Managing Cyber Security Debt: Strategies for Identification, Prioritisation, and Mitigation

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 explores cyber security debt, a technical debt arising from unaddressed security vulnerabilities in an organisation's IT systems. These vulnerabilities accumulate due to resource limitations, time constraints, and expertise gaps, potentially leading to security breaches and data compromises. The paper outlines the cyber security debt management process involving identification, prioritisation, and mitigation strategies. Drawing parallels to financial debt, the authors emphasise the escalating risks of delaying cyber security debt repayment. The paper underscores the significance of diligent debt management in maintaining digital resilience and mitigating cyber threats. The increasing interconnectedness of systems and rapid software development has given rise to a hidden challenge known as cyber security debt. Cyber security debt is posed as a subset of technical debt, encompassing the accumulation of security vulnerabilities within an organisation's IT infrastructure and applications. Drawing a parallel between cyber security debt and its financial counterpart, the authors underscore the grave risks of deferring debt repayment. Just as financial debt accrues interest, unresolved security vulnerabilities compound over time, elevating the likelihood of breaches and data exposure. A poignant case study of the Equifax breach exemplifies the real-world consequences of neglecting security debt management. The failure to patch a well-known vulnerability led to a colossal data breach, highlighting the urgency of addressing security weaknesses promptly. Complex in nature, cyber security debt materialises when organisations fail to address vulnerabilities during various operational life cycles. These vulnerabilities might remain concealed within IT architecture, legacy code, or third-party libraries, posing a formidable challenge to detection and resolution. By understanding the parallels between financial and cyber security debt and proactively managing the latter, organisations can enhance their ability to safeguard against evolving cyber threats and maintain a robust security posture.

Keywords: Cyber security, Cyber security debt, Cyber security debt management

1. Introduction

This paper delves into cyber security debt management, presenting a novel framework designed to address this critical issue. This framework, referred to as the "proposed framework" throughout this paper, represents an innovative approach to tackling cyber security debt. It offers a fresh perspective, drawing on the principles of established methodologies such as Factor Analysis of Information Risk (FAIR) (*The FAIR Institute - Quantitative Information Risk Management*, n.d.), to comprehensively assess and manage cyber security debt.

In a rapidly evolving landscape where new threats constantly emerge, it is crucial to understand the concept of technical debt management and its relevance to the cyber security industry. Technical debt refers to the impact organisations create by taking shortcuts within their technical environment (Cunningham, 1993). Technical debt is mainly referred to within software development. It includes the build-up of poorly designed, unnecessarily complicated, or unwanted code or software, which are deficiencies in internal quality that make it harder to modify and extend a system further. This paper emphasises the need to identify, prioritise, and mitigate accumulated security vulnerabilities to minimise the risk of security breaches and data compromises.

We explore the intricacies of cyber security debt management, delving into the proposed framework and its application within the cyber security landscape. By adopting a methodology grounded in FAIR and considering the principles of technical debt management, organisations can enhance their ability to safeguard their digital assets and minimise the risks associated with unaddressed vulnerabilities. The evolution of cyber threats necessitates our strategies, and this paper strives to provide a forward-thinking approach to meet this challenge head-on.

The next section provides an overview of technical and cyber security debt management. In section 3 the authors present a unique cyber security debt management model and the paper is concluded in Section 4.

2. Technical and Cyber Security Debt Management

Initially, the technical debt metaphor was mainly used as a communication device - shifting the dialogue from a technical vocabulary to a financial language made discussions clearer and easier to understand for non-technical

people (McConnell, 2008). One of the most fruitful areas of achievement in technical debt research is technical debt identification, which is the first step in technical debt management (Seaman et al., 2012).

