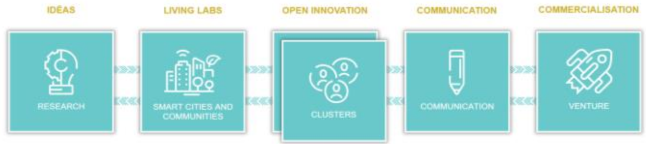


Figure 1: SIN's five innovation platforms.

4.3 Data collection methods

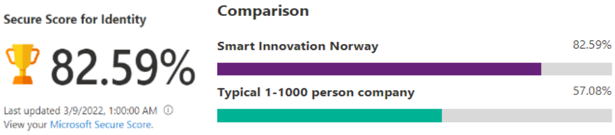
Research data was collected from the case organization in multiple ways such as from the existing servers, awareness training of employees, simulations, user logins, number of compromised guest users, and activities.

- Security analysis from users' activities (anonymized): the general data collection of the security level and risk of users within the organization is based on overall general behavior.
- Compromise rate of users within the organization before / After IT awareness training (anonymized): based on the data collected, users have shown an increase in awareness after training. Following an IT awareness course, users have started to report more emails as phishing and being more suspicious of emails they are not sure about which has increased general awareness and caution throughout the organization.
- Simulation training type: Credential harvest, Drivebyurl, Attachment malware, Social engineering attempts. Data on this topic was collected over a period of three months January, February, and March. The data is intended to give insights into how users are affected by several cyber-attacks and to determine which threats are the most effective in compromising users.
- Blocked Emails: the data is meant to show how many emails have been prevented through E-mail spam filtering and other mitigation processes that are available.

5 DATA ANALYSIS, AND RESULT DISCUSSION

5.1 *Data analysis and result discussion*

- *Security Analysis from users:* based on the data collected during the period of 6 months, the research has concluded that users have become more aware of phishing attempts, malware attachments, and general websites that may have contained some malicious software. This has also been seen in the number of e-mails being reported by users recently which has had an impact on the overall security awareness.



Secure Score for Identity

82.59%

Last updated 3/9/2022, 1:00:00 AM

View your Microsoft Secure Score.

Comparison

Smart Innovation Norway 82.59%

Typical 1-1000 person company 57.08%

Figure 2: SIN Security Score and comparison to other businesses.

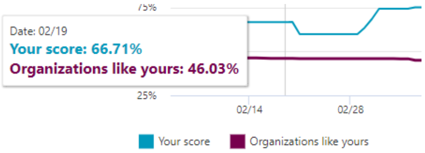


Figure 3: SIN Score based on other organizations.

Some of SIN's main risks, preventive and mitigation actions are presented in Figure 4.

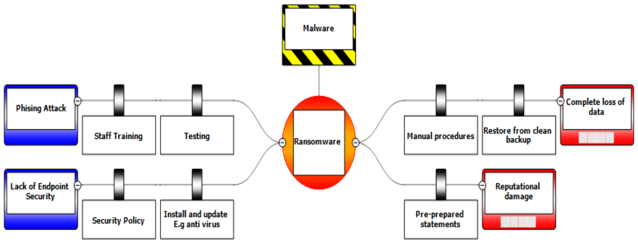
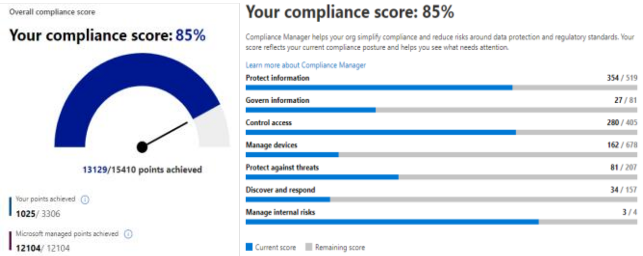


Figure 4: Example Bow tie method for risk management.

- *Results from Awareness training:* the results have shown that specific users, that used to be categorized as risky, have improved their behavior when operating with the company systems and e-mail. This has also had an impact on the methodology outlined in chapter 4.3 about the organization's security culture which has improved during the period under review.

General data about ICT compliance and score based on users' behaviors:

- *Security compliance score based on mitigation efforts:* the results have shown a general increase in the organization's compliance towards applicable ISO 27001 controls, and have shown that ISO certification is not necessarily required for SMEs as their business impact assessment mostly focuses on compliance according to their business needs.



