Quantifying Cyber Security Risk Through Interest Rate Calculation in Debt Management

Christo Coetzer[1] and Louise Leenen[1,2]
[1]University of the Western Cape, Cape Town, South Africa
[2]Center for Artificial Intelligence Research (CAIR), Cape Town, South Africa

coetzercs@gmail.com
lleenen@uwc.ac.za

Abstract: This paper introduces a novel Interest Rate Calculation Model for cyber security risk quantification, addressing the challenges of cyber security debt management. Unlike traditional qualitative risk assessments, this model applies financial principles to quantify risk impact dynamically, integrating seamlessly with industry frameworks. By framing cyber security risks in financial terms, the model enhances decision-making, promotes strategic resource allocation, and fosters stakeholder engagement. Through a structured methodology, it empowers organisations to assess, prioritise, and mitigate cyber security debt efficiently, ensuring long-term resilience in an evolving threat landscape.

Keywords: Cyber security, Cyber security debt, Cyber security debt management, Cyber security interest rate

1. Introduction

This paper is a continuation of previous research in cyber security debt management where the authors presented a novel framework for managing cyber security debt (Coetzer and Leenen, 2024). Their framework is an innovative approach that draws the principles of established industry methodologies to comprehensively assess and manage cyber security debt. Cyber security risk management traditionally relies on qualitative assessments, often failing to convey the financial impact of unaddressed vulnerabilities. This paper presents the Interest Rate Calculation Model, a new approach that translates cyber security risk into a financial metric, bridging the gap between technical assessments and executive decision-making.

The Interest Rate Calculation Model represents an approach to managing cyber security debt. Drawing on financial principles, it employs a dynamic mechanism to quantitatively evaluate the potential financial impact of unmitigated cyber security risks. Translating complex technical risks into a financial context enhances decision-making and promotes active stakeholder engagement. By integrating the probability of risk occurrence with the magnitude of potential losses, the model produces an "interest rate" that vividly illustrates the urgency and severity of specific threats.

This approach transcends technical boundaries, bridging the gap between cyber security professionals and non-technical stakeholders. By framing risk severity in financial terms, the model facilitates effective communication and enables decision-makers to prioritise resource allocation and manage risks more strategically. Through this innovative fusion of financial concepts and cyber security challenges, the Interest Rate Calculation Model delivers a tangible metric for assessing risks, fostering better prioritisation and collaboration. It empowers organisations to address cyber security debt with greater strategic insight, paving the way for sustainable digital resilience.

The outcomes of this study directly address a critical gap in cyber security risk management: the lack of quantifiable financial impact analysis. Current frameworks provide structured risk assessments but lack a dynamic cost-based evaluation of unmitigated risks. The Interest Rate Calculation Model fills this void by offering a tangible financial measure of cyber risk accumulation,

2. Background

Technical debt refers to the impact organisations create by taking shortcuts within their technical environment (Cunningham, 1993). The concept of technical debt, originally emerging within the realm of software engineering, has been transposed to cyber security to encapsulate the accumulation of vulnerabilities within an organisation's IT infrastructure (Kruchten, Nord and Ozkaya, 2012). These vulnerabilities arise from various factors, including resource constraints, time pressures, and expertise gaps. As a subset of technical debt, cyber security debt represents a critical challenge for modern organisations due to its potential to compound over time. Like financial debt, the longer these vulnerabilities remain unaddressed, the greater the associated risks and costs.

In 2017, Equifax was hit with a data breach in which hackers stole nearly 148 million Americans' personal information from an exploited server (Equifax, 2017). The information stolen included customers' names, social security numbers, birthdates and addresses. The impact was so broad in America that nearly half its citizens were affected. As demonstrated by the Equifax breach, failing to promptly address known vulnerabilities can lead to catastrophic data breaches, underlining the urgent need for proactive debt management.

Technical debt offers organisations a trade-off between quality and productivity, allowing for short-term benefits at the expense of future costs. While this trade-off may be strategically advantageous in some scenarios, unmanaged technical debt—particularly in cyber security—can result in significant long-term repercussions. Unlike certain technical debts that may never require repayment, cyber security debt accrues risks that invariably demand resolution, as unaddressed vulnerabilities amplify the likelihood of exploitation.