By incurring technical debt, organisations can trade off quality against productivity. An advantage of this includes short-term reduced maintenance time as well as cost. This, though, comes with the cost of additional work in the future, equivalent to paying interest on a debt. In this sense, technical debt as a term characterises the effect of delaying tasks, such as maintenance, on technical-focused projects. Nonetheless, technical debt is not the same as financial debt. The significant difference is that the interest associated with technical debt may or may not ever need to be paid off (Seaman et al., 2012). For example, it is not necessary to refactor a technical item that is overly complex if no further changes will be requested on that item in the future. This uncertainty differentiates technical debt from financial debt and further complicates the issue. Still, it also allows an organisation to leverage technical debt for their projects. Incurring technical debt has benefits but should be managed before a more significant, long-term cost is realised. Thus, organisations have to balance the costs and benefits of technical debt and make informed decisions on how technical debt should be prioritised and managed.

Cyber security debt is a subset of the above-explained technical debt. Cyber security debt refers to the accumulation of security issues or vulnerabilities in an organisation's IT infrastructure or applications due to various factors, such as limited resources, time constraints, or lack of expertise. These accumulated security issues can create significant technical debt, leading to security breaches and data compromises. Cyber security debt management encapsulates identifying, prioritising, and mitigating accumulated security debt. It involves assessing the organisation's current security posture, identifying security debt items, estimating the cost and effort required to address them, and prioritising the things based on their potential impact and likelihood of exploitation.

The concept of technical debt has been studied and applied in the software engineering domain, where it refers to the cost of future rework due to shortcuts taken during the development process. Researchers have recently proposed using the same concept to cyber security to manage security debt (Kruchten et al., 2012). Understanding and assessing technical debt is crucial. Dan Geer and Gunnar Peterson suggest using a Margin of Safety calculation to compare the 'book value' of an organisation's IT assets with the security controls and services used to defend them to determine its technical or security debt ratio (Geer & Peterson, 2014). Rather than facing forced repayment, an organisation should understand its obligation and implement processes to manage it, such as investing in managed services or taking out cyber insurance.

Short falling on financial debt payments results in more interest and extends the time to reach the principal. Fast falling on cyber security debt does not only delay future projects; it also results in the piling up of vulnerabilities, which places an organisation at greater risk of malicious cyber security exploits. The longer these security debts remain unpaid, the more interest they will accrue to address the shortcomings of the original investment.

An example of cyber security debt management can be found in the Equifax breach (2017). The organisation failed to patch a known vulnerability identified in Apache Struts, an open-source web application framework. Although the patch had been available for months, the organisation failed to deploy it, costing them a cyber security breach that compromised the personal data of more than 147 million people.

The accumulation of cyber security debt occurs when an organisation completes a project without addressing the identified weaknesses and vulnerabilities. Existing cyber security debt worsens if a project delays addressing an identified vulnerability due to pressured timelines. Accumulative cyber security debt can cause immense negative impact within an organisation. Organisations need to spend time and effort managing cyber security debt to minimise cyber security debt.

Cyber security debt is complex and is created by failing to address cyber security within the various organisational defined life cycles, such as project management or software development. As with its financial counterpart, it can be difficult to identify, often hidden deep in an organisation's IT architecture, legacy code, third-party libraries, and even the fundamental economic principles upon which some business models are based (Van Der Walt, 2018). In some cases, the complexity can be so great that the average business may be unable to determine where the interdependencies lie.

Several notable works have paved the way for a deeper understanding of these intertwined concepts in the technical and cyber security debt management landscape. Researchers have extensively explored the realm of technical debt, which initially emerged in software engineering, encompassing the costs incurred due to shortcuts during development. Technical debt principles have been transposed into cyber security, emphasising

identifying, prioritising, and mitigating security vulnerabilities to prevent potential breaches and data compromises (Lehman, 1979). Furthermore, influential studies have advocated adopting technical debt management practices within cyber security (Kruchten et al., 2012). This cross-disciplinary perspective has illuminated the parallel between technical and cyber security debt, underscoring the importance of addressing the accumulated vulnerabilities in an organisation's digital infrastructure. Additionally, foundational works in the field of Factor Analysis of Information Risk (FAIR) by Hubbard (Hubbard, 2020) have provided valuable insights into risk assessment and management, serving as a fundamental framework that forms a cornerstone for the Cyber Security Debt Management Model introduced in this paper. By building upon these established foundations and extending them into the unique domain of cyber security debt, we aim to contribute a practical approach for organisations to manage their digital risk landscape better.

