http://dx.doi.org/10.18623/rvd.v23.6582

A QUALITATIVE CROSS-SECTOR ANALYSIS OF CYBER RESILIENCE MATURITY IN MALAYSIAN FINANCIAL AND MANUFACTURING FIRMS

UMA ANÁLISE QUALITATIVA INTERSETORIAL DA MATURIDADE DA RESILIÊNCIA CIBERNÉTICA EM EMPRESAS FINANCEIRAS E MANUFATUREIRAS DA MALÁSIA

Article received on: 1/16/2026
Article accepted on: 4/15/2026

Sathiyamoothri Palaipan*
***Universiti Teknikal Malaysia Melaka (UTeM), Melaka, Malaysia
Orcid: https://orcid.org/0009-0001-2745-4606
sathism@hotmail.com

Norain Ismail*
***Universiti Teknikal Malaysia Melaka (UTeM), Melaka, Malaysia
Orcid: https://orcid.org/0000-0003-4787-0778
norain@utem.edu.my

Sazelin Arif*
***Universiti Teknikal Malaysia Melaka (UTeM), Melaka, Malaysia
Orcid: https://orcid.org/0000-0001-6145-192X
sazelin@utem.edu.my

The authors declare that there is no conflict of interest

Abstract
Malaysia's financial services and manufacturing sectors form the core of the nation's economy, with both industries rapidly digitising. The business operations to manufacturing plants expand into cyberspace, where they become intertwined with digital frameworks. Consequently, cyber risk no longer resembles isolated information technology (IT) issue but pose significant challenges to fundamental business activities. Therefore, cybersecurity becomes crucial in an organization's risk management framework to protect the assets and operations. This study examines how firms in the financial and manufacturing sectors conceptualise, govern and operationalise cyber resilience, paying particular attention to how sector-specific regulatory environments influence differences in maturity levels among these industries. A qualitative document analysis of Annual and Sustainability Reports from listed companies is utilized. The researcher reads and codes these firms' descriptions of technology, cybersecurity and resilience and subsequently interpret those descriptions through a socio-technical analysis based on a three-layered framework. The findings reveal a contrast between the two sectors. The financial institutions highlight cyber risk as a business priority and guided by Bank Negara Malaysia's Risk Management in Technology (RMiT) policy.

Resumo
Os setores de serviços financeiros e manufatura da Malásia constituem o núcleo da economia do país, estando ambos em rápida digitalização. As operações comerciais das fábricas se estendem ao ciberespaço, onde se entrelaçam com as estruturas digitais. Consequentemente, o risco cibernético não se assemelha mais a uma questão isolada de tecnologia da informação (TI), mas representa desafios significativos para as atividades comerciais fundamentais. Portanto, a segurança cibernética torna-se crucial na estrutura de gestão de riscos de uma organização para proteger os ativos e as operações. Este estudo examina como as empresas dos setores financeiro e manufatureiro conceituam, governam e operacionalizam a resiliência cibernética, prestando atenção especial à forma como os ambientes regulatórios específicos de cada setor influenciam as diferenças nos níveis de maturidade entre essas indústrias. É utilizada uma análise documental qualitativa de Relatórios Anuais e de Sustentabilidade de empresas listadas em bolsa. O pesquisador lê e codifica as descrições dessas empresas sobre tecnologia, segurança cibernética e resiliência e, subsequentemente, interpreta essas descrições por meio de uma análise sociotécnica baseada em uma estrutura de três camadas. Os resultados revelam um contraste entre os dois

Meanwhile, manufacturing firms has no sector-specific regulation and frequently discuss their futuristic and high-tech upgrade plans, but say little about the cyber resilience of these ventures. This research suggests that sector-specific regulation is a primary driver for the consistent formalisation of cyber risk narratives in finance and indicates areas for boards, regulators and policymakers to explore as these risks extend into cyber-physical manufacturing scenarios.

