Evaluating the Attention-Based View in Risk Management and Proposing the New "Top-Down" Continuous and Proactive Security Assessment Model (CAPSAM)

UNIVERSITY OF
LINCOLN

Alfie Atkinson
25715017

25715017@students.lincoln.ac.uk

School of Computer Science

College of Science

University of Lincoln

Submitted in partial fulfilment of the requirements for the
Degree of Master of Science in Computer Science

Module Co-Ordinator	Dr. Saeid Pourroostaei Ardakani
Second Module Co-Ordinator	Dr. Abimbola Sangodoyin

January 2025

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background on Cybersecurity Risks

Cybersecurity is a rapidly growing field focused on safeguarding digital devices, networks, and information from unauthorised access and preventing data theft or alteration (Mijwil et al., 2023). It employs a range of techniques, processes, and practices to protect sensitive information and deter cyber attacks. Tactics for protecting against cyber attacks include firewalls, encryption, secure passwords, and threat detection and response systems, and employees should be trained on these strategies.

Cybersecurity risk is determined by the combination of vulnerabilities, threats, and the potential impact of cyber-attacks. Vulnerabilities are the weaknesses present in the system, and threats are the possibilities of cyber-attacks that exploit these vulnerabilities (Prasad et al., 2020). The Internet and the Internet of Things (IoT) are significant sources of threats, while phishing attacks are becoming increasingly sophisticated, and passwords alone are no longer sufficient for ensuring security. Raising awareness about cybersecurity risks is imperative for effectively handling digital environments and safeguarding them against electronic threats (Mijwil et al., 2023).

1.2 The Role of Information Security Risk Assessments (ISRAs)

Information Security Risk Assessments (ISRAs) are a key tool for identifying and managing vulnerabilities. ISRAs help organisations to identify their security risks and provide a measured analysis of their critical information assets, which informs the development of plans to mitigate these risks (Shedden, Smith and Ahmad, 2010). These assessments are essential for protecting IT assets and form the basis for a secure information system. Shedden, Smith and Ahmad (2010) also say ISRAs enable organisations to prioritise their security efforts, focusing on the most important assets and vulnerabilities as well as helping organisations determine the most cost-effective way to reduce risks.

1.3 Top Management Team (TMT) Involvement

The Top Management Team (TMT) involvement is vital for effective risk management as they are ultimately responsible for ensuring that due diligence is undertaken in identifying risk and implementing effective systems of controls (Fazlida and Said, 2015). TMT engagement can ensure that cybersecurity is viewed as an integral part of the organisation rather than a technical issue handled solely by IT. This involvement ensures a holistic approach to security, with the TMT championing risk assessment exercises and ensuring that cybersecurity receives the necessary resources and attention (Shaikh and Siponen, 2023). Fazlida and Said (2015) also state that TMT attention to security is important to ensure that risk is reduced and the organisation meets its legal obligations.

1.4 Purpose of the Report

This report evaluates the use of the Attention-Based View (ABV) Theory by Shaikh and Siponen (2023), exploring its strengths and limitations. The report will then introduce a new Continuous and Proactive Security Assessment Model (CAPSAM) as a solution. This model addresses the need for a proactive approach to cybersecurity, in contrast to the reactive focus of the ABV. The aim of this report is to critically appraise the ABV, revealing its shortcomings in proactive security planning, and then present CAPSAM as a proactive alternative.

Chapter 2

Case Study Paper – Appraisal of Theoretical Model and Hypothesis

2.1 Summary of the Case Study

In the case study, Shaikh and Siponen (2023) ask: **How do cybersecurity breach costs and Top Management Team (TMT) attention to cybersecurity influence a firm's decision to carry out an Information Security Risk Assessment (ISRA)?**. The research found that higher breach costs result in greater TMT attention to cybersecurity. Additionally, they find that TMT attention to cybersecurity partially mediates the relationship between breach costs and the decision to conduct an ISRA. Further elaborating that while an ISRA might sometimes be initiated by the cybersecurity function independently, the TMT plays a significant role in the decision, especially after high-cost breaches.