3. The Cyber Security Debt Management Model

In this section, we introduce the Cyber Security Debt Management Model, a unique framework developed to address cyber security debt. This novel model is distinctly tailored to the evolving landscape of digital cyber security risk management. We emphasise the need for fresh, innovative approaches to confront the challenges posed by cyber security debt in today's interconnected digital world. The Cyber Security Debt Management Model represents a significant contribution, bridging the gap between technical debt management and cyber security. The model is a comprehensive and innovative framework that redefines how organisations approach and mitigate the ever-growing challenge of cyber security debt. By combining risk assessment, financial valuation, and strategic resource allocation, this model offers a systematic and quantifiable approach to managing cyber security risks and ensuring long-term digital resilience.

Figure 1 illustrates the process flow of the model and is discussed in the subsections that follow.

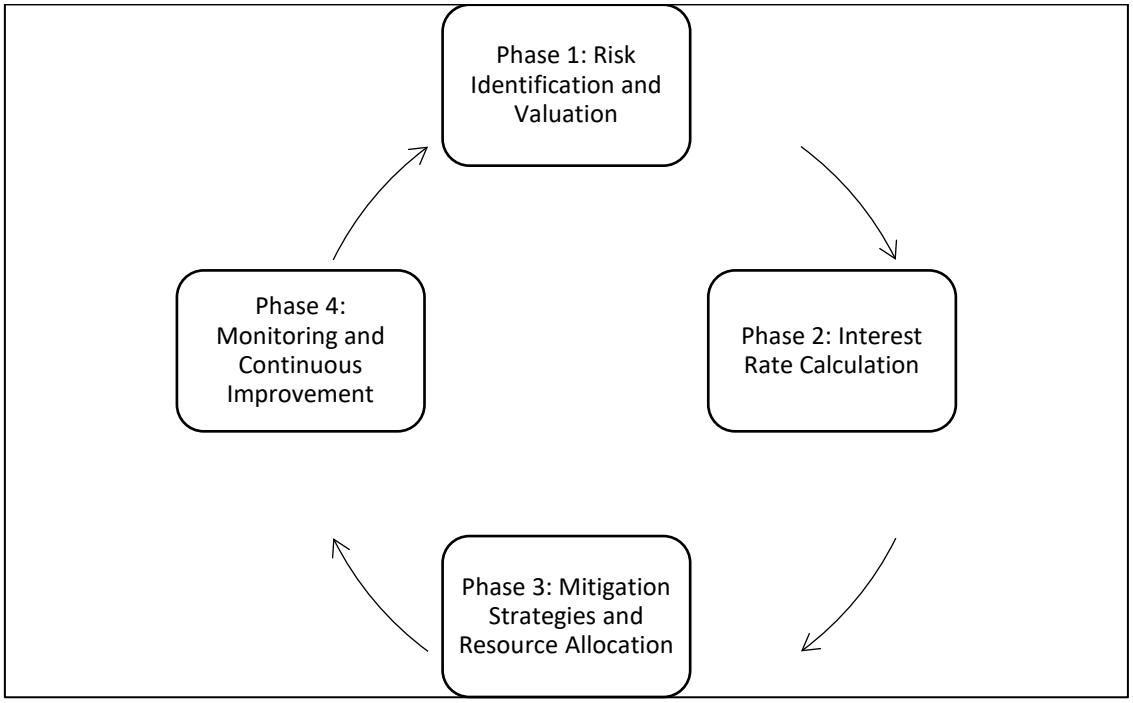

Figure 1: Cyber Security Debt Management Model (Own Compilation)

3.1 Risk Identification and Valuation

The cornerstone of the cyber security debt management model, the Risk Identification and Valuation component, offers a systematic approach to unearthing potential cyber security risks within an organisation's digital ecosystem. This phase is the foundation for effective risk management strategies in a landscape characterised by escalating threats and evolving vulnerabilities.