Keywords: Malaysia. Digitalisation. Cyber. Resilience. Financial. Manufacturing. Industry 4.0. Regulation.

setores. As instituições financeiras destacam o risco cibernético como uma prioridade de negócios e são orientadas pela política de Gestão de Risco em Tecnologia (RMiT) do Bank Negara Malaysia. Enquanto isso, as empresas de manufatura não têm regulamentação específica do setor e frequentemente discutem seus planos futuristas e de atualização de alta tecnologia, mas pouco falam sobre a resiliência cibernética desses empreendimentos. Esta pesquisa sugere que a regulamentação específica do setor é um fator determinante para a formalização consistente das narrativas de risco cibernético no setor financeiro e indica áreas a serem exploradas por conselhos, reguladores e formuladores de políticas, à medida que esses riscos se estendem para cenários ciberfísicos de manufatura.

Palavras-chave: *Malásia. Digitalização. Cibernética. Resiliência. Financeiro. Manufatura. Indústria 4.0. Regulamentação.*

1 INTRODUCTION

Both financial services and manufacturing are cornerstones of Malaysia's economy in terms of their share of gross domestic products (GDP), job creation and contribution to exports. Within financial services, banks and insurers are busy digitising their platforms and exploring partnerships with fintech firms, while manufacturers are increasingly adopting Industry 4.0 tools such as automated production lines, internet-enabled IoT devices and smart-factory setups. These industries expand their presence into cyberspace. Cyberspace is a structure that allows states to wield influence over digital infrastructure, standards, platforms and data flows (Cora & Mikail, 2026).

As more and more of these activities run on systems that are heavy on data and software or are connected by networks, a cyber-incident begins to move from being a purely IT problem to becoming a risk to business continuity, public trust, workplace safety and regulatory compliance. Cyber risk refers to threats to information systems or networks using cyberattacks or illegal data-driven activity like hacking, malware, fraud, espionage and data loss that may lead to substantial harm to the public and businesses (Mahdy, 2026).

Cyber resilience which is understood here as an ability to resist, adapt to and recover from disruptions, whilst ensuring that critical functions remain operational has become a strategic concern in both sectors. Financial firms in Malaysia are subject to comparatively strict regulation, with Bank Negara Malaysia's (BNM) Risk Management in Technology (RMiT) policy for having fairly granular requirements. In contrast, manufacturers operate under less targeted, sector-agnostic guidance.

While Malaysian manufacturing businesses are covered by broader documents like the Malaysia Cyber Security Strategy, the Personal Data Protection Act 2010 and more recently, the Cyber Security Act 2024, there's not a sector-specific regulation with the specificity of or focus on technology risk as in the RMiT. This doesn't mean manufacturers are unaware of cyber risks, but it does point to manufacturers operating with a clearer legal landscape than is available to some other sectors in Malaysia.

Simultaneously, manufacturers are increasingly adopting Industry 4.0 technologies, IoT devices, robotics, smart factories and advanced semiconductor or automotive technology within their manufacturing processes. This leads to the creation of integrated cyber-physical systems where a cyber incident will cause disruptions to production schedules, supply chain activities or even the safety conditions within the manufacturing plant, beyond simply exposing customer data.

Most of the existing research conducted in relation to financial institutions or manufacturing industries separately, with relatively limited work examining how organisations across sectors frame their technology, cybersecurity and resilience activities internally in their annual reports. Earlier examples like Subbarao & Zéghal (1997) have already compared disclosure of human resources information among financial and manufacturing firms across six countries and pointed out differences between firms, though this research is now three decades old and related to human resources disclosure than technology or cybersecurity. Leo (2020) employed text mining to conduct analysis of annual reports of global systemically important banks, concluding that there is a gap between those reporting operational resilience and those which do not report on it, although cybersecurity as such isn't mentioned.

This study addresses that gap by comparing cyber resilience maturity in Malaysian financial and manufacturing firms using qualitative analysis of their latest Annual and Sustainability Reports. The research is guided by two questions:

1. How do financial and manufacturing firms conceptualise, govern and operationalise cyber resilience within their organisational contexts?
2. To what extent do sector-specific regulatory regimes and governance frameworks shape variations in cyber resilience maturity between financial and manufacturing firms?

