# White paper
# Literature Review for the ASCD project

Asmita Dalela[1], Saverio Giallorenzo*[2], Oksana Kulyk[1], and Jacopo Mauro[3]

[1]IT University of Copenhagen
[2]Università di Bologna and INRIA
[3]University of Southern Denmark

December 13, 2020

**Abstract**

The Assessment on the Status of CyberSecurity in Denmark (ASCD) is a research project conducted by the IT University of Copenhagen and the University of Southern Denmark and funded by the Danish Centre for CyberSecurity. The project aims to study and report on the existing cybersecurity and privacy protection practices used in large Danish companies and SMEs, identifying the most important challenges the developers in Denmark face in developing secure and privacy-preserving solutions, and providing guidelines for securing critical infrastructures. This white paper is a report on our work surveying peer-reviewed and non-peer-reviewed literature on human and organisational factors of cybersecurity and privacy, as part of the preparation of the survey developed for the ASCD project.

## 1 Introduction

The Assessment on the Status of CyberSecurity in Denmark[1] (ASCD) is a research project conducted by the IT University of Copenhagen and the University of Southern Denmark and funded by the Danish Centre for CyberSecurity.

The project aims to study and report on the existing cybersecurity and privacy protection practices used in large Danish companies and SMEs, identifying the most important challenges the developers in Denmark face in developing secure and privacy-preserving solutions, and providing guidelines for securing critical infrastructures.

*Work performed while the author was employed at the University of Southern Denmark.
[1]http://ascd.dk

This white paper is a report on our preliminary work surveying peer-reviewed and non-peer-reviewed literature on cyber-security, as part of the preparation of the survey developed for the ASCD project.

## 2 Peer-reviewed Literature Review

To locate the peer-reviewed publications we followed a two-step approach. First, we searched peer-reviewed works regarding cyber-security at both the technological and organisational levels. Specific technical papers (e.g., presenting a specific technical solutions to a specific problem) were not considered to avoid overfitting on a narrow thematic.The search query used for the research was the keyword `Security` in conjunction with the disjunction of the keywords: `Survey`, `SMEs`, `Small Enterprises`, `Medium Enterprises`, `Standards`, `Governance`, and `Management`.

Given the multidisciplinary of our research (which spans from IT-level technical decisions to managerial/economic and legislative ones), we used Google Scholar, which allowed us to extend our queries over the different disciplines, without having to select specific publishers for each specific field, which would have both hampered our research and limited our scope. Since the indexing performed by Google Scholar does not exclusively include peer-reviewed material, we discarded entries correspondent to our research query but not published in either peer-reviewed conferences, journals or magazines. After having collected a first set of papers, we applied a forward and backward snowballing process, looking for the papers that either cite the papers that we included in the first phase or those papers that cite the papers included in the first phase.

In what follows, we briefly present the main content of the selected papers and report how they helped us shaping our survey.

Garfinkel (2012) writes that "cyber-security can be viewed solely as an insider problem", reporting that there is a need for systems that prevent authorised users from acting improperly. Recently, there has been an effort to frame cyber-security as an economic problem in convincing companies to spend resources on defence and training consistent with the risk they face. Technical factors that comprise the cyber-security problem dominate the discussion among both technologists and policymakers. These factors include language and operating system choices, security architectures, usability, and training. Unfortunately, many of the techniques and technologies for developing secure systems that have been shown to reduce security-critical defects have not been widely adopted.

Nontechnical factors impacting cyber-security reflect deep political, social, and economic divisions within the society. These problems include shortened development cycles; the inability to attract and retain the best workers; and the general failure of the schools at early science, technology, engineering, and math (STEM) education. The author, drawing a parallel particularly apt during this COVID-19 period, reports how "just as hand washing and coughing on our sleeves can help halt the spread of influenza, advocates say, good 'cyber hygiene'

such as running up-to-date anti-virus software and only going to clean Web sites run by reputable organisations can help stop the spread of malware and the growth of malicious botnets."