The process is aligned to the ISO/IEC 27005:2022 *Information security, cybersecurity and privacy protection — Guidance on managing information security risks* framework (ISO/IEC 27005, 2022) and commences with a meticulous and comprehensive identification of potential risks. This involves a rigorous analysis of an organisation's digital infrastructure, encompassing information systems, networks, software applications, and

critical assets. By scrutinising the entirety of the digital landscape, the model ensures that no potential risk goes unnoticed. These risks extend beyond technical vulnerabilities to threats posed by external actors, internal vulnerabilities, and emerging attack vectors.

Once identified, each risk undergoes a quantitative valuation to assess its potential financial impact. This valuation relies on a combination of factors, including the possible loss magnitude and the likelihood of risk occurrence. Each risk is assigned a numerical value that reflects its financial implications, allowing for an objective comparison and prioritisation of risks. By quantifying risks in monetary terms, organisations gain a pragmatic understanding of the potential consequences of cyber security debt. The quantification process not only aids in informed decision-making but also provides a crucial metric to communicate risk severity to non-technical stakeholders. Translating technical jargon into financial terms bridges the communication gap between cyber security professionals and organisational leadership. Decision-makers can comprehend the financial implications of unmitigated risks, facilitating more meaningful discussions and collaborative efforts toward risk mitigation.

The Risk Identification and Valuation component is a roadmap for organisations to address cyber security debt proactively. It enables organisations to identify potential vulnerabilities, quantify their impact, and lay the groundwork for effective resource allocation. This phase is instrumental in prioritising mitigation efforts, ensuring that resources are allocated to areas with the highest potential for risk reduction. As the digital landscape evolves and new risks emerge, the component's iterative nature allows organisations to regularly reassess and recalibrate their risk valuations, ensuring continued alignment with the ever-changing threat landscape.

In essence, the Risk Identification and Valuation component of the cyber security debt management model empowers organisations to unearth potential vulnerabilities systematically, assign them tangible financial values and lay the foundation for a comprehensive risk mitigation strategy. This component equips organisations with the insights needed to navigate the intricate cyber security landscape with resilience and efficacy by quantifying risks and fostering a holistic understanding of their financial implications.

FAIR is a robust and widely adopted framework for quantifying and analysing information and cyber security risks (*The FAIR Institute - Quantitative Information Risk Management*, n.d.). Developed by the Open Group, FAIR provides a structured methodology that enables organisations to assess and prioritise risks based on quantitative measurements, enhancing decision-making and resource allocation in cyber security. The framework incorporates financial concepts and risk analysis principles to understand risk exposure comprehensively. The following actions are prescribed:

3.1.1 Integrating FAIR into "Risk Identification and Valuation"

Integrating FAIR principles enhances the "Risk Identification and Valuation" phase in the cyber security debt management model context. By incorporating FAIR into this phase, organisations can enrich their risk assessment process with a quantitative perspective, aligning seamlessly with the model's objective of quantifying risk exposure and prioritising mitigation efforts. FAIR introduces several vital components that can be integrated into the Risk Identification and Valuation phase:

Risk Taxonomy and Definitions: FAIR emphasises the importance of a standardised risk taxonomy and precise definitions for various risk factors. Incorporating FAIR's risk categories and descriptions augments the accuracy of risk identification, ensuring a consistent and shared understanding among stakeholders.

Loss Event Frequency (LEF) and Loss Magnitude: LEF and loss magnitude are fundamental concepts in FAIR. Incorporating these concepts into the model's risk identification phase allows for a more structured assessment of how frequently specific loss events may occur and the potential financial impact if they materialise.

Scenario Analysis: FAIR encourages the creation of well-defined scenarios to assess risks comprehensively. This aligns with the model's objective of scenario design and execution. By integrating FAIR's scenario analysis approach, organisations can delve deeper into risk identification and valuation, capturing nuanced risk profiles.

Risk Measurement: FAIR employs calibrated estimation techniques to quantify risk factors. This can be applied to estimate probabilities and potential loss magnitudes associated with various risks. Integrating FAIR's risk measurement techniques enhances the model's ability to accurately quantify interest rates and cyber security debt.

Data Collection and Analysis: FAIR places emphasis on data collection and analysis to inform risk assessments. Integrating FAIR's data-driven approach into the Risk Identification and Valuation phase ensures that evaluations are grounded in empirical evidence, enhancing the accuracy and reliability of risk valuations.

