© Journal of Security Management, Policy & Administration, Nigerian Defence Academy, Kaduna. Vol. 2, No. 2, 2025 ISSN: 2971-7973
Available on https://jsmpa.com.ng. Thomas ACHU UDUO, and Raymond NSOR AKPET -OBAJI

Security at What Cost: Evaluating Risks, Threats, and Vulnerabilities In Business Practices

By

Thomas ACHU UDUO, PhD

And

Raymond NSOR AKPET-OBAJI, PhD

From

Research Fellow, ICEST Resource Centre, Lagos

Abstract

Cybercrime, insider threats, and regulatory pressures continue to rise, driving organisations to spend heavily on security. Nevertheless, many firms are failing to see outcomes in line with this growing investment. Therefore, this article asks, what is the cost of security? By cost, we consider not just financial outlay but organisational resource allocation and the opportunity cost of shifting funds to security from innovation and competitiveness. To answer this question, we conducted a cross-sectoral survey of 220 medium and large firms in finance, healthcare, retail, logistics, and biotechnology. We applied stratified random sampling and structured questionnaires based on the NIST Cybersecurity Framework and ISO 27001. We found that governance-related vulnerabilities are the strongest predictors of organisational risk, but that organisations often share resources unequally, driven more by compliance requirements and firm size than exposure. These findings support proportional, resilience-oriented investments and embedding security within corporate governance and international policy frameworks.

Keyword: Security, Risks, Threats, Vulnerabilities, business practices

INTRODUCTION

In today's globalised and digitalised economy, organisations face unprecedented challenges in safeguarding their assets, operations, and reputations. Security has become a central concern not only for information systems professionals but also for corporate boards, regulators, and customers. Beck (1992) argued that modernisation produces manufactured risks that are transboundary, systemic, and often beyond the control of individual firms. This is so relevant in today's digital era as the rise of cloud computing, artificial intelligence, and connected supply chains increase the opportunities and vulnerabilities in several ways. Anderson and Moore (2009) stated more than two decades ago that information security is not a technological problem alone, but an economic one. The incentives generally do not favour an optimal outcome. As the cost of security rises, the breaches, disruptions, and reputational losses continue to occur, and the core question of this study emerges: Security at what cost? In many ways, it is always a paradox in terms of the efficacy of security expenditure. Underinvestment can lead to catastrophic losses while overinvestment could have negative consequences and can take away the company's resources from other activities, innovation, and competitiveness (Ahmad, et al 2020).

However, Gordon and Loeb (2002) demonstrated that optimal security investment typically falls below the maximum potential loss, establishing the principle of rational underinvestment. Empirical studies have revealed consistent misalignment between risks and expenditures, for instance, Campbell et al. (2003) showed that reputational damage often exceeds direct financial losses, while Cavusoglu et al. (2004) found that breaches reduce firm value despite creating spillovers for vendors. Romanosky (2016) reinforced this by demonstrating that many firms fail to evaluate costs and benefits systematically. These studies collectively suggest that investment decisions are not always rational, highlighting the need for cross-sectoral empirical analysis. A growing body of scholarship has questioned the assumption of rational investment. Romanosky (2016), in his study of cyber incidents, demonstrated that firms often fail to systematically evaluate costs and benefits, leading to either under-preparedness or inefficient expenditure. Gal-Or and Ghose (2005) argued that firms are reluctant to share information about breaches, even when doing so, would create collective

benefits, because reputational concerns outweigh rational incentives. Again, Fedele and Roner (2022) further reinforced this by showing that the economics of cybersecurity are characterised by externalities and market failures, leaving systemic underinvestment as a persistent challenge. Schneier (2003) captured this dynamic in a more practical sense, describing how many corporate security measures function less as technical protections and more as security theatre designed to reassure stakeholders. These observations indicate that security expenditure is usually ceremonial, where it helps to build institutional credibility, but is not commensurately protective (Asghari, van Eeten, and Bauer, 2015).

As a result of these theoretical and empirical contributions, gaps nevertheless exist in our knowledge regarding the interaction of vulnerabilities, risks, and costs across industries. Most previous studies have concentrated on one of the forms of event-based studies, e.g. market responses to breaches, or theoretical results of optimal spending. Although these methods are helpful, they do not explain cross-sectoral patterns of spending and results comprehensively. In their extensive research on the cost of cybercrime, Anderson et al. (2013) emphasised the need for more detailed empirical data to assess how firms utilise resources and whether these costs lead to quantifiable improvements in resilience. According to Bandyopadhyay, Mookerjee, and Rao (2009) who opine that most organisations do not consider market tools, including cyber insurance, instead reflecting their behaviour and organisational bias rather than sound decision-making. Generally, these suggest there is a need for empirical research to systematically test the association between vulnerabilities, risks, costs, and outcomes.

This gap is fill in the study through a quantitative research design that seeks to investigate the dynamics of security costs in different sectors. First, are governance, technical, and socio-economic vulnerabilities predictors of organisational risk levels? Second, are companies spending security resources in a manner that they are equal to the risk undertaken or are the expenditures not related to the exposures? Third, what are the impacts of security costs on the outcomes of reducing downtimes, efficiency, competitiveness and stakeholder trust? By framing the research around these questions, the study attempt to answer the question of whether firms are rational investors who optimise their costs and benefits or are institutional actors who distribute their

resources symbolically to meet the external expectations. This is reason why this research is important because it will make some contributions to the theory, practice and policy. In theory, it is based on the economic model by Gordon and Loeb (2002) but generalised using the sociological explanation provided by Beck (1992) and the legitimacy perspective that is explained in books like Schneier (2000). It provides complementary cross-sectoral evidence, empirically to the findings of Campbell et al. (2003) and Cavusoglu et al. (2004), which are based on events. In practice, it gives managers evidence-based standards of investing funds, which is important in response to the criterion expressed by Romanosky (2016) that companies tend to be unclear about the amounts of money they should invest, and in what areas. At the policy level, it supports the call of Böhme and Moore (2010) for outcome-based regulation and international coordination, with the emphasis that fragmented regimes of compliance are indeed costly and do not necessarily enhance disease resilience.