A recent study highlights the growing financial losses due to cybercrime; according to Sharif and Mohammed (2022), the annual global cost of cybercrime is projected to reach USD 10.5 trillion by 2025, marking a dramatic increase from USD 3 trillion in 2015. This escalation underscores the financial impact of unaddressed cyber security risks. Their analysis identifies key trends, such as the increasing sophistication of cyber-attacks, the rising cost of prevention measures, and the economic burden on organisations. They argue that cybercrime has become one of the most significant threats to global economic stability, making robust risk management practices imperative. The study also calls attention to the lack of sufficient datasets for cyber risk management, which hampers effective decision-making. This observation highlights the importance of models like the Interest Rate Calculation Model, which aim to bridge the gap between technical risk identification and financial impact analysis (Sharif and Mohammed, 2022).

Effective cyber security risk management requires a balanced approach that integrates both preventive and reactive controls to mitigate financial losses from cyber incidents. According to Bederna and Szádeczky (2023) organisations can optimise their cyber security investments by adopting a risk-based approach that minimises costs while ensuring proportionate protection aligned with business value at risk. Their study introduces novel financial metrics, such as the Effect of Incidents and the Incidence of Incident Recognition, which measure the financial impact of unplanned cyber security events compared to planned budgets. Their study demonstrates how financial analytics can enhance decision-making in cyber security management.

Existing cyber security risk frameworks such as Factor Analysis of Information Risk (FAIR) (The FAIR Institute, n.d), International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) 27005 (ISO/IEC 27005, 2022), and National Institute of Standards and Technology (NIST) (NIST, 2018) provide structured methodologies for risk assessment but lack real-time financial quantification. FAIR, for instance, excels in probabilistic risk analysis but does not dynamically evaluate the financial impact of deferred mitigation. Similarly, ISO/IEC 27005 provides a structured approach to risk management but lacks a monetary risk prioritisation mechanism.

The Cyber Security Debt Management Model expands upon traditional technical debt principles by introducing a structured approach to identifying, prioritising, and mitigating accumulated cyber security debt. This model aligns with established frameworks such as FAIR, which provides a quantitative basis for assessing risk severity and prioritising mitigation efforts. By translating technical vulnerabilities into financial terms, the model fosters a shared understanding among technical and non-technical stakeholders, ensuring that decision-makers comprehend the implications of deferred risk mitigation.

Organisations face an increasingly complex digital threat landscape where cyber security debt often remains hidden within legacy systems, third-party libraries, or deeply embedded IT architectures. The complexity and interdependencies inherent in these environments pose challenges to detection and resolution. The Cyber Security Debt Management Model addresses these challenges through its comprehensive framework, combining risk quantification, financial valuation, and strategic resource allocation to mitigate risks effectively.

Through a structured application of principles such as FAIR, the model quantifies the impact of cyber security debt, empowering organisations to make informed decisions about resource allocation. This approach not only mitigates immediate risks but also establishes a foundation for sustained digital resilience. By adopting this model, organisations can proactively address vulnerabilities, ensuring alignment between cyber security priorities and broader organisational objectives.

3. Overview of the Cyber Security Debt Management Model

The Cyber Security Debt Management Model is an innovative framework designed to address cyber security debt by integrating risk assessment, financial valuation, and strategic resource allocation. The model provides a structured, quantitative approach to managing cyber security risks, ensuring long-term digital resilience while fostering collaboration between technical and non-technical stakeholders. Figure 1 illustrates the process flow of the model and is discussed in the subsections that follow.

