RAIS October 2022 | RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES

DOI: 10.5281/zenodo.7372481

Preconditions for the Compliance in Cybersecurity

Inga Malinauskaite-van de Castel

PhD, Mykolas Romeris University, inga.malinauskaite@mruni.eu

ABSTRACT: In the last few decades, cybersecurity regulations have developed rapidly, and there have emerged new regulatory areas that may influence security, which were not known before, and which have to be followed up on. Individual persons, companies, and states have to adjust quickly to these new approaches and comply with the norms of cybersecurity. This article reveals the main preconditions for a successful cybersecurity compliance process. The aim of this article is to reveal the preconditions which impact a successful cybersecurity compliance process in organizations and companies.

KEYWORDS: compliance, cybersecurity, preconditions for compliance implementation

1. Introduction

The term *compliance* has become well known during the last decade, when regions and countries have enacted new regulations which have had to be implemented. Generally, compliance means adhering to a rule, such as a policy, standard, specification, or law. According to the Cambridge Dictionary (2022), in law the word *compliance* refers to the obeying of a particular law or rule or acting in accordance with an agreement. Political scientist John Scholz has used game theory to understand the interactions between regulators and the regulated and has developed the question of compliance from the perspective of behavioral psychology (Roch, Scholz, and McGraw 2000). These discussions may further lead to sectoral compliance matters, including healthcare, the financial sector, energy, and government. From a practical point of view, compliance needs to be viewed as a continuous organizational process and not as a reactive response.

Cybersecurity covers all aspects of the prevention, forecasting, tolerance, detection, mitigation, removal, analyzis, and investigation of cyber incidents (ENISA 2017). It is critically important to implement the necessary legal regulations (including IT, legal, and privacy norms) in order to ensure the success of cybersecurity. Cybersecurity regulations themselves are quite recent developments, and cybersecurity strategies are akin to guidelines; basic acting points which the governments of different countries follow. Each country chooses its own method of regulating cybersecurity issues by issuing the main cybersecurity laws and the ensuing governmental decisions.

This article researches the connection between compliance and cybersecurity. The author will reveal the main reasons and preconditions for formal compliance and will assess those reasons with the help of experts by implementing qualitative expert questionnaires. The conclusions and recommendations will be presented in the final section of this article.

2. Overview of the Main Reasons and Preconditions for Successful Compliance in Cybersecurity

In reality, compliance ensures a base level of security to which companies must adhere in order to "tick the box" and receive an official signature on a document. The concrete criteria which define compliance in cybersecurity will be further analyzed. Cybersecurity compliance is a continuous process, which should be handled in a very structured and accurate manner in order to achieve the desired results. Having in mind the gap between the legal regulation setting the requirements and real practical implementation in cybersecurity, the process of cybersecurity compliance should be handled very seriously as an important matter. Therefore, there should be a culture and mentality of compliance in cybersecurity from top-level management, which needs to constantly be updated. Afterwards, the necessary resources should be provided – for example, an information security officer, who should lead by continually communicating strategy and a vision of

cybersecurity compliance. Lastly, the required policies should be in place – for example, an information security policy establishing the constant monitoring of cybersecurity matters in the organization and providing annual (or more frequent, if necessary) reports on those matters to management. Each of these criteria is further presented in a more detailed manner.

2.1. The commitment of senior management

The importance of cybersecurity matters in an organization should come from the highest level of management. As was established by ENISA, senior management should set a new direction of security culture through statements, slogans, awareness campaigns, examples, rewards, and sanctions (ENISA 2017). These scientific findings emphasize the critical role that top-level management plays in mediating the influence of institutional pressures on cybersecurity strategy (Ogbanufe, Kim, and Jones 2021).

Organizational culture will change as it is shaped by the commitment of senior management and reinforced through a corporate information security policy. In day-to-day business, senior managers should demonstrate the importance of cybersecurity in organizations. The objects and activities of information security must be in line with the organization's business objectives and the requirements imposed by them. Senior management must take charge of this, providing visible support and showing real commitment. In practical terms, this commitment involves allocating the necessary funding to information security work and responding without delay to new situations. Senior managers should demonstrate an attitude and an ongoing commitment towards the implementation of cybersecurity in their organizations. Senior managers should also take the initiative in organizing cybersecurity awareness programs, which are well established strategies for raising the cybersecurity resilience of employees.

