CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD

White Paper

Cybersecurity Investment Decision-Making

A Best Practice Guide for SMEs

Version 1.1

RISCS Research Institute for Sociotechnical Cyber Security

National Cyber Security Centre

Introduction

There are 6 million Small and Medium-Sized Enterprises (SMEs) in the UK, and they constitute 99% of all businesses.[1] Every day SMEs face hard cybersecurity investment decisions. In 2020, 46% of businesses reported having cybersecurity breaches in the last 12 months. SMEs are considered a softer target by cyber criminals and an easy back door into large businesses as supply chain attacks show. While more than 80% of businesses consider investment in cybersecurity a high priority[2], there are no well-established practices that SMEs may follow to ensure the robustness of cybersecurity investment decision-making.

The existing literature focusing on cybersecurity decision-making in SMEs is scarce. To address this gap, we conducted an exploratory study and interviewed UK-based SMEs to gain a deeper insight into how SMEs, given their limited resources, make cybersecurity investment decisions and how the decision-making process is supported.

We applied rigorous academic analysis to practical knowledge distilled from SMEs and, based on the analysis, we produced a set of practice-inspired and industry-validated recommendations for SMEs on cybersecurity investment decision-making. The Best Practice Guide summarises our recommendations for SMEs and will assist them with making well-informed decisions.

1 https://commonslibrary.parliament.uk/research-briefings/sn06152/

2 https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020

Research Methodology

- ✓ We examined over 150 non-academic publications on cybersecurity economics to better understand decision-making in practice and formulate interview questions.
- ✓ We conducted 15 in-depth interviews with senior executives and IT experts from UK-based SMEs to gain an empirical insight into how SMEs make decisions about cybersecurity investments.
- ✓ We analysed the collected data, distilled common issues and formulated the best practice recommendations.
- ✓ We organised a focus group and gathered feedback from 12 SME representatives to validate the recommendations.

Recommendations

1. Cybersecurity as a Business Enabler and a Competitive Advantage

Executives of SMEs should perceive cybersecurity as a business enabler and a competitive advantage.

Digital transformation can open new business opportunities, enable more optimal ways of working, and make an SME more agile and scalable. Any digital transformation should be undertaken with cybersecurity in mind. Many of the new ways of working are only possible due to cybersecurity. For example, online banking, digital tax records and returns, remote working and online communication with customers are only possible due to encrypted connections and secure data storage.

Cybersecurity could not only prevent losses and act as an insurance but could also offer strategic business growth opportunities and make a business more competitive in the market. The ability to demonstrate a good practice standard and strong culture of cybersecurity will enable SMEs to offer new services, win more tenders (including tenders to local and central government in the UK), and attract a greater number of customers who become ever more aware of the importance of protecting their information. A good cybersecurity posture and a high level of cybersecurity resilience demonstrated by an SME will lead to a higher level of trust from customers providing an advantage over competitors. To offer a competitive advantage, cybersecurity should be taken seriously and be deeply integrated into organisational culture, and not merely be a box-ticking exercise.

The change of attitude towards cybersecurity at the senior executive level of an SME will lead to behavioural change across an entire business. When cybersecurity is treated as a strategic business priority at the most senior level, then the attitude and cybersecurity behaviour of all employees will gradually change as well.

2. Cybersecurity Education for Executives

(Supports Recommendation 1)

Executives should educate themselves in cybersecurity. To be able to make well-informed decisions about cybersecurity investments, executives should understand the key concepts and fundamental principles of cybersecurity, as well as be aware of the modern cyberthreat landscape. Attending an online awareness-level training on cybersecurity tailored for senior executives and delivered by a trusted provider may be a suitable option for people with a busy schedule. NCSC provides a list of certified cybersecurity training, including cybersecurity training options for executives[3]. The knowledge of cybersecurity will empower executives not only to make better-informed decisions, but also to drive the cybersecurity culture change within their business more efficiently.