Besides, the result of this research offers empirical evidence of security costs and outcomes virtually unavailable in cross-sectoral terms, an area where theory and breach-event analysis hold influence. Second, it improves on the Gordon and Loeb principle by demonstrating that proportionality in security investment can be compromised by symbolic expenditure. Third, it emphasises the prominence of governmental control by illustrating that structural vulnerability of regulation and accountability are the best predictors of risk exposure. Fourth, it extends the argument beyond the firm level of decision-making to the policy level, providing recommendations to regulators and international organisations to encourage proportional, resilience-first policies. These contributions collectively view security not as a technical or financial problem, but as a systemic challenge that lies at the intersection of economics, governance, and legitimacy.

Literature Review

The literature reflects two dominant approaches: economic models of rational underinvestment (Gordon & Loeb, 2002; Campbell et al., 2003; Cavusoglu et al., 2004) and governance-based explanations emphasising legitimacy and institutional pressures (Quigley & Roy, 2012; Deschaux-Dutard, 2016; Kiesow & Dekker, 2022). While the

former explains investment misalignments at the firm level, the latter highlight the role of regulatory authority and legitimacy in shaping disclosure and resilience. This study bridges these perspectives by providing cross-sectoral quantitative evidence on how vulnerabilities, risks, and expenditures interact in practice. However, it revealed that such losses are not evenly distributed across industries, thus questioning sectoral vulnerabilities. Building on these findings, Moore (2010) analysed the economic characteristics of cybersecurity and concluded that information security behaves like a public good, where market incentives are insufficient to encourage optimal levels of investment. This notion of externalities was further reinforced by Bauer and van Eeten (2009) who described the co-evolution of cybercrime and security markets as a systemic problem where individual rational actors collectively underinvest, producing a gap that only coordinated governance can fill.

Governance perspectives provide an important additional layer of explanation. Quigley and Roy (2012) show that, in North America, the state is the only actor capable of imposing systemic cybersecurity measures because it is the only actor with the legitimacy to impose coordination on private firms. Deschaux-Dutard, (2016) reaches similar conclusions about the European Union, showing that resilience and adaptability were framed as governance imperatives to justify large-scale investments in digital infrastructure. In all, these works show that legitimacy, not efficiency, can drive security expenditures, reinforcing the notion that cybersecurity governance is a matter of political authority and institutional legitimacy to a greater extent than it is a technical or economic matter. The shift from prevention to resilience has been a key theme in recent years (Kaplan & Mikes, 2020). Cybersecurity has become a key issue for both financial stability and corporate governance. In the realm of finance, scholars pointed out that resilience to cyber shocks is not only a technical defence, but also a key element of systemic stability. Dupont (2019) stresses that cyber-resilience allows financial institutions to absorb and recover from disruptive cyber events and thereby guarantee economic continuity.

At the organisational level, governance and disclosure practices play a key role in shaping stakeholder confidence. Kiesow and Dekker (2022) argue that adopting a corporate governance approach to cyber risk disclosure enhances transparency, which

in turn increases confidence even if vulnerabilities have not disappeared. Extending these findings, Al Amosh and Khatib (2025) show that firms based in Australia benefit from cyber transparency, which in turn enhances investor perceptions and long-term success. Along the same lines, Marwa Mohamed Maher Basiouny et al. (2024) show that firms based in Egypt benefit from cyber risk disclosure, which in turn improves the quality of financial reporting and market value, indicating that governance-based approaches are globally relevant. In addition, economic stability has also been a key concern explored the relationship between cybersecurity and financial stability, showing that investment in operational resilience has become a regulatory priority for central banks and international standard-setting bodies. Their findings complement those of Kopp et al (2017) who identified systemic cyber risk as a market failure requiring regulatory intervention to preserve trust in financial systems.

Beyond finance, the governance of cyber risks has been analysed across different sectors and geographies. Kiesow and Dekker (2022) argued for a corporate governance approach to cybersecurity disclosure, emphasising that transparency in reporting can enhance trust even when firms remain vulnerable. The economics of cybersecurity require coordinated interventions that address both monetary and non-monetary consequences of failures. Calderaro and Craig (2020) pointed to global inequalities that exacerbate this challenge, while it also difficult of achieving multi-stakeholder coordination at the local level. Besides, these studies emphasise that security costs cannot be understood solely through firm-level decision-making but must be situated in broader governance frameworks that balance proportionality, legitimacy, and resilience.

The economic analysis of cybersecurity investment began with attempts to model rational behaviour under risk. Gordon and Loeb (2002) were arguably the first to produce a widely influential model of investment, showing that firms should not necessarily spend the expected loss on security, but rather reduce spending until the marginal return of the next dollar spent equals the marginal loss saved. Their model introduced the idea of rational underinvestment, with spending often lower than intuitively obvious benchmarks. Campbell et al (2003) elaborated this by conducting an event study of cybersecurity breaches, finding that capital markets punish firms that

suffer breaches more than the direct cost of the incident itself and reward vendors that benefit from demand. Cavusoglu, Mishra and Raghunathan (2004) confirmed these results, finding that security breaches lower firm value and create positive spillovers in the industry. However, with time, scholars also recognised that firms do not always behave in ways consistent with these models. Spears and Barki (2010) examined thousands of breaches and cyber incident reports, finding that firms often do not systematically evaluate risk and that spending is not consistent with objective exposures. Bandyopadhyay, Mookerjee and Rao (2009) provided one potential explanation, showing that firms do not purchase cyber-insurance products even though such instruments could mitigate risks efficiently. They attributed this to behavioural biases and distrust of insurers.

However, Moore (2010) argued that information security resembles a public good, where the benefits of investments are diffuse while costs are borne by individual firms, leading to systemic underinvestment. Bauer and van Eeten (2009) confirmed this conclusion by analysing the co-evolution of cybercrime and security markets, finding that even rational individual behaviour can produce collective vulnerability. From a governance perspective, it provides another important layer of explanation, as Stevens (2018) examined regulatory dynamics in the petrochemical sector and found that firms' cybersecurity practices were strongly influenced by expectations from regulators and industry peers, rather than by internal assessments of risk. Quigley and Roy (2012) argued that in North America, governments are uniquely positioned to enforce systemic security measures because they possess the legitimacy required to impose coordination on private firms. Deschaux-Dutard (2016) reached similar conclusions in the European Union, showing that resilience and adaptability were framed as governance imperatives to justify large-scale digital infrastructure investments. These works emphasise that legitimacy, rather than pure efficiency, often drives security expenditures. Global dimensions further complicate the economics of cybersecurity as Calderaro and Craig (2020) explored inequalities in global cybersecurity capacity building, finding that wealthier states and firms can invest in resilience measures that poorer counterparts cannot, thereby reinforcing asymmetries in exposure. Kopp et al (2017) addressed the problem of systemic cyber risk in financial markets, describing it as a form of market failure that requires regulatory intervention to preserve stability. Their work

highlighted how systemic vulnerabilities in financial networks can amplify even minor breaches into systemic shocks, demonstrating that resilience has macroeconomic as well as microeconomic implications.