In addition, senior management must also continuously increase their knowledge regarding cybersecurity. Training for a better understanding of the complexities of cybersecurity is essential for experienced managers to improve their decision-making (Jalali, Siegel, and Madnick 2019).

2.2. Facilitating a culture of cybersecurity

One of the strongest factors in the cybersecurity of an organization is human involvement and engagement in these processes. Considering that nearly half of all cybersecurity incidents are due to human error (Jeong et al. 2019), this author strongly believes that students should become acquainted with certain cybersecurity programs in the early days of schooling. Such programs would contribute to forming the correct beliefs, attitudes, assumptions, and, later, behaviors, which may have a highly relevant impact when addressing cybersecurity culture. Employees are often seen as the weak link in cybersecurity (Reegård, Blackett and Katta 2019). In other words, employees have certain values, and therefore demonstrate certain behaviors that can either support the protection of organizational assets or endanger them (Al Hogail and Mirza 2015). In addition, cybersecurity culture carries important practical consequences. Organizations must develop a certain level of cybersecurity culture in order to reduce or minimize the risks incurred by employees. Scientific research refers to the following dimensions of cybersecurity culture: support of management, cybersecurity policy, cybersecurity awareness and training, involvement and communications, and learning from experience (Al Hogail and Mirza 2015). Other authors refer to strategy, technology, people, organization, and environment (Al Hogail 2015); whilst some refer to management commitment, employees' attitudes, reporting culture and reactions to incident reporting, safety training and education, and general information security issues (Nævestad et al. 2018).

In the opinion of this author, there are 3 important layers when talking about the cybersecurity culture of an organization: 1) personal (human); 2) technological (systems); and

3) organizational (policies). In order to achieve the minimum standard of cybersecurity culture, all 3 layers must be addressed.

At the personal level, aspects such as cyber hygiene, individual personality, self-discipline, and knowledge must be taken into consideration. To ensure personnel are actively contributing to the security culture of their organization, a cybersecurity awareness training program should be developed. An information security officer should be responsible for cybersecurity within their organization – they should oversee the development and operation of the cybersecurity awareness training program. Research implemented in 2012 revealed that individuals with different personality traits indeed reacted differently to the same scenarios, implying that the approach we adopt to cybersecurity training must also differentiate between individual employee personality types (McBride, Carter, and Warkentin 2012).

At the technological level, technological aspects such as software and hardware, portable devices, usage of email, internet, and authentication must be reviewed in the organization. Personnel should be advised to take special care not to post work information online unless authorized to do so, especially on internet forums and on social media. In addition, to ensure that the personal opinions of individuals are not misinterpreted, personnel should be advised to maintain separate work and personal accounts for online services, especially when using social media. When personnel send and receive files via unauthorized online services, such as messaging apps and social media, they often bypass security controls put in place to detect and quarantine malicious code.

Finally, at the organizational level, an empowered and constantly-maintained knowledge-based organizational cybersecurity culture should be promoted. This includes culture through statements, slogans, awareness campaigns, examples, rewards, and sanctions. For example, when entering the organization, future employees should be presented with a cybersecurity knowledge test that evaluates their preparedness to become part of the organization. Based on the first assessment, the employee should then receive proper training and future cybersecurity-awareness-raising activities should be scheduled.

2.3. A dedicated budget

What is the value of cybersecurity in an organization? Most current research suggests that cybersecurity in an organization can improve competitive advantage (Kosutic and Pini, 2022). In order to achieve this goal, organizations should assign a concrete amount of money to the management of cybersecurity. Some organizations even insure their practices against cybersecurity threats. The size of the global cybersecurity insurance market in the post-COVID-19 world is projected to grow from $7.8 billion in 2020 to $20.4 billion by 2025, at a CAGR of 21.2% during the forecast period (MarketsandMarkets 2022).

What is the typical cybersecurity budget of an organization? There is no one-size-fits-all answer when trying to decide what a ‘typical budget’ looks like for cybersecurity operations, but there are a few studies that can provide some insight. A recent study by Deloitte and the Financial Services Information Sharing and Analysis Center (Deloitte Insights, 2020) found that financial services on average spend 10% of their IT budgets on cybersecurity. This is approximately 0.2% to 0.9% of company revenue, or $1,300 to $3,000 spent per full-time employee.