The empirical material comprises firms' self-disclosures. The theoretical perspective builds on a three-layered socio-technical lens: strategic framing, structural governance and operational socio-technical practices. These three layers were used to make comparisons of sectoral maturity and regulatory influence. This paper pays special attention to how Industry 4.0 is represented in manufacturing discourses. The goal isn't to produce a ranking, but to shed light on the impact of different regulatory environments on the discourses firms present concerning their cyber resilience.

2 LITERATURE REVIEW

2.1 Cyber resilience in the financial sector

Cyber resilience is becoming more strategically integrated within financial organizations as opposed to simply an IT consideration, as recent attacks have proven the potential for disruptions localized in one jurisdiction to propagate across global markets and even damage confidence in the broader financial system. Instead of the traditional focus on defensive firewalls or merely adhering to compliance rules, conversations surrounding cyber resilience have begun to involve a synthesis of technology, management and organizational development. While this trend is acknowledged in various writings, the contributing authors focus on distinct facets of this shift and may not all subscribe to the same conception of "resilience".

Dupont (2019) gives an example of cyber resilience. While cyber resilience is popular in policy and industrial dialogue, its boundaries are vague. Definitions vary, measurements differ and a gap remains between ideals and what institutions can practically achieve in a sector where the best-resourced organisations cannot guarantee systems for all foreseeable and unforeseeable circumstances.

Biró (2025) reviewed the frameworks from the IMF, ESRB and the National Bank of Hungary to conclude that cyber resilience at the systemic financial level needs to be achieved by bringing cyber security experts and financial stability experts working closely together in a common effort, instead of by treating them as separate fields.

Ayodele and Adelaja (2024) suggest that financial institutions must have robust governance arrangements, appropriate technical controls and learn adaptive mechanisms to protect their operations because threats environment continues to evolve, consequently, failure potential results in system-wide systemic outcomes not merely localized operational problems. In other words, cyber resilience does not represent a specific situation of preparedness, but the continuous organizational capability to respond appropriately, absorb losses and manage setbacks. Although proportions differ across organizations, locations, jurisdictions, etc., for most financial institutions it means being able to balance response, resilience and adaptation, even though a consensus definition may not emerge quickly.

This has led regulators to incorporate cyber resilience as a key operational risk, expecting detailed stress testing, board-level responsibility and industry-wide stress simulations (Carrillo, 2023). More concretely, this will likely result in regulations that require periodic cyber exercises, establish committees explicitly mandated to cover cyber threat risk management and require evidence of board engagement rather than mere abdication to internal technology specialists. An institution that has put policies in place to holistically counter cyber threats, rather than simply having a security function, is about 64 per cent less vulnerable and recovers from breaches more than 2.3 times as quickly as companies without these policies (Tope Oladele Jooda *et al*., 2023).

In the Malaysian context, financial institutions appear to have a strong potential for cyber resilience through structured governance and adaptive risk management approaches. Hasnan (2023) found that IT governance and risk management positively impact cybersecurity governance. Ayodele and Adelaja (2024) revealed that firms using adaptive resilience where policies adjust with real-time threat information, are much better at preventing and addressing cyber attacks.

These findings are consistent with the available literature that suggests Malaysian financial institutions are potentially at an advantage for implementing more structured cyber resilience practices that are already governed by fairly rigid technology-risk

regulations, such as RMiT, whereas other sectors (e. g. manufacturing) are generally not regulated to nearly this same extent.

2.2 Cyber resilience in the manufacturing sector

On the contrary, cyber resilience in manufacturing tends to focus primarily on Industry 4.0, Smart Factories and cyber-physical systems. The automation and digitisation technologies help lean manufacturing and flexible production systems but inherently introduce vulnerabilities. The interlinking of production lines, IoT sensors and cloud-connected supply chains increases the potential impact of a cybersecurity incident leading to either a disruption in production or a loss of confidential information and in some cases both.