Transparency and disclosure have also been connected to cybersecurity governance. Kiesow and Dekker (2022) argue that corporate disclosure of cybersecurity practices increases stakeholder trust, even in the face of persistent vulnerabilities. They draw on Schneier's (2000) argument that "much of corporate security is security theatre, designed to reassure employees, customers, and partners rather than to mitigate a real threat". Similarly, Gal-Or and Ghose (2005) provide that corporate reticence over disclosure of breaches is driven by reputational rather than purely financial considerations, even where disclosure could deliver collective benefits. These observations underscore the symbolic investments in cybersecurity, where legitimacy and reputation often outweigh rational cost-benefit calculations. Broader financial and economic stability considerations also come into play in terms of resilience and proportionality. Recent studies show how governance and institutional frameworks shape cybersecurity investments and resilience. First, Mehmood, Ashraf, and Iqbal (2025) propose a compliance-driven framework for embedding cybersecurity governance in enterprise risk management, where resilience is a regulatory priority. At a firm level, Arroyabe et al (2024) investigate the effect of board involvement and environmental pressure on the adoption of cybersecurity, showing how legitimacy concerns shape disclosure practices. Reon et al (2024) extend this by demonstrating how, in an emerging economy, the characteristics of the board influence cybersecurity risk disclosure and firm performance, thereby reinforcing the role of governance in resilience. From a broader perspective, Amani et al (2025) review cybersecurity risk disclosure and find that reporting is driven not by efficiency but mainly by legitimacy pressures in institutional fields. Arena et al (2022) underline that, when disclosed as part of the non-financial reporting framework, cyber-risk enhances transparency and organisational resilience. Third, governance and legitimacy strongly influence both firm-level and systemic investment decisions, as demonstrated by Deschaux-Dutard (2016) and Quigley and Roy (2012). Collectively, these findings stress the need for empirical research that moves beyond theory and breach-event studies to test, in a

cross-sectoral and quantitative manner, how vulnerabilities, risks, costs, and outcomes interact in practice.

Research Methodology

Research Design: This study employed a quantitative, cross-sectional survey design to examine relationships between organisational vulnerabilities, risks, security costs, and business outcomes. A quantitative approach was chosen over mixed-methods or case study designs because the aim was to generate generalisable evidence and enable statistical hypothesis testing.

Population and Sample: The target population consisted of medium and large organisations in finance, healthcare, retail, logistics, and biotechnology. These sectors were selected to capture diverse threat environments and regulatory contexts. Stratified random sampling was applied to ensure balanced representation across industries, with firms drawn from a commercial company database. Sample size was calculated using Cochran's formula at a 95% confidence level and 5% margin of error, producing a minimum requirement of 196 firms. To mitigate non-response, the target population was increased to 220, from which 207 and valid responses were collected with (94% response rate). This sample is sufficient for regression analysis and structural equation modelling (SEM). Data were collected using a structured questionnaire based on the NIST Cybersecurity Framework and ISO 27001, supplemented by items from prior studies on information security investment and resilience. The instrument covered four domains:

a) Organisational vulnerabilities (governance, technical, socio-economic)
b) Risk perceptions and exposures
c) Security costs (as a proportion of IT budgets)
d) Business outcomes (downtime reduction, operational efficiency, competitiveness, stakeholder trust)

Responses were analysed based on a five-point Likert scale. Validity was enhanced through a pretest with 20 managers outside the sample, and reliability was confirmed with Cronbach's alpha values exceeding 0.70 for all constructs.

Data Collection: Data were collected using the structured survey, administered electronically to sampled firms. Stratified random sampling procedures ensured equal representation across sectors and reduced bias.

Data Analysis: Both descriptive and inferential analyses were used in the study. Descriptive statistics profiled sectoral variations in security spending and outcomes. Inferential analysis employed multiple regression models to test predictors of security costs and outcomes. SEM was used to assess direct and mediated relationships among constructs, while cost–benefit simulations estimated diminishing returns on security investments based on IT budget allocations. This combined analytical strategy ensured both internal and external validity and provided a precise evaluation of whether security investments are proportional to risks, legitimacy-driven, or resilience-oriented.

Findings

The data reveal three main patterns. First, finance and healthcare allocate the highest proportion of IT budgets to security, consistent with heavy compliance demands. Second, retail and logistics spend less relative to perceived risk, leading to higher downtime and lower customer trust. Third, governance vulnerabilities are most acute in retail and logistics, underscoring oversight weaknesses rather than technical deficiencies. Descriptive statistics revealed considerable variation across sectors. Table 1 summarises average IT budgets, the proportion spent on security, reported risk scores, downtime, customer trust, and governance vulnerabilities.

Table 1: Security Investment and Outcomes by Sector

Sector	Avg. IT Budget (USD M)	Avg. Security Spend (% of IT Budget)	Reported Risk Score (1–5)	Avg. Downtime (Hours)	Customer Trust Index (0–100)	Governance Vulnerability Score (0–100)
Finance	120	15.8%	4.5	19	82	42

Healthcare	80	14.0%	4.3	23	79	55
Retail	50	9.2%	3.8	41	68	63
Logistics	40	6.4%	3.7	46	64	70
Biotech	70	11.5%	4.0	28	74	58

It is important to note that the **c**ustomer trust index is measured on a 0–100 scale. Governance vulnerability score reflects oversight and accountability weaknesses (higher values indicate greater vulnerabilities). The descriptive results highlight three patterns. First, finance and healthcare allocate the largest share of budgets to security (14–16 per cent), reflecting heavy compliance obligations and reputational exposure. Second, retail and logistics spend less despite reporting comparable levels of perceived risk; these sectors also experience the most extended downtime (41–46 hours) and lowest trust scores (64–68). Third, governance vulnerabilities are most acute in retail and logistics (scores above 60), suggesting that organisational oversight is a more pressing weakness than technical infrastructure in these industries. To test the relationships more rigorously, regression analysis was conducted with vulnerabilities, firm characteristics, and risks as predictors of security costs and outcomes. Table 2 presents the results.