Coming from the concrete numbers to the inside of the organization, some important factors should be addressed. Cybersecurity measures in a budget can include regular training, safe email practices, secured systems, and a good cybersecurity policy (Santini 2017). One of the most vulnerable elements of cybersecurity is the personnel or human factor; therefore, some amount of money needs to be dedicated to the constant training of employees. Second comes the technological part of the organization. Each organization is different depending on its size and type of activity; however, the majority are currently dependent on technological

and internet-based solutions, and the protection of this needs to be regularly updated. Therefore, organizations need to dedicate some amount of money to the protection of their assets. Lastly, there exists the possibility to insure the organization against cyberattacks and related damages.

2.4. The information security officer's duties

Studies indicate that following IT security breaches, some impacted firms adopt a reactive plan that entails the re-organization of the existing IT security strategy and the hiring of an information security officer (Karanja 2017). An information security officer should be responsible for the whole continuous process of cybersecurity compliance in the organization, and should have a risk road map for the organization.

This NIS directive helps to empower the information security officer's visibility and communication with the senior management team (European Union Agency for Cyber Security 2016). The information security officer's functions might be as follows:

a) Be responsible for making sure that all information assets and technologies are properly protected, including third parties' handling of them.
b) Own the Information Security Policy in the organization and be responsible for reducing information and IT risks.
c) Direct the establishment and implementation of the Information Security Policy and related procedures.
d) Monitor the application of the information security objectives through key risk indicators.
e) Report and advise the management body regularly and, on an ad hoc basis as needed, report on the status of the information security management system and risks, including cybersecurity policies and material cybersecurity risk to the institution. This may include, for example, information about information security projects, information security incidents, and the results of information security reviews.
f) Ensure, upon signed acknowledgment, the acquainting of new employees with the requirements and responsibilities laid down in the Information Security Policy and other internal legal acts of the organization regulating information security.
g) Ensure the explicit defining of tangible property, as well as the execution and maintenance of the inventory of tangible property.
h) Provide and adapt physical protection measures with the purpose of protection of the organization's property from damage that may be caused by fire, flood, or other natural or human disasters.
i) Organize the risk and compliance assessment.
j) Coordinate the investigation of information security incidents, cooperate with competent authorities, and notify them on information security incidents that have occurred.
k) Notify the Head of Administration of any important security event or incident and their investigation thereof.
l) Organize the training of employees in the field of information security, periodically notify employees of new threats, and submit recommendations regarding information security.

Regarding the hierarchical positioning of the information security officer in the organization, it is definitely encouraged to have them serve as the independent officer accountable to senior management. Studies suggest that there is an alignment with the need for an information security officer to directly report to the board and to be independent (Monzelo and Nunes 2019). There is also the view that the information security officer should

be part of the board itself, deriving from the criticality of their function for business strategy (Monzelo and Nunes 2019).

2.5. Risk management as a process in cybersecurity compliance

Based on the above annual reports (for example, the Netherlands), it might be noted that risk management becomes one of the key elements in cybersecurity. Elements of cybersecurity risk management include identifying risks, defining preventative implementation measures, mitigating the impact of an attack, and establishing a continuity plan.