2.2 Explanation of the Attention-Based View (ABV) Theory

The case study uses the attention-based view (ABV) to explain how TMT attention is directed toward cybersecurity issues. The ABV theory suggests that **firm behaviour is shaped by how decision-makers allocate their attention**. This theory is built on the idea that human rationality is limited, and decision-makers must focus on specific issues to make effective choices. The ABV is composed of three key principles: focus of attention, structural distribution of attention, and situated attention.

2.2.1 Focus of Attention

The principle of the focus of attention explains that due to limited attention capacity, individuals prioritise issues based on their perceived importance and relevance within a given context. **Senior managers must be selective about which issues they focus on** because they cannot effectively attend to everything. Negative events such as high-cost

cybersecurity breaches become salient, thus requiring TMT attention. This focus then dictates the actions decision-makers take.

2.2.2 Structural Distribution of Attention

The principle of structural distribution of attention posits that **an individual's position within an organisation's hierarchy influences what they pay attention to**. TMTs have a fiduciary duty to stakeholders to oversee and assess firm performance and must protect the firm's reputation. As the ultimate decision-makers, they are responsible for oversight. The TMT's hierarchical position means they are expected to pay closer attention to security issues, especially in the face of higher breach costs.

2.2.3 Situated Attention

The principle of situated attention argues that **an individual's attention is a result of the immediate situation**. Urgent issues, such as high-cost cybersecurity breaches that cause material damage to the firm, draw the focus of the TMT. While minor breaches might be handled by IT personnel, breaches with substantial financial or reputational consequences require managerial attention and follow-up.

2.3 Statement of Hypotheses

The case study tested the following four hypotheses related to the impact of cybersecurity breach costs and TMT attention on the decision to carry out an ISRA:

1. Higher cybersecurity breach costs have a positive effect on the decision to carry out an ISRA.
2. Higher cybersecurity breach costs have a positive effect on TMT attention to cybersecurity.
3. TMT attention to cybersecurity has a positive effect on the decision to carry out an ISRA.
4. TMT attention to cybersecurity mediates the positive effect of cybersecurity breach costs on the decision to carry out an ISRA.

2.4 Critical Appraisal of the ABV

2.4.1 Merits/Strengths

The Attention-Based View (ABV) provides a strong framework for understanding why **Top Management Team (TMT) attention to cybersecurity is heightened following a costly breach**. The ABV effectively explains this through its core principles: focus of attention, structural distribution of attention, and situated attention. The focus of attention principle highlights how negative events like significant breaches become salient, compelling the TMT to prioritise cybersecurity, while the structural distribution of attention principle emphasises that the TMT's hierarchical position and fiduciary duty make them responsible for addressing major security failures. Situated attention further reinforces this by illustrating how immediate, severe breaches demand urgent managerial action.

The ABV also explains why some firms might not act on security until a crisis emerges. According to the model, TMTs have a limited attention capacity and will only focus on issues that are deemed the most important. **This limited attention capacity means that cybersecurity may not receive sufficient attention until a significant breach forces the TMT to recognise it as a priority**. This is further supported by the idea that organisations may only react to failures rather than carry out preventive security measures due to difficulty in justifying security investments. The ABV also theorises that breaches can act as a learning opportunity, as they provide inputs to enhance the quality of future security risk assessments.

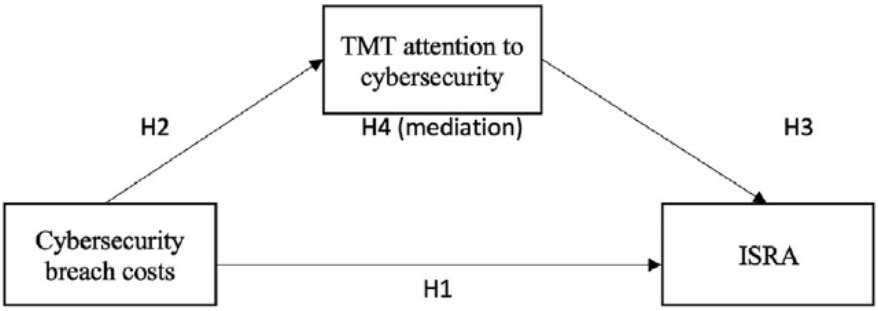

Figure 2.1: The Attention-Based View (ABV) Theory of TMT attention allocation, illustrating how breaches and organisational hierarchy influence decision-makers' focus (Shaikh and Siponen, 2023).