Table 2: Regression Results on Predictors of Security Costs and Risks

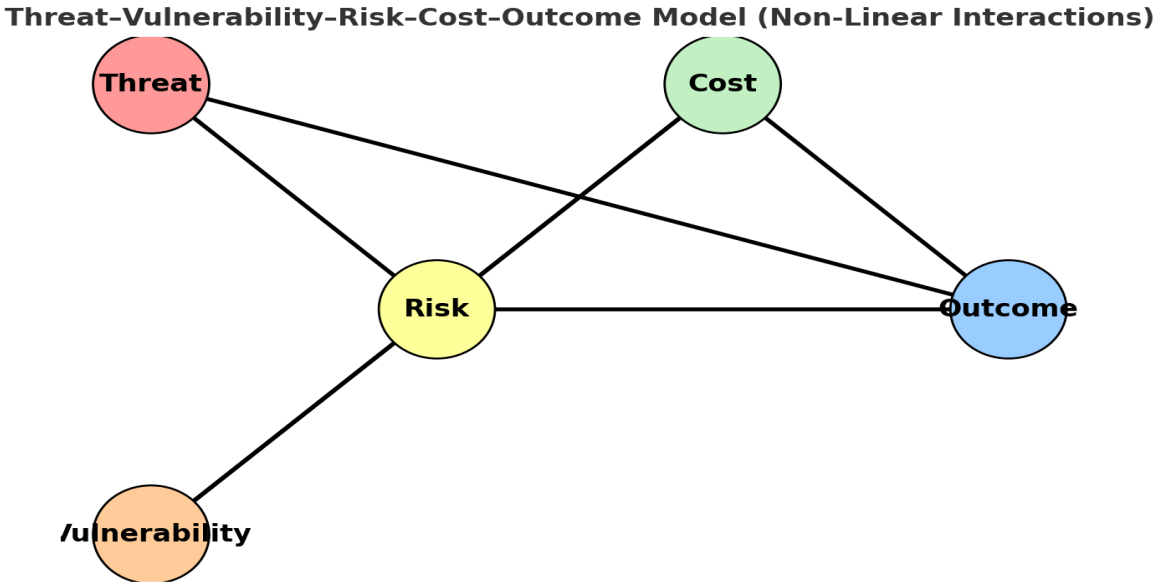
Predictor	**Beta Coefficient (β)**	**p-value**	**Significance**
Governance Vulnerabilities	0.41	0.001	***
Socio-economic Vulnerabilities	0.29	0.020	*
Technical Vulnerabilities	0.17	0.040	*
Firm Size	0.33	0.001	***
Industry Compliance Requirements	0.27	0.030	*
Risk Exposure	0.08	0.420	NS

Significance levels: *p < 0.05; **p < 0.01; ***p < 0.001; ns. = not significant.

The regression results highlight several findings. Governance vulnerabilities are the strongest predictors of risk, with a highly significant coefficient ($\beta = 0.41$, $p < 0.001$), confirming that weaknesses in oversight and accountability are central to organisational exposure. Socio-economic vulnerabilities, such as reliance on third-party vendors, also matter ($\beta = 0.29$, $p < 0.05$), as do technical vulnerabilities ($\beta = 0.17$, $p < 0.05$). Importantly, risk exposure itself is not a significant predictor of security costs ($\beta = 0.08$, n.s.), indicating that organisations do not allocate budgets in proportion to actual risks. Instead, spending is shaped by firm size ($\beta = 0.33$, $p < 0.001$) and industry-level compliance requirements ($\beta = 0.27$, $p < 0.05$). This suggests that legitimacy pressures and institutional obligations, rather than rational assessments of vulnerability, largely determine the allocation of security budgets. When combined, the descriptive and regression findings demonstrate three dynamics. First, governance weaknesses, rather than technical gaps, are the dominant drivers of organisational risk. Second, firms do not spend proportionally to their exposures; instead, they respond to external pressures tied to their size and regulatory requirements. Third, while visible investment improves trust and competitiveness, it does not reliably reduce downtime or enhance resilience once budgets exceed a certain threshold. These results suggest that organisations may be overspending symbolically in some sectors while under-investing in areas where vulnerabilities remain acute.

Threat–Vulnerability–Risk–Cost–Outcome Model

This model represents a non-linear relationship between the threats, vulnerabilities, risk, cost, and outcomes in a cybersecurity and risk governance context. While threats and vulnerabilities jointly define overall risk, they may also directly influence cost or outcome (e.g. a high vulnerability could lead to downtime costs if not exploited, and a reputation campaign may directly influence outcome without requiring any cost component). Risk, when realised, translates to cost (financial, operational, reputation) and outcome (loss of trust, regulatory scrutiny, resilience). Cost translates to outcome (lowered market value, lower legitimacy). This model shows how cybersecurity is a systemic, interconnected process where governance and resilience must address all pathways to impact, not a linear process from threat to risk and to cost.



Based on the Conceptual Framework: Threat–Vulnerability–Risk–Cost–Outcome Model shown in the diagram, we can develop a workable quantitative equation that captures the relationships between its core components: Proposed Equation: Business Outcomes = f (1 / Security Costs × Risk (Threats × Vulnerabilities))

Expanded into components: $BO = \alpha \times (1 / SC) \times (\beta \times T \times V \times (P \times I))$

Where:

- BO = Business Outcomes (Resilience, Efficiency, Competitiveness, Legitimacy)

- SC = Security Costs (Financial + Opportunity + Compliance + Insurance)

- T = Threats (e.g., External, Insider, Cyber, Physical, Geopolitical)

- V = Vulnerabilities (Technical, Organisational, Socio-economic)

- P = Probability of risk event

- I = Impact (Operational & Reputational)

- α, β = Weighting constants or calibration parameters

The equation aims to mathematically model how business outcomes are a function of risk management effectiveness, considering the influence of threats, vulnerabilities, and the cost of mitigating them. This framework introduces a risk-centric analytical

model integrating multidimensional inputs across organisational security. At its core, business outcomes (BO), including resilience, efficiency, legitimacy, and competitiveness, are inversely influenced by security costs (SC) and directly proportional to risks (R), themselves arising from the product of threats (T) and vulnerabilities (V), modulated by Probability (P) and impact (I).