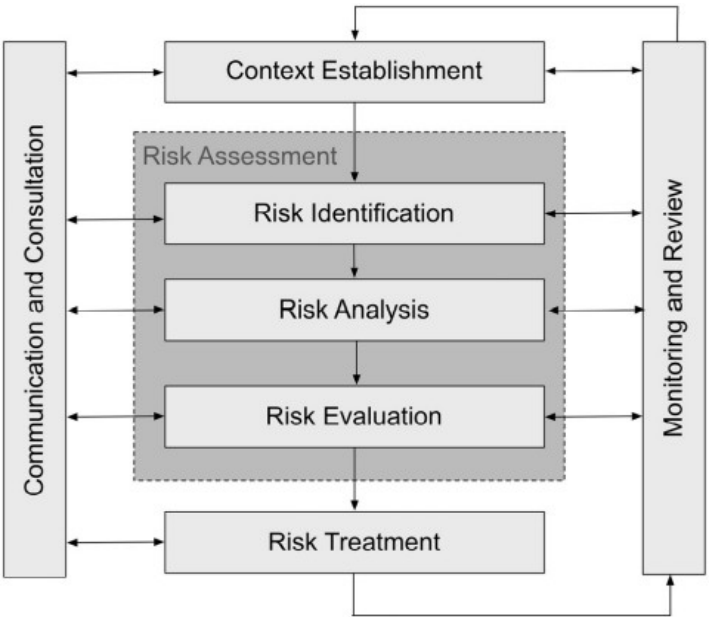

Figure 1. The risk management process

Source: ISO, 2009

A cybersecurity risk assessment helps organizations determine key business objectives and then identify the appropriate IT assets required to realize their objectives. A cybersecurity risk assessment should map out the entire threat environment and how it can impact the organization's business objectives. The result of this assessment should assist security teams and relevant stakeholders in making informed decisions about the implementation of security measures that mitigate these risks.

A range of standards and normative documents related to risk management and risk assessment has been devised over the years for IT systems. The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) is a popular framework (Computer Security Resource Center, no date). The NIST CSF provides a comprehensive set of best practices that standardize risk management and defines a map of activities and outcomes related to the core functions of cybersecurity risk management: protect, detect, identify, respond, and recover. The International Organization for Standardization (ISO) created the ISO/IEC 270001 in partnership with the International Electrotechnical Commission (IEC). The ISO/IEC 270001 cybersecurity framework offers a certifiable set of standards defined to systematically manage risks posed by information systems. Organizations can also use the ISO 31000 standard, which provides guidelines for enterprise risk management. The Department of Defense (DoD) Risk Management Framework (RMF) defines guidelines that DoD agencies use when assessing and managing cybersecurity risks. RMF splits the cyber risk management strategy into six key steps: categorize, select,

implement, assess, authorize, and monitor. The Factor Analysis of Information Risk (FAIR) framework is defined for the purpose of helping enterprises measure, analyse, and understand information risks. The goal is to guide enterprises through the process of making well-informed decisions when creating cybersecurity best practices.

Daily cybersecurity risk management involves many concrete actions which form overall measures in mitigating cybersecurity risks in an organization. Recording cybersecurity incidents in a register can assist with ensuring that appropriate remediation activities are undertaken. When gathering evidence following a cybersecurity incident, it is important that its integrity is maintained. Even though an investigation may not directly lead to a prosecution, it is important that the integrity of evidence, such as manual logs, automatic audit trails, and intrusion detection tool outputs, be protected. Reporting cybersecurity incidents to an organization's information security officer as soon as possible after they occur or are discovered provides senior management with the opportunity to assess the impact on their organization and to take remediation actions if necessary. Cyber supply chain risk management activities should be conducted at the earliest possible stage of procurement processes. In particular, organizations should consider the security risks that may arise as systems, software, and hardware are designed, built, stored, delivered, installed, operated, maintained, and decommissioned. This includes identifying and managing jurisdictional, governance, privacy, and security risks associated with the use of suppliers and service providers.

An important factor is that the organization appoints an individual, for example an information security officer, who is responsible for the risk management process and implements their tasks following those responsibilities. These tasks should be agreed in the internal policies of the organization. In addition, the commitment of management is a key element in the cybersecurity risk management process. If senior management does not demonstrate sufficient attention to the risk management process, the organization may not achieve a successful compliance process. When there is a distance between real and perceived security risk, there is the possibility that the control policy (risk identification, control, monitoring action, compliance) set at the executive management level does not translate in an expected manner to lower-level staff (Barker 2014). The management of cybersecurity risk should be an integrated part of the organization's corporate governance. The implementation of information security governance maybe achieved if: a) the board of directors and executive management place extra attention on information security matters instead of treating them as technological issues that fall under the responsibility of technical managers; b) information security measures are clearly communicated from the top- level management to lower-level staff; c) low-level staff are involved in the formulation of information security policies to avoid setback or policy implementation rejection; and d) all stakeholders are aware of the value added by the implementation of information security governance, which results in higher investment in information security control (Fazlida and Saidb 2015).

2.6. Structured cybersecurity requirements

The potential structure of cybersecurity legal requirements at the national level is a huge challenge. The European Court of Auditors published a report providing an excellent overview of the EU's complicated cybersecurity policy framework. This report identified many challenges to effective policy delivery, such as: the meaningful evaluation and accountability of policy and legislative framework; addressing gaps in EU law and its uneven transposition; aligning investment levels with goals; the need for a clear overview of EU budget spending; adequately resourcing the EU's agencies; and strengthening information security governance and threat and risk assessments (European Court of Auditors 2019).