Among the problems regarding cyber-security cited in (Garfinkel, 2012) we find:

- chief security officers that deploy technology are sometimes criticised for wasting money when new systems are purchased and no attack materialises;
- because today's cyber-infrastructure was designed without attention to security, the proper solution is redesign. At the same time, obsolete, bug-ridden vulnerable systems never seem to get retired;
- difficulty attracting and retaining enough software engineers;
- most computer professionals receive little if any training in security,most CS professors and software engineers try to ignore it, and there are few security specialists;
- most graduates simply lack the experience to write security-critical software because they did not start programming in middle school.

The paper is a good introduction to the latest issues and trends on cyber-security and helped define some initial thematics for our survey.

Banham (2017) conducts a study to assess how "small businesses are a prime target of cyber-criminals" and how "hackers know that smaller organisations don't have the wherewithal to develop a defensive security strategy. But the companies themselves tend to erroneously believe that the bad guys only target big companies.", with hackers realising that they can get into a large business through a small one. From their study, the authors also note how it is considered overly expensive by many small-and-medium-sized (SMBs) businesses to implement a program that prevents, detects, mitigates, and helps a business recover from cyber-incidents. Aside from the expense, many small businesses believe there are scant risks of something bad happening if they skirt the rules. This may explain why many large enterprises that conduct business with smaller companies are now requiring them to provide evidence of their cyber-security practices. The authors report that most prevalent cyber-attacks against SMBs they found were web-based and phishing/social engineering scams, with nearly 6 in 10 respondents to the study saying that they did not have knowledge on what password practices their employee adopted, indicating the possibility of weak password protections.

Ponsard et al. (2019) report about their own experience with a cyber-security awareness program targeting Belgian SMEs, citing also a similar study in the UK which reported than more than 60% of SMEs where attacked in 2017, especially from ransomware, with more than half of the hacked one not being able to recover and going bankrupt within six months after the attack. The

main reported barrier from the study on the Belgian SMEs, is the cost for implementing cyber-security solutions and standards because they are designed for bigger companies. It also revealed that theft of customer data and reputation damage are the most feared consequences of cyber-attacks. The bottom line of the study is that most SMEs seem to have a good and even increasing level of awareness. However, when looking at attack statistics, they still fail to make it effective. A first explanation is that security measures are perceived as too complex, time-consuming, and requiring a high level of technical knowledge regarding IT systems. Another reason is the difficulty to transition from a step of initial awareness to the emergence of an internal cyber-security culture, because of the lack of resources (money, time, expertise). SMEs are also weak at deploying policies and defining responsibilities. As part of the study to rise awareness of SMEs for cyber-security, the authors analyse the following set of instruments: awareness campaigns, general information and guides (also checklists), personae (personae are archetypal descriptions of users that embody their goals, and related to cyber-security, personae can be useful for associating specific threats, vulnerabilities or risks in their environment), quizzes (A quiz is a game or light form of assessment used in education and awareness.), and assessments and audits (structured forms of evaluation). We draw inspiration from this paper when laying out the questions of our survey on the perception of the surveyees about security measures, their importance, and the trade-offs associated with them.

Osborn (2015) performs a survey on SMEs in the UK, to establish what barriers they might face in terms of cyber-security, with a total of 33 responders. The survey uses a questionnaire to collect a coherent set of results, while working within the time constraints faced by SME directors. Participants were given additional contact details, to allow those who had more time and wished to continue interacting with the researcher the chance to express their interest. Highlights from the results are that:

- there is a lack of focus from the cyber-security industry on the types of measures SMEs think they need within an SME budget—"simple effective measures that are not too time-consuming and require a great in-depth knowledge of IT systems";
- there is a lack of well-evolved incentives encouraging SMEs to interact with cyber-initiatives. This leaves SMEs attempting to handle to problem alone, while other stakeholders become increasingly concerned about the wider implications of their lack of cyber-security;
- it is difficult to engage with SMEs in the cyber-security dialogue, mainly due to the lack of resources;
- respondents show a need for unbiased advice. SME owners are not the typical employee in need of awareness training, so further consultation on developing the content of SME-specific awareness programs is required. SMEs may, for example, require more information about vulnerabilities than tool implementation, to facilitate their capacity to self-assess risks;

- a means of providing accessible and accurate threat intelligence to SMEs, and potentially a selection of reviewed security tools suitable for their needs;
- there are two different cyber-security business models accessed by SMEs. The corporate cyber-security marketplace tends to be product-centric, providing a security layer for existing infrastructures. The home cyber-security market is user-centric, a configuration is simplified and cyber-products are offered as part of larger purchases, or as software for evaluation. The respondents are indicating that there is a market for more cyber-security in SMEs, should some of the barriers they face be handled. An expansion of the user-centric business model beyond the endpoint may provide the best opportunity to bridge the gap between current home and corporate security offerings;
- the standardisation of a portion of the cyber-measures employed in cloud computing services, and an improvement in the quality of information about the security offered as part of cloud service provision, so that there are less barriers for SMEs wanting to use these services.