Technology and digitalisation promise sizeable efficiency gains, yet they also introduce intricate cybersecurity vulnerabilities that are not easy to manage with ad hoc fixes. Ribeiro *et al*. (2021) state that digitalisation increases both production system agility and vulnerability to communication disruptions. Ghobakhloo *et al*. (2023) provides a comprehensive roadmap showing how Industry 4.0 can enhance supply chain resilience through functions like automation, improved visibility, and adaptive capabilities. El-Breshy *et al*. (2024) stated that manufacturing systems become more connected and need more resilience strategies, which involve a holistic integration of technical and organisational measures. Consistently highlighted that those risks cannot be handled in isolation, in the view of the authors, they ought to be handled in a proactive manner, taking into account the intimate relationship between IT and OT.

Heikkila *et al*. (2016) highlight that manufacturing systems' digital transformations increase vulnerability, with cybersecurity being a "continuous cat-and-mouse game". Manufacturing companies face significant challenges, including a lack of awareness, limited cybersecurity literacy, and constrained financial resources (Junior *et al*., 2023). A clear regulatory and preparedness gap, with financial institutions showing more advanced, holistic approaches to cyber resilience compared to the manufacturing sector (Tope Oladele Jooda *et al*., 2023).

Malaysia's industrial digital transformation is accelerating the pace of connection and network within the sector beyond the capabilities of many companies to create

adequate levels of cybersecurity. IoT adoption is growing, and firms are pressured by competitive pressures to digitalise to stay alive just to maintain an edge on their competitors, but the required security infrastructure to protect these networked production systems is not growing alongside it. Various studies have pointed out that the implementation level of cloud services and standard security protocols (as used to guard sensitive company databases) remains to be low because of the significant costs associated with such an investment. Ling *et al*. (2020) which examined 11 common implementation challenges versus Malaysia's own national policy in Industry 4.0, the report revealed that the national policy itself missed three implementation challenges from international studies, showing a blind spot somewhere in how the transition is managed at the national level.

The image deepens for Malaysian Small and Medium Enterprises (SMEs), according to Wong and Kee (2022), Industry 4.0 adoption among Malaysian manufacturing SMEs remains minimal, the binding constraints are with organisational capabilities and not the technology availability. According to a systematic review of 57 Malaysian studies under PRISMA conducted by Ludin *et al*. (2025), six recurring barriers to cybersecurity program adoption were identified which are financial constraints, human resource limitations, insufficient management support, cultural resistance, inadequate technical infrastructure, and weaknesses in legal and data protection compliance.

Unlike the financial sector, Malaysian manufacturing sector does not operate under a sector-specific mandatory cybersecurity framework. As investigated by Wallang *et al*. (2022), within the Malaysian SME context, cybersecurity adoption is identified to be a contextual and structural obstacle, instead of just a firm-level choice, due to the lack of mandatory regulations like those in the financial institutions.

Across these studies, there is a visible tension between the digitalisation effort making production faster and data driven while exposing factories to cyber-physical risks that the companies lack the required resources, skilled talent and regulatory pressure to manage. The integration between IoT-enabled production and risk management has only weaknesses, and without much help and regulation from the industry authorities, leaves Malaysia's manufacturers more susceptible to disruptions arising from these cyber-physical intrusions. This strengthens the argument to draw parallels between the cyber-resilience maturation in the financial industry compared to the manufacturing industry.

2.3 Socio-technical perspectives on cyber resilience

Originally developed in the 1950s by Ken Bamforth and Eric Trist of the Tavistock Institute of Human Relations and later elaborated upon by Eric Emery, socio-technical systems theory posited that optimal organisational performance relied on simultaneously optimizing its social (people, culture, relationships) and technical (equipment, processes, technology) subsystems than solely focusing on one (Pasmore *et al*., 1982; Walker *et al*., 2008). It was extended to cybersecurity to claim that cyber resilience is a result of how these technology-dependent components function interdependently and complement each other: the cybersecurity solutions people use, their behaviour within and beyond systems, the institutional processes they observe and how these elements interrelate in defending against cyber threats (Cavelty *et al*., 2023; Malatji *et al*., 2019; Pollini *et al*., 2021).

