Evaluating the Attention-Based View in Cybersecurity Risk Management and Proposing the "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

A general overview of the increasing prevalence and sophistication of cyber threats. Highlight the potential for significant damage to businesses from cyber breaches. Emphasise that cybersecurity is a crucial concern for all organisations.

1.2 The Role of Information Security Risk Assessments (ISRAs)

Introduce ISRAs as a key tool for identifying and managing vulnerabilities. Note that ISRAs are essential for protecting IT assets. Explain that risk assessments help with prioritising security efforts.

1.3 Top Management Team (TMT) Involvement

Explain that the TMT has a critical role in cybersecurity governance. Mention that their involvement is vital for effective risk management. Indicate that TMT engagement can ensure a holistic approach to security.

1.4 Purpose of the Report

State that this report evaluates the case study's use of the Attention-Based View (ABV) theory. Introduce your proposed Continuous and Proactive Security Assessment Model (CAPSAM) as a solution. Clearly state the aim of the report, which is to critically appraise the ABV, and present a proactive approach through CAPSAM.

Chapter 2

Case Study Paper – Appraisal of Theoretical Model and Hypothesis

2.1 Summary of the Case Study

Briefly describe the case study's central question: how do cybersecurity breach costs and TMT attention to cybersecurity influence the decision to conduct an ISRA. Summarise the key findings of the research, for example, that TMT attention increases with higher breach costs and that TMT attention mediates the decision to carry out an ISRA.

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

2.2.1 Focus of Attention

Discuss how limited attention affects decision-making within an organisation.

2.2.2 Structural Distribution of Attention

Detail how an individual's hierarchical position shapes what they pay attention to.

2.2.3 Situated Attention

Explain how immediate events and situations influence the focus of attention.

2.3 Statement of Hypotheses

Clearly state the four hypotheses tested in the paper:

1. Higher breach costs increase the likelihood of carrying out an ISRA.
2. Higher breach costs increase 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

Discuss the ABV's capacity to explain why TMT attention is heightened following a costly breach. Explain the model's ability to show why firms might not act on security until a crisis emerges.

2.4.2 Demerits/Weaknesses

Point out that the ABV focuses on a reactive response to breaches, and overlooks proactive security planning. Explain that the model assumes that TMT attention is driven primarily by negative events, ignoring other influences. Highlight that the ABV does not provide a framework for proactive security measures.

2.5 Transition to New Model

Briefly indicate that the limitations of the ABV highlight the need for a new, proactive model which you will present in the next chapter.

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.

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.

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.