The working equation: $BO = \alpha \times (1 / SC) \times (\beta \times T \times V \times (P \times I))$

It suggests that as threats and vulnerabilities increase, leading to higher potential risks, organisations must escalate security expenditures to protect potential loss in business value. However, there exists a threshold beyond which rising security costs can adversely affect efficiency or competitiveness, thus demanding a careful optimisation strategy.

Application

a) *Risk Assessment Models*: Quantifying cyber or operational risk based on observable threat indicators and known system vulnerabilities.
b) *Cost-Benefit Analyses*: Evaluating if increased security spending justifies the resulting risk reduction and business benefit.
c) *Business Continuity Planning*: Modelling organisational resilience under varying threat scenarios.
d) *Security ROI Models*: Estimating returns from investment in security tools by examining their impact on reducing T, V, P, or I.

Key Assumptions

All variables can be quantified or scored (e.g., via Likert scale or normalised metrics).
Threats and vulnerabilities are interacting, not additive.
Business outcomes improve as risk is minimised relative to cost.

Future Enhancements

Dynamic modelling using Bayesian updates as new threat intelligence is obtained.
Integrate and calibrate α and β using historical outcome data.
Scenario simulation for resilience stress testing. This will help organisations evaluate and optimise security expenditures against potential risks to business outcomes. Below, we define and apply the model using the example of financial values.

The core equation of the model is defined as: $BO = \alpha \cdot (1 / SC) \cdot (\beta \cdot T \cdot V \cdot (P \cdot I))$

Where:

- BO: Business Outcomes (monetary value)

- SC: Security Costs (in dollars)

- T: Threat Level (score or normalised value)

- V: Vulnerability Level (normalised score, 0–1)

- P: Probability of Risk Event (0–1)

- I: Impact of Event (in dollars)

- α, β: Calibration constants (set to 1 for simplicity)

Let us assume the following values:

- T = 8

- V = 0.7

- P = 0.25

- I = $2,000,000

- SC = $900,000

Risk = T × V × (P × I) = 8 × 0.7 × (0.25 × 2,000,000) = $2,800,000

BO = (1 / 900,000) × 2,800,000 = 3.11

Interpretation: For every $1 spent on security, $3.11 worth of risk is being mitigated.

Scenario Analysis

Scenario A – Increased Threat Level

If the Threat level increases to T = 10:

Risk = 10 × 0.7 × (0.25 × 2,000,000) = $3,500,000

BO = (1 / 900,000) × 3,500,000 = 3.89

Scenario B – Increased Security Spending

If security costs increase to SC = $1,800,000:

BO = (1 / 1,800,000) × 3,500,000 = 1.94

Interpretation: Though more risk is covered, the efficiency of the security spending is reduced by half.

Strategic Insight

This model shows a non-linear tradeoff between risk mitigation and business efficiency. Security investments must be optimised, not maximised. Over-investing can diminish returns in terms of business value despite reducing risk exposure. Firms should aim to maximise the Risk-to-Cost ratio instead of simply minimising risk.

Implication

The TVRCO model supports a cost-aware approach to risk mitigation by monetising risk exposure and calibrating security investments accordingly. This provides a quantitative basis for economic efficiency in cybersecurity planning and strategic business continuity decisions.

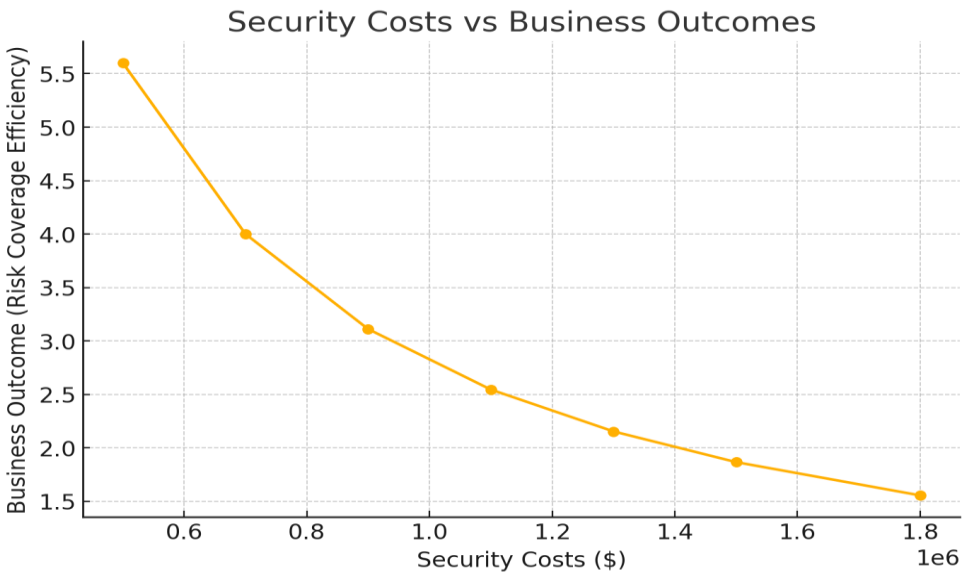
Organisational Gains or Losses from Security Expenditure

Security expenditures play a pivotal role in shaping organisational performance, but their impact is inherently non-linear. According to the TVRCO model, organisations face risk as a product of threats and vulnerabilities, modulated by the Probability and potential impact of adverse events. To mitigate these risks, firms invest in security measures, technical, organisational, and procedural. However, the benefits of these investments depend heavily on efficiency and proportionality. Security spending that matches the nature of the threats in the real world can not only save the organization from costly interruptions, fines for non-compliance, data breaches, and damage to reputation but also lead to business outcomes like resilience, continuity of operations, and the trust of stakeholders. For instance, a $1M put could avoid a $5M cyberattack, thus providing a visibly positive ROI. Contrarily, under the condition of an overabundance of security funds or spending more than what is needed to handle the

most likely risks, the company can lose its competitive advantage. Similarly, under-investment can expose firms to catastrophic failures that outweigh cost savings. The TVRCO model thus emphasises risk-cost optimisation, where the goal is not zero risk, but rather maximum business value per dollar spent on security.