2.4.2 Demerits/Weaknesses

Despite its strengths, the ABV has some notable weaknesses. A significant limitation is that **it primarily focuses on a reactive response to breaches**, overlooking proactive security planning. The model is designed to explain how TMT attention is drawn to cybersecurity after a breach has occurred, but it does not adequately address how to prevent breaches in the first place. The ABV's emphasis on learning from failures shows its reactive stance, meaning that firms are continually playing catch up, rather than staying ahead of emerging threats.

Additionally, the model **assumes that TMT attention is driven primarily by negative events, ignoring other influences**. While high-cost breaches undoubtedly capture the TMT's attention, Gale, Bongiovanni and Slapnicar (2022) state that **regulatory changes and industry standards are the most influential driver of board director's involvement in cybersecurity oversight**. The ABV's narrow focus on breach-driven attention may lead to an incomplete understanding of the broader factors influencing security governance.

Furthermore, the **ABV does not provide a framework for proactive security measures**. The model explains why TMTs react to breaches, but it offers little guidance on how to implement a security posture that anticipates threats. The model's focus on how the TMT reacts after a breach also overlooks the need for continuous monitoring, security by design, and other proactive strategies.

2.5 Transition to New Model

The limitations of the ABV indicate the need for a new, proactive model. While the ABV explains how firms respond to crises, a more comprehensive approach is required to prevent them. The next section will present a new model for information security risk assessment that shifts from a reactive to a proactive approach and addresses the limitations of the ABV. This new model is intended to help organisations implement security at every stage, rather than after they have already suffered a costly breach.

Chapter 3

New "Top Down" Model Selection for Information Security Risk Assessment

3.1 Introduction to the New Model

This chapter introduces a new "top-down" Continuous and Proactive Security Assessment Model (CAPSAM) framework as a response to limitations in traditional risk assessment approaches. The case study by Shaikh and Siponen (2023) addressed the reactive nature of the Top Management Team (TMT)'s attention in its influence on the decision to carry out an Information Security Risk Assessment (ISRA). This reveals the need for a new proactive, continuous security model that integrates information security across all layers of an organisation.

3.2 Overview of the CAPSAM Framework

3.2.1 Purpose, Goals, and Intended Outcomes

The CAPSAM framework is designed to **address the limitations of cybersecurity models** by emphasising a proactive and continuous approach to risk assessment. Its primary purpose is to **integrate information security considerations from the earliest stages of system development** and throughout its lifecycle.

The main goal of CAPSAM is to minimise the likelihood and impact of cybersecurity breaches through vigilant, ongoing risk management. The model aims to **integrate information security across all layers of an organisation** and focuses on continuous improvement, ensuring a resilient security posture that adapts to the ever-changing threat landscape. By doing this, CAPSAM prioritises the protection of all stakeholders—including the customer and their data—strengthening overall organisational security and trust.

3.2.2 The Five Pillars of CAPSAM

The core philosophies of CAPSAM can be summarised in five pillars: **Culture, Continuous, Auditing, Response, Proactive (CCARP)**. These pillars are illustrated in

Figure 3.1 and form the foundation of the model's approach to information security risk management.