3 https://www.ncsc.gov.uk/information/certified-training

Recommendations

3. Cybersecurity Ambassador

(Supports Recommendations 1 and is linked with Recommendation 2)

An SME should appoint a person responsible for cybersecurity who will report to senior executives on a regular basis. A cybersecurity ambassador should promote a view of cybersecurity as a business enabler and aspire to communicate the strategic business importance of cybersecurity to executives, presenting information in a way that is easily-accessible and more compelling for a non-technical audience.

Who within a business takes responsibility for cybersecurity depends on the specifics of an SME. Typically, SMEs do not have a person responsible for cybersecurity, and traditionally cybersecurity becomes an additional duty of IT staff. Senior experienced IT staff usually have a good understanding of cybersecurity as well as respect and trust from senior executives. In many SMEs, senior IT staff are well positioned to embrace the role of a cybersecurity ambassador within their SMEs. However, the pitfall which should be avoided when appointing IT staff as a cybersecurity ambassador is that cybersecurity remains being seen as a purely technical rather than strategic business issue.

Ultimately, SMEs should aim to have an executive member of staff responsible for cybersecurity, thereby ensuring that cybersecurity risk is owned at the governance and management levels. This makes improving cybersecurity education and awareness of executive staff (Recommendation 2) a prerequisite for this recommendation.

4. Risk-based Approach to Cybersecurity

(Supports Recommendation 1)

An SME should adopt a risk-based approach to cybersecurity. It is beneficial for SMEs to identify, assess and manage cybersecurity risks in a consistent manner because it leads to a better organised and planned approach to cybersecurity. Following a well-known and tested risk assessment and management methodology should be preferred. However, using a proprietary ad hoc approach is better than using none.

SMEs could choose or develop a simple practical risk assessment technique to suite their specifics. The NCSC guidance on risk management [4] is a good starting point for SMEs interested in adopting or improving their risk-based approach to tackling cybersecurity risks.

4 https://www.ncsc.gov.uk/collection/risk-management-collection

Recommendations

5. Understand Full Costs of a Cybersecurity Breach

(Supports Recommendations 3 and 4)

Our study shows that SMEs focus on only a few costs associated with a potential or past cybersecurity breach, e.g. staff time on addressing the consequences and revenue loss due to downtime. However, to gain a better understanding of cybersecurity risks and make well-informed decisions, **SMEs should consider all contributing costs arising from a cybersecurity breach**. The recent report commissioned by the Department for Digital, Culture, Media and Sport (DCMS) *"Analysis of the full costs of cyber security breaches"* [5] provides a comprehensive list of 41 costs that might be associated with a security breach, and a free tool that supports documentation and an estimation of the costs.

5 https://www.gov.uk/government/publications/cyber-security-incentives-regulation-review-government-response-to-the-call-for-evidence

6. Important Factors to Consider

An SME should consider the following factors to make well-informed decisions about cybersecurity investments:

- (Perceived) Risk reduction offered by a new cybersecurity solution,
- Customer expectations and requirements,
- Compliance and regulatory requirements,
- Cost of a solution,
- Cybersecurity best practices,
- Competitive advantage a solution may lead to,
- Ease of implementation and maintenance,
- Compatibility and integration with already owned IT and security products,
- Trust in a security vendor/consultant (brand awareness),
- Reputation of a security solution,
- Staff familiarity with a security solution,
- Available technical support and its accessibility,
- Indirect benefits a solution may offer (e.g. reduction of insurance premium or fewer audits)

Recommendations

7. Identify a Set of Cybersecurity Metrics that Fits Your Needs

An SME should identify a combination of cybersecurity metrics for supporting decision-making and develop a narrative behind it tailored for their specific needs. Executives and IT staff should work collaboratively to develop a set of cybersecurity metrics that is practical and mutually-accessible and useful for them.

Our study shows that there is no one single cybersecurity metric that works for all SMEs, and that a combination of metrics should be used. Often, SMEs lack knowledge on what cybersecurity metrics (quantitative indicators) are available and appropriate for supporting cybersecurity investment decision-making. Below we present a list of cybersecurity metrics that the participants of our study found useful, and which could be considered by other SMEs:

- Percentage of (non-executive and executive) employees completing security awareness training (supported by cybersecurity knowledge and competency tests),
- Number of discovered vulnerabilities,
- Total number of attacks over a given period,
- Number of prevented cyber-attacks,
- Percentage of prevented cyber-attacks (% of total),
- Likelihood of cyber-attacks (categorised by type, by sector, by business size),
- Cost of a (prevented) security breach,
- Mean time to breach (also referred to as mean time to compromise),
- Return on security investments (more suitable for hardware solutions),
- Percentage of data that can be restored after a cyber-attack,
- Percentage of CPU load or latency due to a security product.