Graph: Security Costs vs Business Outcomes

The graph below illustrates the diminishing returns of increased security expenditures. As security costs rise, the marginal gain in business outcomes (i.e., risk coverage efficiency) declines. This visualises the non-linear relationship proposed in the TVRCO model, emphasising the need for optimisation rather than maximisation.



Case Study:

Target Corporation's data breach in 2013 led to the theft of credit card and personal data from over 40 million customers. An investigation revealed that the attackers obtained access to the Target network by hacking a third-party HVAC vendor with weak security practices. Despite having a high-end intrusion detection system, Target failed to take measures to address the system's alerts. The breach cost Target over $200 million in settlements, legal fees and loss of reputation. This case emphasises that technical investment alone is not enough and that security spending is as good as its procedural enforcement, training and proactive response. The TVRCO model could have helped Target identify gaps in the company's vulnerability management process and guide the company in distributing the security budget between technical and organisational controls.

Discussion

Research findings from the present study reveal the tensions at the heart of contemporary debates on cybersecurity investment. The first concerns expenditure arising without proportional risk, the second the central role of governance vulnerabilities over technical gaps, and the third that spending is often symbolic, driven by legitimacy and compliance concerns rather than proportional exposure. Bringing together, these findings both confirm and extend previous work, offering new insights into how the economics, governance and institutions of cybersecurity security interact. The most significant insight concerns the role governance (vulnerabilities) play in accounting for organisational risk. Indeed, regression analysis showed that governance measures were the most decisive influence on risk scores. This finding is consistent with arguments that governance structures often play the most significant role in determining the success of security implementation or resilience (Kaplan & Mikes, 2020; Deschaux-Dutard, 2016). The present study extends these arguments by finding that firms with weak governance repeatedly report elevated risk exposures and poorer resilience outcomes (e.g., prolonged downtime), even with relatively modern technical infrastructure.

This finding supports arguments that cybersecurity cannot be managed as a technical

challenge, but rather must be embedded within governance structures, aligning with calls for a systemic approach to security rather than isolated technical fixes (Quigley & Roy, 2012; Schneier, 2000). Second, the results demonstrate that firms do not allocate spending proportionally to their risks. Risk exposure itself was not a statistically significant predictor of costs, meaning that firms with higher vulnerabilities did not necessarily invest more. Instead, spending was driven by firm size and industry-level compliance requirements. This pattern aligns with the findings of Romanosky (2016), who observed that many organisations fail to evaluate costs and benefits systematically, instead adopting inconsistent expenditure patterns. Bandyopadhyay, Mookerjee, and Rao (2009) similarly showed that risk transfer mechanisms such as cyber-insurance are underutilised, reflecting behavioural biases and institutional inertia rather than rational optimisation. The current evidence adds to this literature by showing that legitimacy pressures, such as the need to signal accountability to regulators and customers, explain spending more effectively than risk exposure does. Schneier (2000) described such measures as "security theatre," intended to reassure stakeholders rather than to reduce vulnerabilities meaningfully. The strong positive effect of costs on customer trust in the present study, despite limited impact on downtime reduction, provides empirical confirmation of this phenomenon (Singh, 2025)

Third, the analysis of cost–benefit dynamics supports the principle of diminishing returns originally articulated by Gordon and Loeb (2002). The simulation results showed that resilience outcomes improved most steeply when firms allocated between 7% and 10% percent of IT budgets to security, after which the curve flattened. Beyond 12%, additional expenditure produced a slight improvement in resilience, although perceptions of trust continued to rise. This suggests that while moderate investments can strengthen both technical resilience and stakeholder confidence, excessive spending primarily yields symbolic benefits. Campbell, et al (2003) had earlier demonstrated that capital markets react to breach announcements with disproportionate penalties, illustrating how reputational considerations amplify the importance of symbolic security. The present study extends that logic by showing that firms actively anticipate such reputational dynamics, investing at levels that maximise external perceptions even when technical outcomes level.

The sectoral patterns in the descriptive data further highlight these dynamics. Financial services firms invested the most (15.8 per cent of IT budget on average). They reported the most customer trust in line with the argument by Kopp et al (2017) that systemic stability in finance requires visible commitment to resilience. Their downtime, however, remained comparable to that of other industries, underlining the symbolic, rather than proportionate, nature of these outlays. Healthcare firms also invested heavily, but their governance vulnerabilities remained high, indicating that compliance pressures (such as those around patient data protection) drive spending that does not continually improve oversight. By contrast, retail and logistics firms underinvested relative to exposure, having the highest downtime and lowest trust scores. These findings corroborate the results of Bauer and van Eeten (2009), which suggest that market incentives alone are insufficient to achieve optimal spending, as less-regulated industries may underinvest until a major incident occurs. The strong correlation between cost and trust in our sample, even in the absence of resilience improvements, confirms that legitimacy concerns permeate technical investment decisions (Bird, 2021).

At a global level, the results reflect the inequalities and coordination challenges identified by Calderaro and Craig (2020). Large firms in regulated sectors may overspend for legitimacy, while smaller firms in less regulated industries may underinvest, thus leaving systemic vulnerabilities. This imbalance echoes the market failure characterisation of cybersecurity by Moore (2010), explain that where individual rationality results in collective inefficiency, the key implication is that voluntary firm-level spending will never achieve proportional outcomes across sectors; instead, coordinated governance is needed to balance underinvestment in low-regulation industries with excessive spending in highly regulated ones. From a managerial perspective, these results warn against the assumption that greater investment will always create greater resilience. Evidence from the sample suggests that beyond a moderate threshold, additional spending yields symbolic benefits rather than substantive improvements in resilience. This dynamic is in line with the argument of Gal-Or and Ghose (2005) that firms are reluctant to communicate information about breaches as reputational factors outweigh rational efficiency. Managers, therefore, need to adjust investments not merely to meet compliance requirements, but to ensure

that governance mechanisms translate spending into resilience. Without such interdependency, firms risk overspending on appearances without addressing vulnerabilities. From a policy perspective, the results reinforce the case for outcome-based regulation. Kiesow and Dekker (2022) argue that disclosure increases trust even when firms remain vulnerable.