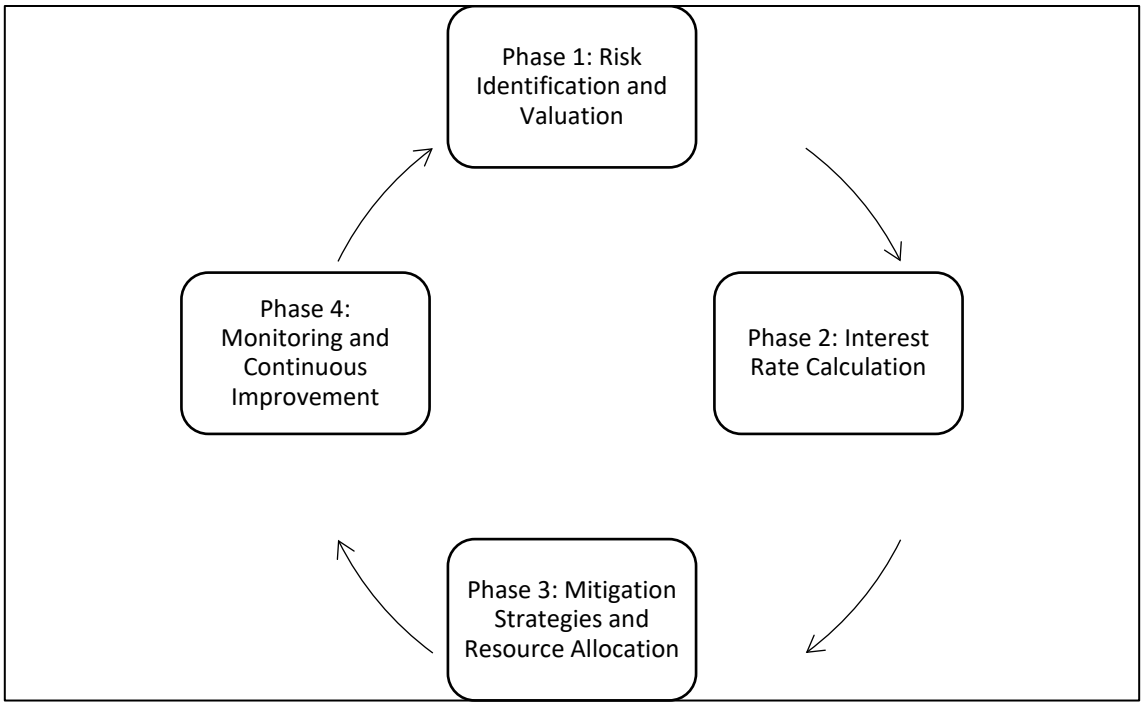

Figure 1: Cyber Security Debt Management Model (Own Compilation)

Key Components the model includes:

- **Phase 1 - Risk Identification and Valuation:** Systematically identifies and quantifies cyber security risks, translating them into financial terms for prioritisation and stakeholder communication. It incorporates frameworks like ISO/IEC 27005 and FAIR for robust risk assessment.
- **Phase 2 - Interest Rate Calculation:** A novel metric inspired by financial principles, quantifying the financial impact of unaddressed risks to highlight urgency and severity. It supports risk prioritisation and bridges communication gaps.
- **Phase 3 - Mitigation Strategies and Resource Allocation:** Guides strategic deployment of resources to high-impact risks, ensuring efficient risk reduction and fostering accountability through measurable progress.
- **Phase 4 - Monitoring and Continuous Improvement:** Promotes ongoing vigilance and adaptability, ensuring the model evolves with emerging threats and organisational changes. It fosters a proactive culture of risk management and accountability.

By combining financial and cyber security perspectives, the model empowers organisations to manage cyber security debt strategically, aligning risk management with business objectives for sustainable digital resilience.

The following sections will focus on the Interest Rate Calculation phase of the model. This phase introduces a structured methodology for quantifying cyber security risks using financial metrics. By applying financial principles, the model transforms qualitative risk factors into measurable financial terms, enabling organisations to assess their cyber security debt dynamically. The subsequent sections will detail the process, key components, and practical applications of the Interest Rate Calculation Model, providing a robust framework for prioritising risk mitigation based on financial exposure.

4. The Interest Rate Calculation Model

Corporate risk management plays a crucial role in mitigating cyber threats by integrating cyber risk considerations into broader organisational risk strategies. According to Bederna and Szádeczky (2023), firms with robust risk management frameworks are better equipped to anticipate, identify, and respond to cyber threats, thereby enhancing their overall security posture. Their study provides empirical evidence demonstrating that structured risk management practices reduce cyber risk exposure, ensuring organisations can proactively address vulnerabilities before they escalate into major incidents. This aligns with the Interest Rate Calculation Model, as both approaches emphasise a quantitative, data-driven strategy for prioritising risk mitigation.