The cyber security debt management model leverages a quantitative and standardised framework for assessing and quantifying risks by infusing FAIR principles into the Risk Identification and Valuation phase. This integration facilitates a more rigorous and comprehensive understanding of risk exposure, enabling organisations to prioritise mitigation efforts based on quantifiable data and aligning with the overarching goal of effective cyber security debt management.

FAIR enriches the Risk Identification and Valuation phase by introducing structured risk taxonomy, quantitative measurement techniques, scenario analysis, and data-driven assessments. By incorporating FAIR principles, organisations can enhance their ability to identify, assess, and quantify risks accurately, ultimately strengthening the foundation of the cyber security debt management model's risk assessment process.

3.2 Interest Rate Calculation

A defining innovation within the cyber security debt management model, the Interest Rate Calculation component, introduces a dynamic and intuitive mechanism to quantify the potential financial consequences of unmitigated cyber security risks. Unfortunately, there were not many new research papers found in the field of cyber security debt with a focus on interest calculations. Drawing parallels from the financial domain, where interest rates reflect the cost of borrowing money, this component leverages this concept to express the cost of deferring risk mitigation efforts over time. In this context, the interest rate encapsulates the cumulative financial impact that a particular cyber security risk may incur if left unaddressed. Computed through the fusion of risk occurrence probability and potential loss magnitude, the interest rate paints a vivid picture of the urgency and severity associated with each risk. A high-interest rate signifies a rapidly accumulating cyber security debt, spotlighting the criticality of timely risk mitigation.

This quantitative representation of risk underscores the far-reaching implications of cyber security debt. Like compounding interest in finance, unmanaged risks can compound over time, magnifying financial repercussions. The interest rate is a decision-support metric and offers a tangible measure to illustrate the potential long-term costs of neglecting risk mitigation efforts.

The interest rate calculation introduces a uniform framework for risk prioritisation, allowing organisations to compare and rank risks based on their calculated rates objectively. This empowers decision-makers to allocate resources prudently, directing them towards addressing risks with the highest potential financial impact. In doing so, the organisation can optimise resource utilisation, strategically deploying mitigation measures to areas that promise the most significant reduction in cyber security debt. Furthermore, the interest rate calculation component transcends technical jargon, enabling effective communication between cyber security professionals and non-technical stakeholders. By expressing cyber security risks in terms familiar to financial discussions, the model facilitates a shared understanding of risk severity. This alignment enhances communication, enabling decision-makers to grasp the financial stakes and make informed choices regarding resource allocation and risk management strategies. In addition, the Interest Rate Calculation component provides a dynamic and adaptable metric that evolves with the ever-changing cyber security landscape. As threat vectors evolve and organisational priorities shift, the model accommodates adjustments to risk occurrence probabilities and potential loss magnitudes. This flexibility ensures that the calculated interest rates remain relevant and reflect emerging risks, empowering organisations to respond proactively.

The Interest Rate Calculation component of the cyber security debt management model presents a ground-breaking methodology to quantify the financial implications of cyber security risks. Drawing inspiration from financial principles and applying them to cyber security, this component offers a tangible and intuitive metric that enhances risk prioritisation and fosters effective communication. It empowers organisations to address cyber security debt with strategic insight. The model highlights the intersection of financial and cyber security considerations through the interest rate calculation, forging a path towards proactive risk mitigation and sustainable digital resilience.

3.3 Mitigation Strategies and Resource Allocation

The Mitigation Strategies and Resource Allocation component is a pivotal pillar within the cyber security debt management model, translating quantitative risk assessments into actionable strategies that fortify an

organisation's cyber security posture. This dynamic phase harnesses the insights from risk valuation and interest rate calculation to guide judicious resource allocation and strategic risk mitigation.

With interest rates that quantify the potential financial consequences of unaddressed cyber security risks, supported by debt calculation, organisations embark on a strategic journey of resource allocation. The calculated interest rates serve as a compass, directing decision-makers towards risks with the highest potential impact. By focusing resources on threats with elevated interest rates, organisations ensure that their mitigation endeavours yield maximum value in risk reduction and cyber security debt alleviation.