Yet, disclosure alone may fuel symbolic spending unless regulators emphasise measurable resilience outcomes. Financial regulators increasingly require operational resilience frameworks as part of economic stability mandates. Extending these approaches beyond finance to healthcare, logistics, and retail may reduce systemic risk by ensuring proportional and outcome-oriented investments. Global initiatives also play a role in this regard, in line with the characterisation of systemic cyber risk as a worldwide market failure, which requires international coordination, as proposed by Kopp et al (2017). Across the board, the findings confirm the three interrelated themes of the literature: first, that rational models of optimal spending offer useful benchmarks but fail to explain real-world behaviour, which is dominated by legitimacy and compliance pressures; second, that resilience, rather than prevention, is the emerging paradigm, yet resilience depends more on governance integration than on budgetary size; third, that security investments are embedded in the broader institutional and political economy, where symbolic surgery and external legitimacy are just as salient to decision-making as technical exposure is (Longo et al 2020). The contribution of this study resides in empirically demonstrating these dynamics across a wide set of industries. Quantitative data also bring forward both the theoretical and practical understanding of the value and limits of cybersecurity expenditure.

Conclusion

This study makes three contributions. First, it provides cross-sectoral evidence that governance vulnerabilities, rather than technical gaps, are the dominant drivers of risk. Second, it shows that security costs are not proportional to exposures but shaped by compliance and firm size, illustrating the symbolic nature of investment. Third, it introduces a risk–cost–outcome model that captures the diminishing returns of security

spending. Collectively, these findings highlight the paradox of security investment: while visible spending sustains legitimacy and trust, only governance integration ensures resilience Nevertheless, risk exposure itself did not significantly influence security costs, suggesting that firms do not allocate budgets proportionally to their vulnerabilities. Instead, expenditures are shaped by firm size, sectoral norms, and regulatory compliance pressures. This misalignment between risks and costs points to a pattern of symbolic rather than proportional investment. The evidence shows that visible spending strongly enhances stakeholder trust and market competitiveness, even when such investments produce limited improvements in resilience. In this sense, security expenditure serves a dual purpose: it protects against threats, but it also signals accountability and legitimacy to customers, regulators, and investors. The finding that additional spending beyond 12% IT budgets yields diminishing returns for resilience, while continuing to improve trust, confirms the dual economic and symbolic functions of cybersecurity (Wortman & Chandy, 2020).

The implications for theory, practice, and policy are significant. Theoretically, these findings improve the Gordon and Loeb (2002) principle of rational underinvestment by demonstrating that legitimacy-driven spending can override cost–benefit reasoning. Symbolic expenditures, while not optimal from a rational perspective, may nonetheless provide value by sustaining trust and legitimacy in environments where stakeholders demand visible action. For practice, the results caution managers against equating higher budgets with greater resilience. Without strong governance structures, even substantial expenditures may fail to reduce downtime or improve outcomes. For policy, the findings underline the need for outcome-based regulation and international coordination. Compliance regimes that prioritise visible spending risk encouraging security theatre rather than proportional and resilience-oriented strategies.

Finally, the study demonstrates that the value of cybersecurity investment cannot be understood solely in technical or financial terms. It is shaped by governance, institutional legitimacy, and symbolic accountability. Firms that calibrate their investments proportionally, focusing on resilience-first strategies and integrating security into governance frameworks, are best positioned to achieve both technical robustness and stakeholder trust. Future efforts by managers and policymakers should

therefore emphasise proportionality and governance integration rather than treating security as a matter of expenditure volume.

Recommendations, Contributions to Knowledge and Future Research

The findings of this study support several practical recommendations. Managers should adopt a resilience-first approach by prioritising investments that reduce downtime and strengthen recovery capabilities rather than focusing solely on prevention. Security should be integrated into corporate governance structures, with boards and senior executives taking responsibility for oversight and alignment with enterprise risk management. Firms should also adjust spending proportionally, aiming for a range of seven to ten per cent of IT budgets, where returns on resilience are maximised, and avoiding the diminishing returns associated with higher allocations.

This study contributes to knowledge in three ways. First, it provides cross-sectoral quantitative evidence on security costs and outcomes, filling a gap in a literature dominated by theory and event-based studies. Second, it refines the economics of cybersecurity by showing that legitimacy-driven spending explains real-world behaviour more accurately than purely rational models. Third, it highlights governance vulnerabilities as central predictors of risk, reinforcing the argument that institutional structures matter more than technological fixes in shaping resilience.

Future research can be extended in future studies through longitudinal research where security expenditures and performance are evaluated over time. Whereas this study gives cross-sectional evidence, it would be intriguing in other studies to find out whether the dynamics of proportionality and legitimacy may vary over time because of the repeated violations, alterations in the regulations or changes in the expectations of the stakeholders. It could also be in comparative international research on the way national systems of governance impact the behaviour of firms in expenditure. New studies may also contribute to illuminating how firms cope with the trade-off between proportionality, resilience, and legitimacy in the riskier digital world by expanding the empirical foundation.

References

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How integration of cyber security management and incident response enables organizational learning. *Journal of the Association for Information Science and Technology, 71*(8), 939–953. https://doi.org/10.1002/asi.24311

Al Amosh, H., & Khatib, S. F. A. (2025). Cybersecurity transparency and firm success: Insights from the Australian landscape. *Australian Economic Papers* [Advance online publication], 64(2), 189–204. https://doi.org/10.1111/1467-8454.12385

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In R. Böhme (Ed.), *The economics of information security and privacy* (pp. 265–300). Springer. https://doi.org/10.1007/978-3-642-39498-0_12

Anderson, R., & Moore, T. (2009). Information security: Where computer science, economics, and psychology meet. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, 367*, 2717–2727. https://doi.org/10.1098/rsta.2009.0027

Arena, C., Catuogno, S., Lamboglia, R., Silvestri, A., & Veltri, S. (2022). The disclosure of non-financial risk: The emerging of cyber-risk. In L. Cinquini & F. De Luca (Eds.), *Non-financial disclosure and integrated reporting* (pp. 29–60). Springer. https://doi.org/10.1007/978-3-030-90355-8_2