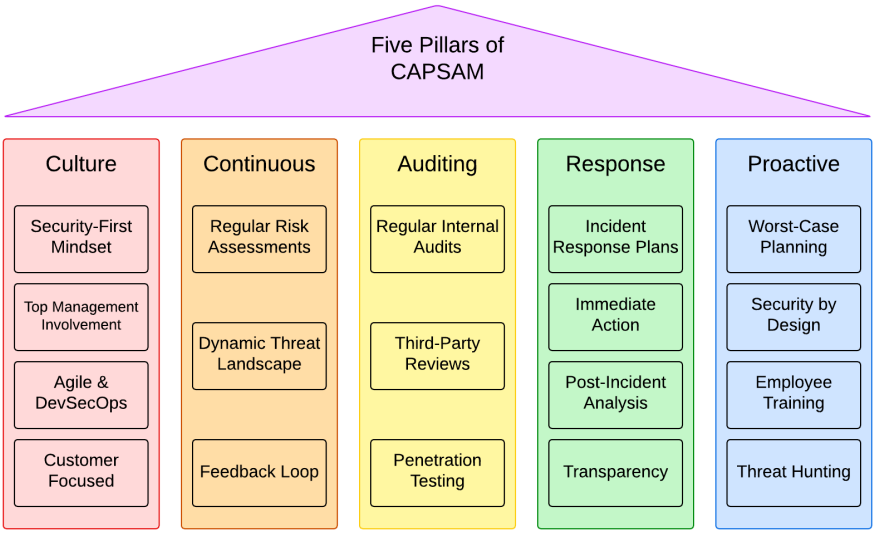

Figure 3.1: The Five Pillars of CAPSAM: Culture, Continuous, Auditing, Response, and Proactive (CCARP) and their components, explained in Table 1 in appendices.

3.2.3 FAMRM Cycle

The CAPSAM framework operates within the FAMRM cycle (New **Feature**, Information Security Risk **Assessment**, Proactive **Mitigation** Strategies, Incident **Response** Planning, and Continuous Threat **Monitoring**). This cycle ensures that each new feature or system development is subject to proactive mitigation strategies, and continuous risk assessments where feedback loops inform the next ISRA. The FAMRM cycle is illustrated in Figure 3.2.

Figure 3.2: FAMRM Cycle for Integrating Security into New Feature Development, Highlighting Continuous Risk Assessment, Proactive Mitigation, and Feedback Loops in Agile and DevSecOps Environments.

3.3 Justification for a Top-Down Approach

3.3.1 Establishing a Strong Security Posture through Executive Leadership

A top-down approach to information security risk management ensures strategic alignment and organisational commitment to security. By prioritising executive leadership, strategic priorities are set, resources allocated, and security policies enforced, framing information security as a core corporate governance issue rather than merely a technical concern (Linkov et al., 2014; Fazlida and Said, 2015). This alignment mirrors CAPSAM's emphasis on integrating security into organisational culture and fostering a "security-first mindset" among all stakeholders, as outlined in the 'Culture' pillar.

In contrast, bottom-up approaches focus on identifying technical vulnerabilities but often lack strategic direction, executive support, and adequate resource allocation (Fazlida and Said, 2015). Without such oversight, efforts may neglect broader risks, including human and social factors, hindering a cohesive and effective security strategy (Shedden, Smith and Ahmad, 2010).

3.3.2 Corporate Governance and Strategic Integration

A top-down approach aligns with corporate governance by ensuring the Board of Directors (BOD) and executive management recognise their responsibility to safeguard information assets. Fazlida and Said (2015) explain that executive involvement integrates security into organisational strategies, enhancing competitive advantage, client satisfaction, and trust. This perspective aligns with CAPSAM's goal of embedding security considerations at all organisational levels, enabling seamless integration of security measures into daily operations. CAPSAM's FAMRM cycle, along with the 'Culture' pillar, reinforce this integration by ensuring top management's active engagement and resource allocation.

3.3.3 Addressing the Limitations of Bottom-Up Approaches

Bottom-up approaches face significant challenges, including limited management buy-in and insufficient coordination across departments (Shaikh and Siponen, 2023). This results in an overemphasis on technical controls while neglecting non-technical factors, such as human error and social engineering risks (Shedden, Smith and Ahmad, 2010). Furthermore, these strategies often fail to address the complex interactions of technical, social, and economic factors shaping an organisation's risk profile (Cai and Arney, 2017). CAPSAM's top-down emphasis mitigates these issues by aligning policies with organisational needs and fostering a culture of security awareness through its 'Culture' and 'Proactive' pillars, ensuring holistic risk management.