Cardoso et al. (2017) present a survey on Portuguese organisations to map their cyber-security culture and corresponding processes. The survey was conducted on a set of medium-sized and large companies (59 respondents in total) The analysis suggests that in the Portuguese organisations the top management is knowledgeable about some of the topics covered and is aware of some risks in the information security field. However, for some organisations top management, these risks still do not justify the adoption of specific measures such as the hiring of some specialised personnel or the creation of specific infrastructures within the institutions which can be entirely dedicated to the information security subject. The study also revealed that some Portuguese companies, by their lack of adaptation and strategy towards information security, may incur in future risks due to a cultural resistance towards the adoption of new measures and infrastructures. This work helped us shed some light on the dialogues on cyber-security within companies and to orient our questions to extract the relevant information on those processes.

Anwar et al. (2017) conduct a cross-sectional survey study among employees of diverse organisations to explore to what extent gender plays a role in mediating the factors that affect cyber-security beliefs and behaviours of employees, showing that gender has some effect in security self-efficacy, prior experience and computer skills and little effect in cues-to-action and self-reported cyber-security behaviours. The study draws an interesting framework to better understand the specific attitudes of workers with respect to cyber-security, however we chose not to include questions on this matter, as considered too specific for the purpose of our survey.

Evans et al. (2016) research cyber-security assurance processes, i.e., on the impact of the human element on cyber-security assurance, with the objective to identify elements of cyber-security that would benefit from further research

and development based on the literature review findings. Interestingly, 50% of the worst breaches mentioned in the related references of the paper were caused by inadvertent human error, rising from 31% the previous year. Therefore, the authors conduct half of significant security incidents as due to a particular element, which has not been changed since the inception of information security management, which is people and their unintentional mistakes and errors. The authors also report that there a lack of consistency and clarity regarding cyber-security standards, leading to few applications of cyber-security assurance to be comparable, advocating for the industry to reach a more prescriptive hierarchy of standards. In their research, they find that ISO/IEC 27001 remains the leading general standard for security management. From the point of view of insider threat, the authors report how companies are more concerned by inadvertent insider threat data leak breaches than malicious data breaches. Regardless of the motivation of an insider, be it a deliberate act of theft or designed to embarrass an organisation, or if the breach was inadvertent due to a lack of internal controls, the threat from "insiders" is a real for companies.

The study also found that people were willing to undertake risky practices. Individuals were actually rewarded as they were seen as helpful for allowing an event to take place without applying security controls or practice. The study gave us a number of pointers for our questions on cyber-security frameworks and on the "soft" side of cyber-security regarding people's perceptions and attitudes.

Hadlington (2017) presents a study that explores the relationship between risky cyber-security behaviours, attitudes towards cyber-security in a business environment, Internet addiction, and impulsivity. 538 participants in part-time or full-time employment in the UK completed an online questionnaire, with responses from 515 being used in the data analysis. The survey included an attitude towards cyber-crime and cyber-security in business scale, a measure of impulsivity, Internet addiction and a "risky" cyber-security behaviours scale. The results demonstrated that Internet addiction was a significant predictor for risky cyber-security behaviours. A positive attitude towards cyber-security in business was negatively related to risky cyber-security behaviours. Finally, the measure of impulsiveness revealed that both attentional and motor impulsivity were both significant positive predictors of risky cyber-security behaviours, with non-planning being a significant negative predictor. The results present a further step in understanding the individual differences that may govern good cyber-security practices, highlighting the need to focus directly on more effective training and awareness mechanisms. Similarly to (Evans et al., 2016), this study gave us good starting points to address the side of cyber-security regarding people's perceptions and attitudes.