At the organizational level, the main requirements of cybersecurity are structured in the cybersecurity strategy document. A cybersecurity strategy sets out an organization's guiding

principles, objectives, and priorities for cybersecurity, typically over a three-to-five-year period. In addition, a cybersecurity strategy may also cover an organization's threat environment, cybersecurity initiatives, or investments the organization plans to make as part of its cybersecurity program. The policy owner should be the information security officer, who is responsible for the successful implementation of the cybersecurity requirements. The application of the defence-in-depth principle to the protection of systems and different hardware through the execution of physical security should be described and implemented in the organization.

In addition to the cybersecurity strategy, an organization may approve system-specific security documentation, such as a system security plan, incident response plan, continuous monitoring plan, or security assessment report. As such, it is important that those documents are developed by personnel with good understandings of security matters, the technologies being used, and the business requirements of the organization. For example, having an incident response plan ensures that when a cybersecurity incident occurs, a plan is in place to respond appropriately to the situation. In most situations, the aim of the response will be to prevent the cybersecurity incident from escalating, restore any impacted system or data, and preserve any evidence. A continuous monitoring plan can assist organizations in proactively identifying, prioritizing, and responding to security vulnerabilities.

Following the implementation of the cybersecurity strategy, frequent reports should be drafted by the information security officer and presented to the senior government of the organization. This will assist the organization in performing the minimum necessary control over the actions of the cybersecurity process as well as guiding the development of the future plan of action and milestones.

3. Conclusions

A sound cybersecurity compliance process can be achieved through continuous and complex daily work. The aim of this article was to reveal the main factors which describe a successful cybersecurity compliance process. The implemented research revealed several factors which can contribute towards a successful compliance process in an organization: the commitment of senior management, facilitating a cybersecurity culture, and the continuous implementation of a risk management process.

Senior management should set the guiding direction of a security culture through statements, awareness campaigns, and other concrete actions. In day-to-day business, senior managers should demonstrate the importance of cybersecurity in the organization. Organizations must develop a certain level of cybersecurity culture in order to reduce or minimize the risks incurred by employees. Such a culture should be maintained through certain programs and constant training in order to achieve cybersecurity awareness and secure the involvement of employees. Annually-implemented risk management includes identifying risks, defining preventative implementation measures, mitigating the impact of an attack, and establishing a continuity plan. This approach to cybersecurity needs to be based on risk management. Additional preconditions – such as a dedicated cybersecurity budget, structured and followed-up-on cybersecurity requirements, and the active role of the information security officer – serve as secondary criteria which should additionally support the successful implementation of the cybersecurity compliance process in an organization.

In real-life situations, the main preconditions for the implementation of cybersecurity compliance might also be implemented incorrectly or only partially. For example, cybersecurity policies are often not properly communicated to employees or do not receive sufficient commitment from senior management, and therefore pose the risk of merely formal implementation of cybersecurity requirements in practice.

Acknowledgement

The author is grateful for the European Social Fund measure No 09.3.3-LMT-K-712 'Development of Competences of Scientists, other Researchers and Students through Practical Research Activities' under grant agreement with the Research Council of Lithuania, who funded this article as a part of the research 'The Problematic Matters and Solutions of Formal Compliance in Cybersecurity'.

References

Cambridge Dictionary. 2022. 'Compliance'. Available at: https://dictionary.cambridge.org/dictionary/english/compliance?q=compliance (Accessed: 1 April 2022).

Computer Security Resource Center (n.d). *NIST Risk management framework*. Available at: https://csrc.nist.gov/projects/risk-management/about-rmf (Accessed: 1 April 2022).

Deloitte Insights. 2020. *Reshaping the cybersecurity landscape*. Available at: https://www2.deloitte.com/content/dam/Deloitte/pt/Documents/risk/Cybersecurity.pdf.

Directive (EU) 2016/1148 of the European Parliament and the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. OJ L 194, 19.7.2016, pp. 1–30. Available at: https://eur-lex.europa.eu/eli/dir/2016/1148/oj (Accessed: 1 April 2022).