Overall compliance score

Your compliance score: 85%

13129/15410 points achieved

Your points achieved
1025/ 3306

Microsoft managed points achieved
12104/ 12104

Your compliance score: 85%

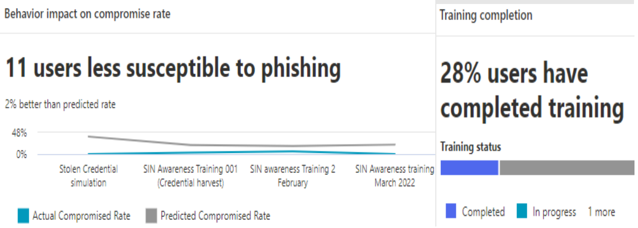
Compliance Manager helps your org simplify compliance and reduce risks around data protection and regulatory standards. Your score reflects your current compliance posture and helps you see what needs attention.

Learn more about Compliance Manager

Protect information	354 / 519
Govern information	27 / 81
Control access	280 / 405
Manage devices	162 / 678
Protect against threats	81 / 207
Discover and respond	34 / 157
Manage internal risks	3 / 4

Figure 5: SIN Compliance score based on Microsoft's guidance on ISO 27001 Controls.

- *Compliance improvement actions that still remain after implementation:* in the case of SIN, there are still some improvement actions (bow tie method Figure 4, compliance score Figure 5) that should be made to ensure the security of the data in the organization. However, they have not been implemented due to the negative effect on the working environment that may result.
- *ISO 27001 compliance level:* the results have confirmed that a compliance level of around 68% based on the ISO requirements is sufficient for SMEs to aspire to and/or exceed to be more secure than most companies of the same size. The results also show the importance of having conducted a proper business impact assessment to ensure that the most sensitive documents and intellectual property are sufficiently protected.



Behavior impact on compromise rate

11 users less susceptible to phishing

2% better than predicted rate

48%
0%
Stolen Credential simulation
SIN Awareness Training 001 (Credential harvest)
SIN awareness Training 2 February
SIN Awareness training March 2022
Actual Compromised Rate
Predicted Compromised Rate

Training completion

28% users have completed training

Training status

Completed
In progress
1 more

Figure 6: Phishing training score for users in SIN 2022.

- *Completed user training:* users have shown an interest in taking IT awareness training when failing security tests sent out by IT administrators, and have become less susceptible to phishing attempts.

6 CONCLUSION

The paper identified key aspects of cyber and information security and discussed them by considering the case research organization. The result showed how awareness training within an organization can reduce the susceptibility to phishing attempts with only 28% of users completing the cyber security awareness training. The secure identity score of SIN is calculated at 82.59% which is better compared to similar size organizations(typical 1-1000 person companies with 57.08%). The total compliance score of SIN is 85% demonstrates that there is still a need for improvement in managing cyber security.

REFERENCES

[1] Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10).

[2] Ciolan, I. M. (2014). Defining cybersecurity as the security issue of the twenty-first century. A constructivist approach. Revista de Administratie Publica si Politici Sociale, 12(1), 40.

[3] Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. computers & security, 38, 97-102.

[4] Reid, R., & Van Niekerk, J. (2014, August). From information security to cyber security cultures. In 2014 Information Security for South Africa (pp. 1-7). IEEE.

[5] Cains, M. G., Flora, L., Taber, D., King, Z., & Henshel, D. S. (2021). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. Risk Analysis.

[6] Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2020). A cyber-security culture framework for assessing organizational readiness. Journal of Computer Information Systems, 1-11.

[7] Glaspie, H. W., & Karwowski, W. (2017, July). Human factors in information security culture: A literature review. In International Conference on Applied Human Factors and Ergonomics (pp. 269-280). Springer, Cham.

[8] Choi, J., Kaplan, J., Krishnamurthy, C., & Lung, H. (2019). Hit or myth? Understanding the true costs and impact of cybersecurity programs. Perspectives on Transforming Cybersecurity, Digital McKinsey and Global Risk Practice, 8-17.

[9] Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. Computers in industry, 114, 103165.

[10] Schneider, G. (2018). European intellectual property and data protection in the digital-algorithmic economy: a role reversal (?). Journal of Intellectual Property Law & Practice, 13(3), 229-237.

[11] Sandru, D. M. (2019). On the Relationship between the Data Protection (the General Data Protection Regulation Specifically) and the Intellectual Property. RRDE, 21.

[12] Kure, H. I., Islam, S., & Razzaque, M. A. (2018). An integrated cyber security risk management approach for a cyber-physical system. Applied Sciences, 8(6), 898.