The Interest Rate Calculation Model integrates financial and cyber security principles to produce a quantifiable metric that captures the urgency and severity of unmitigated risks. It operates by calculating an "interest rate" based on the likelihood of a given cyber security threat materialising and the estimated financial impact of the threat, should it occur. These two factors interact dynamically to provide a robust foundation for assessing the financial consequences of cyber security risks. By framing risks in terms of interest rates, organisations gain a clearer understanding of the potential financial ramifications of deferred mitigation efforts.

The Interest Rate Calculation Model's integration of financial and cyber security principles aligns closely with findings in the broader field of managing cyber security incidents.

Bederna and Szádeczky (2023) highlight the importance of incorporating financial analysis tools such as Net Present Value (NPV) and Annualised Loss Expectancy (ALE) to assess the economic implications of security breaches. NPV is a financial tool used to assess the profitability of investments by calculating the present value of expected cash inflows and outflows. In the context of security breaches, it helps quantify the long-term economic impact by considering the time value of money. ALE estimates the yearly financial loss an organisation might incur due to security breaches. It combines the cost of a single incident with its likelihood, providing a clear metric to prioritise risk management efforts. This methodology supports the interest rate calculation approach by ensuring that costs associated with security risks are evaluated against their potential financial impact, which aligns with principles of optimal security expenditure.

By including such financial metrics, the Interest Rate Calculation Model quantifies risks and prioritises them in a way that resonates with business decision-makers. This facilitates the selection of balanced security controls that optimise both preventative and reactive measures, ensuring proportional allocation of resources to manage risks effectively.

A recent study by Orlando (2021) introduced the concept of Cyber Value at Risk (Cy-VaR), which quantifies cyber risks using methodologies derived from financial risk assessment. Cy-VaR provides organisations with a statistical probability and potential financial impact of cyber threats, enabling decision-makers to prioritise resource allocation based on both likelihood and impact. By aligning to such principles, the Interest Rate Calculation Model enables organisations to assess the financial implications of cyber risks systematically.

Orlando's study highlights the integration of key components such as vulnerability assessment, asset valuation, and attacker profiling to calculate Cy-VaR effectively. The methodology emphasises that effective cyber risk quantification must consider extreme loss scenarios and their probabilities, using tools like quantile-based metrics to evaluate potential financial impacts. Furthermore, it underscores the importance of combining Cy-VaR with traditional financial metrics such as Return on Security Investment (ROSI) and NPV to optimise cyber security investments. This comprehensive approach ensures that risk mitigation efforts align with an organisation's financial and operational objectives.

The Interest Rate Calculation Model provides a single metric by combining risk occurrence probability with potential loss magnitude. This quantitative approach transforms the abstract concept of cyber security risk into a tangible financial measure, facilitating better communication across organisational hierarchies. Decision-makers, armed with this financial perspective, can prioritise risk mitigation efforts and allocate resources more effectively.

The model's adaptability further enhances its applicability in dynamic environments. As new threats emerge or organisational priorities shift, the interest rates are recalculated to reflect the evolving risk landscape. This iterative process ensures that the model remains relevant and aligned with the organisation's objectives. Additionally, by incorporating principles from established frameworks such FAIR, the model benefits from a robust theoretical foundation. FAIR's emphasis on quantitative risk analysis aligns seamlessly with the model's objectives, offering a structured methodology for assessing and managing cyber security risks.

The implications of the Interest Rate Calculation Model extend beyond immediate risk management. By providing a clear financial rationale for addressing vulnerabilities, the model fosters alignment between technical teams and executive leadership. This shared understanding is crucial in securing buy-in for cyber security initiatives and ensuring their successful implementation. Moreover, the model's focus on quantifying risks enables organisations to demonstrate accountability and compliance with regulatory requirements. By tracking changes in interest rates over time, organisations can showcase their progress in mitigating cyber security debt and improving their overall security posture.

The Interest Rate Calculation Model offers a transformative approach to managing cyber security debt. By marrying financial concepts with cyber security principles, it provides a pragmatic framework for quantifying and prioritising risks. Its adaptability, theoretical grounding, and practical applications make it an invaluable tool for organisations seeking to enhance their digital resilience and mitigate the financial impact of cyber security vulnerabilities.