ENISA. 2017. *ENISA overview of cybersecurity and related terminology* (Version 1). Available at: https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology (Accessed: 1 April 2022)

ENISA. 2018. *Cyber security culture in organisations*. Available at: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations (Accessed: 1 April 2022).

European Commission. 2020. *Joint communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade* (Brussels, 16.12.2020, JOIN(2020) 18 final). Available at: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital- decade-0 (Accessed: 1 April 2022).

European Court of Auditors. 2019. *Challenges to effective EU cybersecurity policy.* Available at: https://www.eca.europa.eu/lists/ecadocuments/brp_cybersecurity/brp_cybersecurity_en.pdf (Accessed: 1 April 2022).

European Union Agency for Cyber Security. 2016. *Cyber insurance: Recent advances, good practices & challenges*. ENISA. DOI: https://doi.org/10.2824/065381.

Fazlida, M.R. and Saidb, J. 2015. "Information security: Risk, governance and implementation setback." *Procedia Economics and Finance* 28: 243–248. DOI: https://doi.org/10.1016/S2212- 5671(15)01106-5.

ISO 31000:2009. Available at: https://bambangkesit.files.wordpress.com/2015/12/iso-31000_principles-guidelines-risk-manajemen.pdf (Accessed: 1 April 2022).

Jalali, M.S., Siegel, M. and Madnick, S. 2019. "Decision making and biases in cybersecurity capability development: Evidence from a simulation game experiment." *The Journal of Strategic Information Systems 28(1):* 66–82. DOI: https://doi.org/10.1016/j.jsis.2018.09.003.

Jeong, J., Mihelcic, J., Oliver, G. and Rudolph, C. 2019. "Towards an improved understanding of human factors in cybersecurity." *IEEE 5th International Conference on Collaboration and Internet Computing (CIC)*, pp. 338–345. DOI: https://doi.org/10.1109/CIC48465.2019.00047.

Karanja, E. 2017. "The role of the chief information security officer in the management of IT security." *Information and Computer Security* 25(3): 300–329. DOI: https://doi.org/10.1108/ICS-02-2016- 0013.

Kosutic, D. and Pini, F. 2022. "Cybersecurity: Investing for competitive outcomes." *Journal of Business Strategy* 43(1): 28–36. DOI: https://doi.org/10.1108/JBS-06-2020-0116.

Marketsandmarkets. 2022. "New Market Reports." Available at https://www.marketsandmarkets.com/new-reports.asp.

McBride, M., Carter, L. and Warkentin, M. 2012. *Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies* (prepared by RTI International – Institute for Homeland Security Solutions under contract 3-312-0212782). Available at: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.453.3551&rep=rep1&type=pdf (Accessed: 1 April 2022).

Monzelo, P. and Nunes, S. 2019. "The role of the chief information security officer (CISO) in Organizations." *CAPSI 2019 Proceedings*, 36. Available at: https://aisel.aisnet.org/capsi2019/36/ (Accessed 1 April 2022)

Nævestad, T.O., Meyer, S.F. and Honerud, J.H. 2018. "Organizational information security culture in critical infrastructure: Developing and testing a scale and its relationships to other measures of information

security." In Haugen, S., Barros, A., van Guijk, C., Kongsvik, T. and Vinnem, J.E. (eds.), *Safety and reliability–Safe societies in a changing world*. London: CRC Press, pp. 3021–3029.

Ogbanufe, O., Kim, D.J. and Jones, M.C. 2021. "Informing cybersecurity strategic commitment through top management perceptions: The role of institutional pressures." *Information & Management* 58(7): 103507. DOI: https://doi.org/10.1016/j.im.2021.103507.

Reegård, K., Blackett, C. and Katta, V. 2019. "The concept of cybersecurity culture." In Beer, M. and Zio, E. (eds.), *Proceedings of the 29th European Safety and Reliability Conference*. Singapore: Research Publishing, pp. 4036–4043. DOI: http://dx.doi.org/10.3850/978-981-11-2724-3_0761-cd

Roch, C.H., Scholz, J.T. and McGraw, K.M. 2000. "Social networks and citizen response to legal change." *American Journal of Political Science* 44(4): 777–791. DOI: https://doi.org/10.2307/2669281.

Santini, F. 2017. "Prioritizing cybersecurity on a limited budget." *Law Practice* 43(5): 59–61.