The component's essence lies in optimising resource utilisation to address the most pressing vulnerabilities. It empowers organisations to allocate personnel, time, and financial investments where they are most needed. High-interest-rate risks demand immediate attention and a robust allocation of resources to mitigate their potential financial ramifications. This strategic deployment of resources enables organisations to enact proactive measures that reduce the long-term accrual of cyber security debt.

Mitigation strategies span a spectrum of approaches, from technical solutions such as software patching and network segmentation to non-technical measures like employee training and incident response planning. The model facilitates a comprehensive understanding of the most effective strategies for each risk, resulting in a tailored and pragmatic approach to risk mitigation. Resources are channelled strategically, reflecting an organisation's unique risk profile and priorities.

The component also instils a culture of accountability by establishing measurable targets for risk reduction. Progress is tracked through a tangible decrease in interest rates, reflecting the diminishing potential financial impact of mitigated risks. This quantifiable improvement enables organisations to showcase their commitment to cyber security resilience, bolstering stakeholder confidence and demonstrating proactive risk management.

Furthermore, the iterative nature of the model ensures that mitigation strategies remain adaptable to the evolving threat landscape. As new risks emerge and organisational priorities shift, the component enables organisations to recalibrate resource allocation and adjust mitigation strategies accordingly. This dynamic responsiveness is crucial for maintaining an effective and up-to-date cyber security posture, safeguarding against emerging vulnerabilities.

The Mitigation Strategies and Resource Allocation component empower organisations to leverage quantified risk assessments for strategic decision-making. Organisations take decisive steps toward minimising cyber security debt by allocating resources where they are most impactful and tailoring mitigation strategies to individual risks. This component fosters a culture of proactive risk reduction, enhancing digital resilience and positioning cyber security as an integral aspect of organisational sustainability. Organisations forge a path toward a secure digital future through strategic resource allocation, adeptly managing the cumulative consequences of cyber security debt.

3.4 Monitoring and Continuous Improvement

The bedrock of the cyber security debt management model's resilience and effectiveness lies within the Monitoring and Continuous Improvement component. In an era marked by dynamic and relentless cyber threats, this phase serves as a strategic compass that enables organisations to navigate the ever-evolving digital landscape with agility and foresight.

This component recognises that cyber security risks are not static entities but dynamic forces that demand ongoing vigilance. It underscores the importance of continuous monitoring, regular reassessment, and iterative refinement. As the threat landscape mutates and organisational priorities shift, the model adapts to ensure that risk assessments remain relevant and resource allocation remains aligned with emerging risks. By consistently monitoring the efficacy of risk mitigation strategies, organisations can gauge the actual impact of their efforts. The model encourages a proactive approach, allowing organisations to identify potential gaps, emerging vulnerabilities, or changes in risk profiles. This real-time assessment empowers organisations to refine their strategies promptly, ensuring that cyber security debt remains under control and that the risk landscape is met with adaptive defences.

The iterative nature of the component extends to the interest rate calculation, which allows organisations to adjust risk valuations and potential loss magnitudes based on evolving circumstances. This flexibility ensures that the model remains responsive and adaptable to new threat vectors, technologies, and organisational developments. As a result, the calculated interest rates accurately reflect the potential financial impact of cyber security risks, guiding resource allocation with precision. Moreover, the continuous improvement cycle

reinforces a culture of proactive risk management and accountability. Stakeholders witness tangible progress as interest rates decrease over time, showcasing the organisation's commitment to reducing cyber security debt. This transparent and quantifiable improvement strengthens stakeholder trust and fosters a culture of collective responsibility, positioning cyber security as a fundamental aspect of overall business resilience.

The Monitoring and Continuous Improvement component also holds the potential to uncover valuable insights that inform strategic decision-making. Organisations can glean actionable intelligence by analysing trends and patterns in risk valuations and mitigation efforts. These insights empower organisations to forecast potential risk trajectories, allocate resources pre-emptively, and identify emerging threats before they escalate into substantial cyber security debt.