Nelson and Madnick (2017) introduce a framework for evaluating the trade-off between the reliance of a company on digital technologies and cyber-security risks. Through a mixed-method approach (a survey and interviews), the authors position companies in different quadrants on an innovation/cyber-security matrix overlaid with the negative impact of cyber-security controls on the innovative projects. According to their findings, only 13% of companies believe that they have found the right balance between the two priorities. It is also clear that

some companies take on too much risk, often without fully realising it, while others may not be taking full advantage of the available technology, missing innovation opportunities. Nelson and Madnick (2017) highlight how cyber-security posture and management are primarily related to the regulatory environment, innovation pressures and the publicity of cyber-breaches. Since these factors are primarily external, they need to be well understood and incorporated into the overall company's cyber-security posture and related strategy. Company factors and technology management practices are those over which companies have most control. From the study, those factors have the highest numbers of issues, specifically: operating model and organisation structure; company culture and tensions created by cyber-security efforts; board of directors and their role in cyber-security and innovation trade-off decisions; education, communication, and organisational awareness; Legacy architectures; IT governance and resource allocation. Maturity of technologies considered for various innovation projects also plays a significant role in the amount of cyber-risk and how it gets addressed. Those companies that take security seriously and address it at the industry, company and technology levels, will be well-positioned to not only protect the existing value of their company, but create new value as cyber-security gets built into all new innovative technologies at the foundational levels. This work inspired questions in the survey regarding the perceived gains and losses of adopting and implementing cyber-security measures in organisations.

Jang-Jaccard and Nepal (2014) present an overview of the most exploited vulnerabilities in existing hardware, software, and network layers of IT systems. That includes the main cyber-security concerns and an analysis of the understanding of surrounding issues of diverse cyber-attacks and a comment on the defence strategies (i.e., countermeasures) that preserve confidentiality, integrity and availability of any digital and information technologies. Finally, the authors discuss new attack patterns in emerging technologies such as social media, cloud computing, smartphone technology, and critical infrastructure. The study inspired our questions on attack vectors and the list of possible mitigations employed by the surveyed organisations.

Habibzadeh et al. (2019) looks at deployments of cyber-physical systems in smart cities (as more and more systems embrace IT automation, like healthcare, transportation services, and utilities) and the increased vulnerability and risk of their digital transformation. They survey the theoretical and practical challenges and opportunities of the digital transformation and they enumerate them in a systematic way both in terms of their technical aspects and of the related policy and governance issues. We draw inspiration from this study when surveying on the challenges of the digital transformation in the surveyed organisations.

Mouheb et al. (2019) consider the educational aspect of cyber-security (and the relative lack of professionals that received education on that). They present an overview and comparison of existing curriculum design approaches for cyber-security education, to help researchers and educators have an overview of the existing approaches and to help them develop comprehensive cyber-security curricula. The study helped us collect the main subjects of knowledge on cyber-

security and shape our profiling questions in the survey.

Rees et al. (2011) present a decision-support system to estimate the risks faced by an organisation under cyber-attack, as a function of uncertain threat rates, countermeasure costs, and impacts on its assets. The paper helped us define the elements considered (or that organisations should consider) when defining their risk of cyber-attacks and the related countermeasures (and their trade-offs).

Li et al. (2019) provide a theoretical model to capture and reason on employees' security behaviour, which is then tested with a survey on 579 business managers and professionals. From their results, the authors highlight that, when employees are aware of their company's information security policy and procedures, they are more competent to manage cyber-security tasks than those who are not aware of their companies' cyber-security policies. The study also indicates that an organisational information security environment positively influences employees' threat appraisal and coping appraisal abilities, which in turn, positively contribute to their cyber-security compliance behaviour. The paper informed our decision to include questions on the level of integration of surveyees in the diffusion and knowledge on the company's cyber-security policies and on the decision processes behind them.

Bhatia et al. (2016) examine the trade-off between the need for potentially sensitive data and the perceived privacy risk of sharing that data (across government agencies and companies and within and across industrial sectors). They divide their study into two parts: a data-usage estimate built from a survey of 76 security professionals and a privacy-risk estimate that measures privacy risk using, factoring in data purposes with different levels of societal benefit (e.g., terrorism, imminent threat of death, economic harm, and loss of intellectual property). Their results show which data types are high-usage, low-risk versus those that are low-usage, high-risk. The results of this paper inspired us to consider questions on the relationship between the surveyed organisations and the government and the perceived risks of sharing security-critical data.