4.1 Explaining the Cyber Security Debt Interest Rate Calculation Process

The Interest Rate Calculation component within the cyber security debt management model provides a dynamic method for quantifying the financial consequences of unaddressed cyber security risks. This innovative approach draws inspiration from financial principles, where interest rates reflect the cost of borrowing money. In the context of cyber security, the interest rate represents the accumulating financial burden of deferring risk mitigation efforts over time.

The calculation process begins by identifying the specific cyber security risk and estimating the likelihood of its occurrence. For example, an organisation may face a vulnerability in a web application, and the probability of it being exploited within a given period is assessed. This is followed by estimating the potential financial impact resulting from such an event, factoring in costs such as reputational damage, legal fees, fines, and revenue loss.

Once the probability of occurrence and potential loss is determined, the interest rate is calculated using the formula *Interest Rate=P×L*, where '**P'** is the probability of the risk occurring, and '**L'** is the potential loss magnitude.

The resulting interest rate quantifies the financial cost the organisation may incur if the risk is not addressed, serving as a metric to prioritise risk mitigation efforts. A higher interest rate indicates a more pressing need to act, highlighting the criticality of timely risk intervention.

This calculation empowers decision-makers to allocate resources more effectively and provides a clear, financial metric that can be easily communicated to both technical and non-technical stakeholders. By framing cyber security risks in terms familiar to financial discussions, it bridges the gap between technical teams and business leadership, enabling informed, proactive risk management. Through this process, organisations can optimise their approach to cyber security, reducing long-term risks and ensuring sustainable digital resilience by addressing the most financially impactful threats first.

4.2 Applying the Interest Rate Calculation to Cyber Security Risk Management

An organisation faces a significant cyber security risk related to a vulnerability in its web application. The vulnerability could allow attackers to access sensitive customer data if exploited. The organisation has assessed the potential risk, but due to resource constraints, it has decided to delay the implementation of a fix for six months. This delay poses a financial risk, as the vulnerability could be exploited during this period, leading to reputational damage, potential legal costs, and loss of revenue.

The first step is to identify the risk and assess its likelihood of occurring during the six-month delay. The identified risk is exploiting a vulnerability on a key web application. Based on historical data, threat intelligence, and the current cyber security landscape, the probability of an attack exploiting this vulnerability within the next six months is estimated at 40%.

Next, the potential financial impact of an exploited vulnerability is estimated. This includes costs related to data breach notification, legal fees, reputational damage, loss of customer trust, and potential fines. The organisation estimates the potential financial loss from an exploitation event to be ZAR 2 million.

The interest rate can be calculated using the risk occurrence probability and the potential loss magnitude. The interest rate represents the cumulative financial impact that will accrue if the risk is left unmitigated over time.

Interest Rate = P×L

Interest Rate = 0.40 × ZAR 2,000,000

Interest Rate = ZAR 800,000

In this case, the "interest rate" for the cyber security debt associated with this particular vulnerability is ZAR 800,000 over the six-month period. This amount represents the estimated financial cost the organisation will incur as a result of delaying risk mitigation efforts.

This calculated interest rate of ZAR 800,000 is a dynamic, quantifiable metric that can inform decision-making. It serves as a direct measure of the financial burden of deferring risk mitigation. The higher the calculated interest rate, the more urgent it is for the organisation to address the vulnerability. In this example, a ZAR 800,000 potential loss highlights the significant cost of inaction. This interest rate can be compared with other risks in the organisation's risk portfolio, allowing decision-makers to prioritise the highest financial impact risks.

The interest rate calculation provides a clear and understandable metric that can be communicated to both technical and non-technical stakeholders. By framing the risk in financial terms, stakeholders—including senior management—can grasp the potential costs and the urgency of mitigating the risk.

5. Advantages of the Model

The Interest Rate Calculation Model provides a suite of advantages that enhance its practical applicability and theoretical significance. Foremost among these is its ability to create a universal language for discussing cyber security risks. By translating technical vulnerabilities into financial terms, the model enables a shared understanding between technical experts, business executives, and other stakeholders. This shared framework facilitates strategic discussions about resource allocation, priority setting, and long-term planning, thus aligning technical objectives with business goals.