In addition to the above, the following time-based metrics could be considered by SMEs in decision-making process:

- Staff time on implementing a security countermeasure (as a measure of cost)
- Downtime due to a cyberattack (as a measure of loss)
- Staff time on mitigating the consequences of a cyberattack (as a measure of loss)
- Reduction of downtime (as a measure of solution effectiveness)
- Staff time saved due to new ways of working enabled by a solution (as a contributing measure of benefit)

Recommendations

8. Cybersecurity "Driving License"

One should not drive a car without a driving licence! A similar idea should apply to businesses operating in a digital space: **any SME with a digital footprint should have a cybersecurity "driving licence" - an evidence that the business has a good practice standard in cybersecurity.**

While to date having a cybersecurity "driving licence" is not mandatory in general, SMEs will undoubtedly benefit from working towards and obtaining it voluntarily. A cybersecurity certification is a valuable marketing asset for SMEs which reassures cybersecurity-aware customers.

It is up to an SME to choose a cybersecurity certification which can act as their cybersecurity "driving licence". Cyber Essentials[6] is a popular government-endorsed scheme, which enables organisations to be certified independently for having met a good practice standard in the technical aspect of cybersecurity. For SMEs who are fully committed to cybersecurity, achieving ISO27001 certification will demonstrate to their corporate clients and customers that cybersecurity is integrated into the management culture and is addressed comprehensively with the business.

6 https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

9. Customer Requirements Drive Strengthening of Cybersecurity

The study shows that SMEs react positively and rapidly to the cybersecurity requirements of existing and prospective customers. Customer requirements play an important constructive role in the improvement of the security posture of SMEs already, but there is a room for improvement. If more individual and corporate customers become aware of cybersecurity risks and demand a good-practice standard in cybersecurity as a contractual requirement, this will lead to the gradual strengthening of cybersecurity nationally.

An SME as a customer should require their contractors to adhere to best cybersecurity practices and evidence it by a cybersecurity certification appropriate to each supply chain. This will, over time, result in the improvement of the cybersecurity posture of an entire supply chain.

Call for Contributions

This Best Practice Guide is a living document. We plan to update it when new relevant findings emerge. We would like to invite all individuals that are well-positioned to reflect on cybersecurity investment decision-making practices in SMEs to contribute their opinion to the next version of the Guide. We would like to hear from SMEs about any aspect of the cybersecurity investment decision-making process, including influencing factors, metrics and tools used for supporting the process.

Please contact Dr Yulia Cherdantseva if you would like to contribute your opinion to the next version of the Guide.

Funding

This project was funded by the Research Institute for Sociotechnical Cyber Security and the UK National Cyber Security Centre.

RISCS

National Cyber Security Centre

Academic Team

Dr Yulia Cherdantseva (Principal Investigator)

School of Computer Science and Informatics, Cardiff University

cherdantsevayv@cardiff.ac.uk

Dr Izidin El Kalak (Co-Investigator)

Cardiff Business School, Cardiff University

ElKalakI@cardiff.ac.uk

Harry Batchelor (Project Coordinator)

School of Computer Science and Informatics, Cardiff University

BatchelorH@cardiff.ac.uk

Centre for Cyber Security Research

Canolfan Ymchwil Seiberddiogelwch

Prifysgol Caerdydd

Cardiff University is the home of the Cardiff Centre for Cyber Security Research which unites interdisciplinary research expertise and education across the University. The Centre is recognised by the NCSC in partnership with the Engineering and Physical Sciences Research Council (EPSRC) as an Academic Centre of Excellence in Cyber Security Research (ACE-CSR). This study was conducted by the members of the Cardiff Centre for Cyber Security Research Dr Y. Cherdantseva and Dr I. El Kalak.