The Monitoring and Continuous Improvement component of the cyber security debt management model ensures the model's relevance and efficacy in the face of an ever-changing threat landscape. By instilling a proactive mindset, fostering adaptive risk management, and providing a mechanism for ongoing assessment and refinement, this component enables organisations to mitigate cyber security risks with agility and foresight. It underscores the importance of sustained vigilance, resilience, and continuous evolution in pursuing long-term digital security and mitigating cyber security debt.

4. Conclusion

In the face of the relentless evolution of digital landscapes and the pervasive threats they bring, adopting the cyber security debt management model emerges as a seminal advancement in cyber security risk management. This innovative model encapsulates a transformative approach that transcends traditional boundaries, offering organisations a robust framework to combat the burgeoning challenge of cyber security debt effectively.

The model's emphasis on quantification presents a paradigm shift that addresses the limitations of qualitative risk assessments. By translating cyber security risks into tangible financial terms, decision-makers gain unprecedented clarity into the potential consequences of unmitigated vulnerabilities. This newfound comprehension enhances communication between technical experts and non-technical executives, fostering critical collaborative efforts in an increasingly interconnected business environment.

Integrating financial concepts within cyber security signifies a monumental leap towards aligning security efforts with overarching business objectives. The model's ability to articulate risks in financial language bridges the gap between cyber security and executive leadership, positioning cyber security debt as a strategic concern integral to an organisation's overall risk management strategy. This alignment ensures that cyber security professionals and executives have a common understanding, enabling well-informed decision-making that resonates with broader business goals.

The dynamic nature of the model, underscored by the iterative process of continuous monitoring and improvement, amplifies its resilience in the face of ever-evolving threats. As the threat landscape mutates and organisational priorities shift, the model adapts by recalibrating risk valuations and resource allocations. This agility ensures that organisations remain proactive in addressing emerging vulnerabilities, thereby pre-emptively curbing the accrual of cyber security debt.

The cyber security debt management model engenders a culture of accountability, optimisation, and resilience within organisations. The model enables organisations to proactively reduce cyber security debt and curtail potential financial losses by quantifying risks, determining interest rates, and steering resource allocation. It positions cyber security as an imperative facet of strategic decision-making, emphasising the importance of strategic resource allocation and fostering a proactive stance against the long-term implications of unmanaged risks. As organisations confront an increasingly intricate digital landscape, adopting the cyber security debt management model offers a formidable arsenal for risk mitigation. Its integration of financial and cyber security concepts and its quantifiable framework empowers organisations to address cyber security debt comprehensively. In doing so, the model equips organisations to navigate the complexities of the digital age, safeguard valuable assets, and ensure sustained success in an evolving and interconnected world.

References

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

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

Geer, D., & Peterson, G. (2014). Measuring Security Book Value. In *Columns - Margin of Safety or Speculation* (pp. 49–51).

Hubbard, D. W. (2020). The failure of risk management: Why it's broken and how to fix it. *The Failure of Risk Management: Why It's Broken and How to Fix It*, 1–366. https://doi.org/10.1002/9781119521914

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

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

Lehman, M. M. (1979). On understanding laws, evolution, and conservation in the large-program life cycle. *Journal of Systems and Software*, *1*(C), 213–221. https://doi.org/10.1016/0164-1212(79)90022-0

McConnell, S. (2008). *Managing Technical Debt | Construx*. https://www.construx.com/resources/whitepaper-managing-technical-debt/

Seaman, C., Guo, Y., Zazworka, N., Shull, F., Izurieta, C., Cai, Y., & Vetrò, A. (2012). Using technical debt data in decision making: Potential decision approaches. *2012 3rd International Workshop on Managing Technical Debt, MTD 2012 - Proceedings*, 45–48. https://doi.org/10.1109/MTD.2012.6225999

The FAIR Institute - Quantitative Information Risk Management. (n.d.). Retrieved August 16, 2023, from https://www.fairinstitute.org/

Van Der Walt, C. (2018). *Understanding and Assessing Technical Debt for Improved Cybersecurity*. https://www.cbronline.com/opinion/technical-debt-cybersecurity