A further advantage of the model lies in its capacity for dynamic adaptability. As organisations face evolving threats and shifting operational priorities, the model recalibrates its interest rate calculations to reflect the changing risk landscape. This iterative adaptability ensures that the organisation’s resource allocation remains optimally aligned with its current risk profile, avoiding the pitfalls of static risk management approaches. In practice, this means that as new vulnerabilities are identified, or as the probability and potential impact of existing risks change, the model seamlessly integrates these updates into its assessments.

The Interest Rate Calculation Model's ability to communicate risks in financial terms brings significant advantages, as evidenced in similar approaches discussed by Bederna and Szádeczky (2023). Their research underscores that quantifying the financial effects of incidents—such as deviations in planned budgets due to unexpected cyber events—enhances accountability and aids in demonstrating value to stakeholders. Furthermore, linking financial impacts to metrics like ALE and ROSI strengthens an organisation's ability to make informed decisions.

Another advantage is the model's adaptability, which allows recalibration based on evolving threat landscapes. Bederna and Szádeczky (2023) emphasise that iterative approaches, supported by dynamic financial metrics, enable organisations to remain agile and responsive to emerging risks. This ensures that security investments are not only cost-effective but also aligned with overarching organisational objectives.

The model’s quantitative foundation enhances accountability and compliance efforts. By providing a clear and objective metric for cyber security risk—the interest rate—organisations can easily demonstrate their risk management efforts to regulatory bodies and auditors. This transparency is especially critical in sectors like financial technology, where regulatory scrutiny is high, and the consequences of non-compliance are severe. By tracking changes in calculated interest rates over time, organisations can document their progress in mitigating risks and reducing their cyber security debt.

Another notable advantage is the model’s ability to drive cost-effective resource allocation. By focusing on high-interest-rate vulnerabilities, organisations can ensure that limited cyber security budgets deliver maximum impact. For example, addressing vulnerabilities in legacy systems with high-interest rates may yield greater risk reduction than spreading resources thinly across all identified risks. This targeted approach not only reduces overall risk exposure but also ensures that investments in cyber security are strategic and impactful.

The model also fosters a proactive approach to risk management. By quantifying the escalating financial costs of deferred mitigation, the model highlights the urgency of addressing vulnerabilities before they compound. This foresight prevents organisations from falling into a reactive cycle of responding to breaches after they occur,

instead enabling them to anticipate and mitigate risks in advance. The proactive mindset encouraged by the model thus contributes to long-term resilience and reduces the likelihood of catastrophic incidents.

Furthermore, the model integrates seamlessly with existing risk management frameworks, such as FAIR, ISO/IEC 27005 and NIST guidelines. This compatibility ensures that organisations can adopt the model without overhauling their current risk management processes. Instead, the Interest Rate Calculation Model enhances these frameworks by introducing a quantitative dimension that strengthens their overall effectiveness.

The Interest Rate Calculation Model serves as a catalyst for organisational culture change. By framing cyber security as a financial imperative rather than merely a technical challenge, the model elevates its importance within the organisational hierarchy. This shift encourages greater investment in cyber security initiatives and fosters collaboration between departments, ultimately embedding risk management as a core organisational competency. By demonstrating how addressing cyber security debt can positively impact the bottom line, the model ensures that cyber security is viewed not as a cost centre but as a strategic enabler of business success.

6. Conclusion

The Interest Rate Calculation Model represents a pivotal advancement in the ongoing quest to bridge financial principles with cyber security challenges. By introducing a quantitative approach to risk assessment, the model transforms how organisations perceive and address cyber security debt. Its core strength lies in its ability to demystify the financial implications of unmitigated risks, fostering alignment between technical teams and executive leadership. This alignment ensures that cyber security is no longer treated as a siloed function but as an integral aspect of strategic decision-making.

The model's adaptability and robustness make it especially suited for dynamic environments like the South African financial technology sector. By recalibrating risk assessments in response to evolving threats and organisational priorities, the model ensures continued relevance and effectiveness. This iterative nature empowers organisations to remain agile, reducing their cyber security debt and enhancing their resilience against emerging vulnerabilities.