3.4 Theoretical Foundations

3.4.1 Attention-Based View (ABV) and CAPSAM's Culture Pillar

The Attention-Based View (ABV) theory highlights the importance of prioritising issues that are contextually relevant and salient (Shaikh and Siponen, 2023). CAPSAM operationalises this theory by maintaining continuous focus on cybersecurity, thereby ensuring top management prioritises and allocates resources for proactive security measures. The 'Culture' pillar reinforces this by securing top management involvement and embedding security as a core organisational value. This approach aligns with findings that management attention significantly increases the likelihood of conducting robust Information Security Risk Assessments (ISRAs) (Shaikh and Siponen, 2023).

3.4.2 Agile and DevSecOps Principles in the Continuous Pillar

Agile methodologies and DevSecOps principles form a foundation for CAPSAM's 'Continuous' pillar, promoting adaptability, speed, and integration of security into the development lifecycle (IBM, 2021; Dingsøyr et al., 2012). Agile's iterative approach enables rapid adjustments to evolving threats, while DevSecOps emphasises visibility and auditability. The FAMRM cycle embodies these principles by incorporating ongoing risk assessments and iterative feedback loops, aligning security measures with the dynamic threat landscape (IBM, 2021).

3.4.3 ISO 31000: Risk Management Standard and the FAMRM Cycle

ISO 31000 provides a comprehensive framework for risk management, emphasising communication, monitoring, and continuous improvement (Purdy, 2010). CAPSAM integrates these principles through the FAMRM cycle, ensuring a proactive and iterative approach to risk management. By focusing on dynamic assessments and mitigation strategies, CAPSAM addresses the limitations of static risk models, aligning with ISO 31000's definition of risk as the "effect of uncertainty on objectives" (Purdy, 2010).

3.4.4 Organisational Learning and Feedback in CAPSAM

CAPSAM emphasises continuous learning through feedback loops, refining security measures based on insights from incident responses, audits, and risk assessments. This iterative approach, central to the FAMRM cycle, aligns with organisational learning principles advocating adaptation and sustained improvement (Murray and Chapman, 2003). Regular audits and third-party reviews further support this dynamic model, enhancing resilience against evolving threats.

3.4.5 Trust and Customer-Focused Security

CAPSAM prioritises customer-focused security by embedding data protection at every stage of system development, reflecting stakeholder theory and corporate social responsibility (CSR) principles (Moir, 2001; Parmar et al., 2010). The Culture pillar's emphasis on transparency and proactive incident response aligns with trust theory, which underscores the role of organisational credibility in fostering stakeholder trust (Castelfranchi and Falcone, 2010). Trust is treated as relational capital, benefiting both the organisation and its stakeholders by enhancing credibility and reliability (Castelfranchi and Falcone, 2010).

3.5 Critical Analysis of CAPSAM

3.5.1 Strengths of CAPSAM

CAPSAM stands out due to its proactive nature, allowing organisations to address potential threats before they manifest, thus reducing the likelihood of successful cyberattacks. It fosters a "security-first mindset", ensuring security is a shared responsibility across the organisation. By integrating security into agile development cycles and DevSecOps practices, CAPSAM supports iterative, security-conscious development. Its continuous improvement cycle, driven by ongoing risk assessments and feedback loops, ensures that security remains robust in the face of emerging threats. Additionally, CAPSAM's focus on customer data protection builds trust by embedding security throughout the system development process.

3.5.2 Limitations of CAPSAM

Despite its advantages, CAPSAM presents several challenges. The model requires continuous updates to risk assessments, which can be resource-intensive. Ongoing monitoring demands significant resources and may lead to over-reliance on specific teams or individuals. CAPSAM's success hinges on top management's commitment to allocating resources for cybersecurity, which can be a hurdle. Regular internal audits and third-party reviews, including penetration testing, are necessary but can be time-consuming and require external expertise. Consistent application of CAPSAM's principles in large organisations can also prove difficult (Purdy, 2010).