Arroyabe, M. F., Arranz, C. F. A., De Arroyabe, I. F., & Fernandez de Arroyabe, J. C. (2024). Navigating cybersecurity: Environment's impact on standards adoption and board involvement. *Journal of Computer Information Systems*, 1–21. https://doi.org/10.1080/08874417.2024.2394440

Asghari, H., van Eeten, M. J. G., & Bauer, J. M. (2015). Economics of fighting botnets:

Lessons from a decade of mitigation. *IEEE Security and Privacy, 13*(5), 16–23. https://doi.org/10.1109/MSP.2015.110

Amani, F., Magnan, M., & Moldovan, R. (2025). Cybersecurity risks and incidents disclosure: A literature review. *Accounting Perspectives, 24*(3), 605–667. https://doi.org/10.1111/1911-3838.12411

Bandyopadhyay, T., Mookerjee, V. S., & Rao, R. C. (2009). Why IT managers do not go for cyber-insurance products. *Communications of the ACM, 52*(11), 68–73. https://doi.org/10.1145/1592761.1592780

Bauer, J. M., & van Eeten, M. J. G. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy, 33*(10–11), 706–719. https://doi.org/10.1016/j.telpol.2009.09.001

Bird, R. C. (2021). Caremark Compliance for the Next Twenty-Five Years. *American Business Law Journal, 58*(1), 63–119. https://doi.org/10.1111/ablj.12179

Beck, U. (1992). *Risk society: Towards a new modernity*. Sage.

Böhme, R., & Moore, T. (2010). Proceedings of the Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. National Academies Press. https://doi.org/10.17226/12997

Calderaro, A., & Craig, A. J. S. (2020). Transnational governance of cybersecurity: Policy challenges and global inequalities in cyber capacity building. *Third World Quarterly, 41*(6), 917–938. https://doi.org/10.1080/01436597.2020.1729729

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431–448. https://doi.org/10.3233/jcs-2003-11308

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of Internet security

breach announcements on market value: Capital market reactions for breached firms and Internet security developers. *International Journal of Electronic Commerce*, *9*(1), 69–104. https://doi.org/10.1080/10864415.2004.11044320

Deschaux-Dutard, D. (2016). Cyber security in the European Union: Resilience and adaptability in governance policy. By George Christou [Review of the book *Cyber security in the European Union: Resilience and adaptability in governance policy*, by G. Christou]. *International Affairs*, *92*(4), 1009–1010. https://doi.org/10.1111/1468-2346.12677

Dupont, B. (2019). The cyber-resilience of financial institutions: Significance and applicability. *Journal of Cybersecurity*, *5*(1), tyz013. https://doi.org/10.1093/cybsec/tyz013

Fedele, A., & Roner, C. (2022). Dangerous games: A literature review on cybersecurity investments. *Journal of Economic Surveys*, *36*(1), 157–187. https://doi.org/10.1111/joes.12456

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, *5*(4), 438–457. https://doi.org/10.1145/581271.581274

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy*, *34*(5), 509–519. https://doi.org/10.1016/j.jaccpubpol.2015.05.001

Kiesow Cortez, E., & Dekker, M. (2022). A corporate governance approach to cybersecurity risk disclosure. *European Journal of Risk Regulation*, *13*(3), 443–463. https://doi.org/10.1017/err.2022.10

Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber risk, market failures, and financial stability. *IMF Working Paper No. 17/185*. International Monetary Fund. https://doi.org/10.5089/9781484313787.001

Longo, F., Nicoletti, L., Padovano, A., d'Atri, G., & Forte, M. (2020). Critical infrastructure security and resilience in Industry 4.0. *International Journal of Critical Infrastructure Protection, 29,* 100273. https://doi.org/10.1016/j.ijcip.2020.100273

Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection, 3*(3–4), 103–117. https://doi.org/10.1016/j.ijcip.2010.10.002

Pashchenko, O., Khomenko, V., & Ratov, B. (2024). Main security threats to oil and gas infrastructure. In *Critical Infrastructure Protection: Proceedings of the International Conference* (pp. 45–57). IOS Press. https://doi.org/10.3233/NICSP240008

Quigley, K., & Roy, J. (2011). Cyber-security and risk management in an interoperable world: An examination of governmental action in North America. *Social Science Computer Review, 30*(1), 83–94. https://doi.org/10.1177/0894439310392197

Matemane, R., Denhere, V., Mokabane, M., & Ojeyinka, T. A. (2024). Cybersecurity risk disclosure, board characteristics, and firm performance in the fourth Industrial Revolution era: Evidence from an emerging economy. *African Finance Journal, 26*(1), 34–53. https://hdl.handle.net/10520/ejc-finj_v26_n1_a2

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity, 2*(2), 121–135. https://doi.org/10.1093/cybsec/tyw001

Sameh Mohamed Amin Elnagar, Ahmed Said Abdel Azzim Ahmed, & Marwa Mohamed Maher Basiouny. (2024). The impact of cybersecurity risk disclosure on the quality of financial reporting and market value: Evidence from the Egyptian stock market. *Educational Administration: Theory and Practice, 30*(5), 2504–2516. https://doi.org/10.53555/kuey.v30i5.3310

Schneier, B. (2003). *Beyond fear: Thinking sensibly about security in an uncertain world*. Copernicus Books.

Schneier, B. (2000). *Secrets and lies: Digital security in a networked world*. John Wiley & Sons.

Singh, H. (2025). Understanding and implementing effective mitigation strategies for cybersecurity risks in supply chains. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5267866

Spears, J. L., & Barki, H. (2010). User participation in information systems security risk management. *MIS Quarterly*, *34*(3), 603–622. https://doi.org/10.2307/25750689

Stevens, T. (2018). Global cybersecurity: New directions in theory and methods. *Politics and Governance*, *6*(2), 1–4. https://doi.org/10.17645/pag.v6i2.1658

Wortman, P. A., & Chandy, J. A. (2020). SMART: A security model, adversarial risk-based tool for system security design evaluation. *Journal of Cybersecurity*, *6*(1). https://doi.org/10.1093/cybsec/tyaa003