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

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.

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 of the Continuous and Proactive Security Assessment Model (CAPSAM)

Introduce CAPSAM as a "top-down" approach to information security risk assessment. State that this model addresses the limitations of reactive approaches and the ABV. Emphasise that it is designed to integrate security into every stage of system development.

3.2 Theoretical Foundations of CAPSAM

3.2.1 DevSecOps Principles

Explain that DevSecOps integrates security into all phases of the software development lifecycle. Emphasise the 'shift left' principle which promotes security from the beginning of development. Show how CAPSAM aligns with these principles by integrating security from the earliest stage. (IBM, 2021)

3.2.2 Risk Management Theories

Contrast CAPSAM with Financial Theory, Agency Theory, Stakeholder Theory, and New Institutional Economics. Point out that, while relevant, these theories do not provide a framework for continuous and proactive security. Highlight that the theories from the MPRA paper have low empirical verification. Use the New Institutional Economics to justify the consideration of governance processes and socio-economic institutions. (Klimczak, 2007)

3.3 Components of CAPSAM

3.3.1 Initial Risk Assessment

Explain the need for a comprehensive initial assessment at multiple levels (system, component, feature). Highlight the importance of worst-case scenario planning.

3.3.2 Proactive Measures

Describe the necessity of integrating security by design. Emphasise the need for top management involvement. Explain the importance of regular employee training.

3.3.3 Continuous Risk Assessment

Explain the need for ongoing assessments throughout the system's lifecycle. Highlight the importance of feature-level assessments. Describe the need to monitor the evolving threat landscape.

3.3.4 Incident Response Planning

Explain the need for predefined incident response plans. Highlight the importance of taking immediate and decisive action.

3.3.5 Regular Audits and Reviews

Explain the need for regular internal audits. Highlight the value of external reviews.

3.3.6 Feedback Loop

Describe the need to use findings from assessments and incidents to improve the system. Highlight how this iterative process ensures that the system adapts to new threats.

3.4 Importance of TMT Buy-In for CAPSAM

Argue that TMT involvement is crucial for aligning security with business objectives. Explain that TMT engagement fosters a proactive security culture.

3.5 Benefits of CAPSAM Over Reactive Approaches

Highlight that it promotes a proactive rather than reactive security stance. Emphasise that CAPSAM encourages continuous vigilance. State that it offers a holistic approach to security. Demonstrate that CAPSAM is adaptable to new threats.

3.6 Real-Life Examples

Include case studies or real-life examples to back up your points. Reference literature that supports proactive security. Discuss how known data breaches could have been prevented by proactive models like CAPSAM.

3.7 CAPSAM as a Strategic Approach

Show that the model treats security risk as a business issue, not just an IT concern. Explain how TMT involvement in CAPSAM aligns security with strategic objectives.

3.8 Implementation Stages of CAPSAM

Describe the four stages: initiation, design and development, operational, and feedback and improvement.

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

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 p. 2).

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).

IBM (Oct. 2021). *DevSecOps*. URL: https://www.ibm.com/think/topics/devsecops (cit. on p. 7).

Klimczak, Karol Marek (2007). 'Risk Management Theory: A comprehensive empirical assessment'. In: (cit. on p. 7).

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).

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).

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. 2, 3).

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