3.5.3 Comparison with Case Study Approach

CAPSAM's proactive approach contrasts with the reactive strategy of the case study, which focuses on addressing issues after a breach has occurred. CAPSAM integrates security from the earliest stages of development, embedding it across all organisational levels. In contrast, reactive approaches often prioritise technical fixes without addressing underlying managerial issues (Shedden, Smith and Ahmad, 2010; Shaikh and Siponen, 2023). CAPSAM's continuous nature allows for dynamic responses to emerging threats, while reactive methods are limited to incident response and do not ensure long-term resilience. By addressing vulnerabilities early and continuously, CAPSAM avoids many issues seen in reactive models.

3.5.4 Challenges in Implementing CAPSAM

Implementing CAPSAM requires securing top management support to allocate resources and prioritise cybersecurity as a strategic objective (Shedden, Smith and Ahmad, 2010). Fazlida and Said (2015) highlight that gaining board of directors (BOD) support can be difficult, as cybersecurity is often viewed solely as an IT issue, with some boards lacking the expertise to address risks and being overwhelmed by "technical jargon" (Hartmann and Carmenate, 2021). CAPSAM also necessitates consistent cross-department communication, ongoing training, and significant resources for continuous monitoring, including staffing and tools. Overcoming resistance to change from those accustomed to reactive approaches is another challenge (Murray and Chapman, 2003), and regular audits and penetration tests require additional expertise and time.

3.6 Implementation of CAPSAM

3.6.1 Phase 1: Planning and Preparation

The first phase involves securing commitment from top management to allocate resources and prioritise cybersecurity as a core strategic objective. It is essential to conduct an initial risk assessment, identify stakeholders, define roles and responsibilities, and establish clear communication channels. Aligning the security risk management policy with the organisation's overall strategy ensures that security is integrated into the organisation's broader objectives. This phase also involves fostering a cultural shift towards security and collaboration across departments, breaking down silos and encouraging organisation-wide engagement.

3.6.2 Phase 2: Implementation

In this phase, organisations adopt a DevSecOps approach, integrating security throughout the software development lifecycle. Organisations conduct risk assessments to identify vulnerabilities, prioritise risks, and develop mitigation strategies. Security must be addressed from the start and continuously monitored to maintain a proactive security posture. Mitigation strategies should be implemented to manage identified risks, and regular training should be provided to ensure employees understand their role in managing security risks, reinforcing a shared responsibility across the organisation.

3.6.3 Phase 3: Review and Improvement

The final phase focuses on regular assessments to review the effectiveness of CAPSAM and adapt it based on insights from risk assessments, incident responses, and business changes. This phase promotes continuous improvement, ensuring that the system's security posture evolves to meet emerging threats. Additionally, fostering a culture of ongoing vigilance and collaboration is essential to ensure that security remains a core value across the organisation, preventing a return to siloed working.

Chapter 4

Conclusion

4.1 Summary of the Case Study Evaluation

Summarise your evaluation of the case study and the use of the ABV theory. Restate the limitations of the ABV model regarding its reactive nature.

4.2 Key Features of CAPSAM

Reiterate the core components of CAPSAM. Re-emphasise why it is an improvement over reactive approaches.

4.3 Role of the TMT

Restate the critical role of the TMT in the success of CAPSAM. Explain how CAPSAM promotes a strategic approach to information security by requiring TMT involvement.

4.4 Benefits of CAPSAM

Highlight how CAPSAM enhances an organisation's overall cybersecurity posture. Reiterate the value of the proactive and continuous nature of the model.

References

Cai, Yu and Todd Arney (2017). 'Cybersecurity should be taught top-down and case-driven'. In: *Proceedings of the 18th Annual Conference on Information Technology Education*, pp. 103–108 (cit. on p. 10).

Castelfranchi, Christiano and Rino Falcone (2010). *Trust theory: A socio-cognitive and computational model*. John Wiley & Sons (cit. on p. 11).

Dingsøyr, Torgeir et al. (2012). *A decade of agile methodologies: Towards explaining agile software development* (cit. on p. 11).

Fazlida, Mohd Razali and Jamaliah Said (2015). 'Information security: Risk, governance and implementation setback'. In: *Procedia Economics and Finance* 28, pp. 243–248 (cit. on pp. 2, 9, 10, 13).