Craig et al. (2015) characterise the (existing) concept of "proactive security" and analyse the proactive cyber-security movement through a breakdown of industry practices and comparative regulations. The term is actually an umbrella-terminology that ranges from "hack-back" retaliation strategies, to technological best practices (itself extending from real-time analytics to cyber-security audits), measures for detecting or obtaining information on possible cyber-attack, impending cyber-operations, or determining the origin of an operation that involves launching a pre-emptive, preventive, or counter-operation against the source. Besides the technical aspects, the authors also look at the legal environment within which those proactive cyber-security programs have been operating, investigating the potential emergence of a proactive cyber-security norm in international law along with the implications of this movement for contemporary Internet governance debates. The cited study mainly inspired the enumeration of cyber-threats and solutions employed by the surveyed organisations in our questionnaire.

Finally, Ricci et al. (2019) present a survey (taken by 233 participants) to

analyse the interest of adults for "cyber-threat education seminars", e.g., how to protect themselves and their loved ones from cyber-threats. Specifically, they asked questions to identify a possible audience as well as their willingness for paying/time commitment, fields of interest, and background. From their results, the authors report that the majority of surveyees are worried about cyber-security threats, however they did not seem keen on getting an educating through seminars as a priority and, in case they did, they would have spent a relatively limited amount of time (1-1.5 hour on seminars). The study helped define the available solutions presented to individuals to become more knowledgeable on cyber-security and their willingness to endeavour in such activities.

# References


M. Anwar, W. He, I. Ash, X. Yuan, L. Li, and L. Xu. Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69:437–443, 2017.

R. Banham. Cybersecurity threats proliferating for midsize and smaller businesses. *Journal of Accountancy*, 224(1):75, 2017.

J. Bhatia, T. D. Breaux, L. Friedberg, H. Hibshi, and D. Smullen. Privacy risk in cybersecurity data sharing. In *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, pages 57–64, 2016.

M. G. Cardoso, R. D. Laureano, and C. Serrão. Cybersecurity culture in portuguese organizations: an exploratory analysis. In *2017 12th Iberian Conference on Information Systems and Technologies (CISTI)*, pages 1–5. IEEE, 2017.

A. N. Craig, S. J. Shackelford, and J. S. Hiller. Proactive cybersecurity: A comparative industry and regulatory analysis. *American Business Law Journal*, 52(4):721–787, 2015.

M. Evans, L. A. Maglaras, Y. He, and H. Janicke. Human behaviour as an aspect of cybersecurity assurance. *Security and Communication Networks*, 9 (17):4667–4679, 2016.

S. L. Garfinkel. The cybersecurity risk. *Communications of the ACM*, 55(6): 29–32, 2012.

H. Habibzadeh, B. H. Nussbaum, F. Anjomshoa, B. Kantarci, and T. Soyata. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society*, 50:101660, 2019.

L. Hadlington. Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7):e00346, 2017.

J. Jang-Jaccard and S. Nepal. A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*, 80(5):973–993, 2014.

L. Li, W. He, L. Xu, I. Ash, M. Anwar, and X. Yuan. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45:13–24, 2019.

D. Mouheb, S. Abbas, and M. Merabti. Cybersecurity curriculum design: A survey. In *Transactions on Edutainment XV*, pages 93–107. Springer, 2019.

N. Nelson and S. Madnick. Studying the tension between digital innovation and cybersecurity. Association for Information Systems, 2017.

E. Osborn. Business versus technology: Sources of the perceived lack of cyber security in smes. 2015.

C. Ponsard, J. Grandclaudon, and S. Bal. Survey and lessons learned on raising sme awareness about cybersecurity. In *ICISSP*, pages 558–563, 2019.

L. P. Rees, J. K. Deane, T. R. Rakes, and W. H. Baker. Decision support for cybersecurity risk planning. *Decision Support Systems*, 51(3):493–505, 2011.

J. Ricci, F. Breitinger, and I. Baggili. Survey results on adults and cybersecurity education. *Education and Information Technologies*, 24(1):231–249, 2019.