Moreover, the model's integration with established frameworks like FAIR and ISO/IEC 27005 underscores its practical utility. These frameworks provide a solid foundation for implementation, ensuring that the model complements existing risk management practices rather than replacing them. This compatibility reduces barriers to adoption, enabling organisations to integrate the model seamlessly into their operations.

The real-world implications of the model extend beyond immediate risk mitigation. By providing clear metrics for accountability and compliance, the model supports organisations in meeting regulatory requirements and demonstrating their commitment to robust cyber security practices. The quantifiable improvements in risk metrics, such as reduced interest rates, serve as tangible evidence of progress, bolstering stakeholder confidence and trust.

In a broader sense, the Interest Rate Calculation Model serves as a blueprint for fostering a culture of proactive risk management. By emphasising the financial consequences of deferred mitigation, the model incentivises organisations to address vulnerabilities before they escalate into significant incidents. This shift from reactive to proactive risk management has far-reaching implications for organisational resilience and sustainability.

Future research should explore the application of this model across diverse industries and geographical regions, tailoring it to specific contexts to uncover new insights into its efficacy and refinement. Implementing AI-driven analytics and machine learning techniques could enhance predictive accuracy by adapting risk interest rates based on real-time threat intelligence, improving proactive cyber security debt management. Empirical validation through case studies in various industries would help refine assumptions and establish industry-specific benchmarks. Aligning the model with cyber insurance frameworks could enable risk-based premium adjustments, allowing insurers to offer precise coverage and incentivise proactive mitigation. Further work should also incorporate additional financial variables such as market impact, regulatory penalties, and operational downtime costs to provide a comprehensive financial assessment of cyber security risks, ensuring greater accuracy in prioritising mitigation strategies.

In conclusion, the Interest Rate Calculation Model is a transformative tool for addressing the complexities of cyber security debt. Its fusion of financial and cyber security principles offers a pragmatic and impactful solution to one of the most pressing challenges facing organisations today. By adopting this model, organisations can not only mitigate their cyber security risks but also position themselves for long-term success in an increasingly interconnected and digital world.

References

Bederna, Z. and Szádeczky, T. (2023) 'Managing the financial impact of cybersecurity incidents', *Security and Defence Quarterly* [Preprint]. Available at: https://doi.org/10.35467/sdq/159625.

Coetzer, C. and Leenen, L. (2024) 'Managing Cyber Security Debt: Strategies for Identification, Prioritisation, and Mitigation', *International Conference on Cyber Warfare and Security*, 19(1), pp. 439–446. Available at: https://doi.org/10.34190/ICCWS.19.1.2178.

Cunningham, W. (1993) 'The WyCash portfolio management system', *ACM SIGPLAN OOPS Messenger*, 4(2), pp. 29–30. Available at: https://doi.org/10.1145/157710.157715.

Equifax (2017) *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes | Equifax*. Available at: https://investor.equifax.com/news-and-events/press-releases/2017/09-15-2017-224018832 (Accessed: 19 February 2021).

ISO/IEC 27005 (2022) *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. Available at: https://www.iso.org/standard/80585.html (Accessed: 22 August 2023).

Kruchten, P., Nord, R.L. and Ozkaya, I. (2012) 'Technical debt: From metaphor to theory and practice', *IEEE Software*, 29(6), pp. 18–21. Available at: https://doi.org/10.1109/MS.2012.167.

Md Haris Uddin Sharif and Mehmood Ali Mohammed (2022) 'A literature review of financial losses statistics for cyber security and future trend', *World Journal of Advanced Research and Reviews*, 15(1), pp. 138–156. Available at: https://doi.org/10.30574/wjarr.2022.15.1.0573.

NIST (2018) *Cybersecurity Framework | NIST*. Available at: https://www.nist.gov/cyberframework (Accessed: 8 April 2021).

Orlando, A. (2021) 'Cyber risk quantification: Investigating the role of cyber value at risk', *Risks*, 9(10). Available at: https://doi.org/10.3390/risks9100184.

The FAIR Institute - Quantitative Information Risk Management. (n.d.). Retrieved August 16, 2024, from https://www.fairinstitute.org/