Gale, Megan, Ivano Bongiovanni and Sergeja Slapnicar (2022). 'Governing cybersecurity from the boardroom: challenges, drivers, and ways ahead'. In: *Computers & Security* 121, p. 102840 (cit. on p. 6).

Hartmann, Caroline C and Jimmy Carmenate (2021). 'Academic research on the role of corporate governance and IT expertise in addressing cybersecurity breaches: Implications for practice, policy, and research'. In: *Current issues in auditing* 15.2, A9–A23 (cit. on p. 13).

IBM (Oct. 2021). *DevSecOps*. URL: https://www.ibm.com/think/topics/devsecops (cit. on p. 11).

Linkov, Igor et al. (2014). 'Risk-based standards: integrating top–down and bottom–up approaches'. In: *Environment Systems and Decisions* 34, pp. 134–137 (cit. on p. 9).

Mijwil, Maad et al. (2023). 'Exploring the top five evolving threats in cybersecurity: an in-depth overview'. In: *Mesopotamian journal of cybersecurity* 2023, pp. 57–63 (cit. on p. 1).

Moir, Lance (2001). 'What do we mean by corporate social responsibility?' In: *Corporate Governance: The international journal of business in society* 1.2, pp. 16–22 (cit. on p. 11).

Murray, Peter and Ross Chapman (2003). 'From continuous improvement to organisational learning: developmental theory'. In: *The learning organization* 10.5, pp. 272–282 (cit. on pp. 11, 13).

Parmar, Bidhan L et al. (2010). 'Stakeholder theory: The state of the art'. In: *Academy of Management Annals* 4.1, pp. 403–445 (cit. on p. 11).

Prasad, Ramjee et al. (2020). 'Cyber threats and attack overview'. In: *Cyber Security: The Lifeline of Information and Communication Technology*, pp. 15–31 (cit. on p. 1).

Purdy, Grant (2010). 'ISO 31000: 2009—setting a new standard for risk management'. In: *Risk Analysis: An International Journal* 30.6, pp. 881–886 (cit. on pp. 11, 12).

Shaikh, Faheem Ahmed and Mikko Siponen (2023). 'Information security risk assessments following cybersecurity breaches: The mediating role of top management attention to cybersecurity'. In: *Computers & Security* 124, p. 102974 (cit. on pp. iii, 2, 3, 5, 7, 10, 12).

Shedden, Piya, Wally Smith and Atif Ahmad (2010). 'Information security risk assessment: towards a business practice perspective'. In: (cit. on pp. 1, 9, 10, 12, 13).

Appendices

Table 1: Components of the CAPSAM Pillars as shown in 3.1.

Pillar	Component	Explanation
Culture	Security-First Mindset	Fostering a security-first mindset across the organisation.
	Top Management Involvement	Ensuring commitment from top management for necessary resources and support.
	Agile & DevSecOps	Embedding security into the agile development cycle and DevSecOps practices.
	Customer Focused	Prioritising consumer data protection and building trust through embedded security.
Continuous	Regular Risk Assessments	Conducting regular and dynamic risk assessments throughout the system's lifecycle.
	Dynamic Threat Landscape	Continuously monitoring and adapting strategies to emerging risks.
	Feedback Loop	Using insights from assessments and responses to refine security measures.
Auditing	Regular Internal Audits	Regular audits to ensure compliance and assess security measure effectiveness.
	Third-Party Reviews	Engaging external experts for unbiased security evaluations.
	Penetration Testing	Simulating real-world attacks to identify and mitigate vulnerabilities.
Response	Incident Response Plans	Developing and regularly updating plans for potential security incidents.
	Immediate Action	Swift and decisive action to limit damage during security breaches.
	Post-Incident Analysis	Analysing breaches to understand and address vulnerabilities.
	Transparency	Clear communication with stakeholders about security incidents.
Proactive	Worse-Case Planning	Proactive measures and worst-case scenario planning.
	Security by Design	Integrating security into every phase of system development.
	Employee Training	Regular training in cybersecurity best practices.
	Threat Hunting	Actively searching for potential vulnerabilities and threats.