Research consistently shows that human error causes between 80-90% of security breaches (Burrell & Nobles, 2022). Fairburn *et al*. (2021) emphasise to effectively increase cybersecurity resilience, one needs to understand interaction among people, systems and organisations-going far beyond technical fixes. Jeong *et al*. (2019) further state that the current path towards an enhanced state of cybersecurity resilience is neither through any given technologies, but instead by understanding those interlocking socio-technical networks by which security operates.

This study draws on such socio-technical thinking to organise organisational narratives into three layers:

a. Strategic framing (how cyber resilience is positioned and legitimised);
b. Structural governance (how roles, rules and frameworks are arranged);
c. Operational socio-technical practices (how people, processes and technologies interact in practice).

These lens enables a structured comparison of how financial and manufacturing firms in Malaysia conceptualise and operationalise cyber resilience in their public disclosures.

3 METHODS

3.1 Research design

Qualitative document analysis sets as its primary method of data collection and analysis for this study.

In this approach, pre-existing texts are examined systematically to identify patterns, themes and meanings that are relevant to the research questions. Annual Reports and Sustainability Reports are particularly suitable for such analysis. These are authoritative, accessible documents produced by firms that set out their stated intentions, risk environment, risk controls, and internal structures for all their stakeholders.

Annual Reports and Sustainability Reports provide vital evidence of how firms choose to represent topics such as technology, risk and resilience. Beattie *et al*. (2004) states that corporate narrative reports are analytically weighty beyond numerical disclosure, especially when reading strategically than anecdotally. Coding topics and types of narrative helps to identify how firms disclose issues of such magnitude and intricacy to their different audience types. In this study each report used as the source document. The technology strategy sections, risk management, cybersecurity, operational resilience and digital transformation, passages relevant to research are coded using an analytical coding framework, in order to compare them structurally across firms and between sectors.

The Annual and Sustainability reports that analysed were for 2023-2025 financial years. This period is interesting for analysing cybersecurity risks and regulatory priorities concerning technology and operational resilience, as cyber threats and sophisticated methods are growing, and regulators and policymakers have paid greater attention to these issues. These documents serve the study goals because they simultaneously encapsulate changing regulatory expectations and a management narrative about cybersecurity resilience.

3.2 Sampling strategy and rationale

This study employs a purposive sampling approach for the selection of firms. Purposive sampling involves the selection of cases for a particular study on the basis that they can address the research question and offer insight into the research phenomenon (Palinkas *et al*., 2015) and the objective of analysis and theorisation (Campbell *et al*., 2020).

Two main criteria guided the case selection for this study. First, the companies selected had to be from the financial and manufacturing industries. Second, they were chosen on the basis of active technology and cybersecurity disclosure in their reports to allow sufficient depth of material for analysis in relation to the present research questions. To capture variation within these sectors, diverse business types were selected. In the financial sector, they included banks, insurance and takaful operators. In the manufacturing sector, it includes automotive original equipment manufacturers (OEMs), component manufacturers and other industrial manufacturers. This maximum-variation purposive sample aimed to select the most diverse cases in terms of these key dimensions, thereby documenting the breadth of variations and also identifying themes that occurred across the variation (Nyimbili & Nyimbili, 2024).

In total, Annual and Sustainability Reports from 33 listed firms were analysed. There were 15 financial institutions that consisted of banks and/or insurance and takaful operators, and 18 manufacturing firms ranging from the automotive original equipment manufacturers, component makers, to general industrial production and manufacturers of consumer goods. One or two reports for each company were scrutinised for 40 reports, all of which underwent qualitative review and analyses.

A purposive sampling strategy was used to capture variation across two economically critical sectors and to focus specifically on firms that actively disclose technology and cyber topics:

- Sectors:
  - Financial sector: banks and insurance/takaful operators listed on Bursa Malaysia;
  - Manufacturing sector: automotive OEMs, automotive components, other components (e.g. electronics/EMS), and wood-related or diversified industrial manufacturers.

- Inclusion criteria:
  - Latest available Annual and/or Sustainability/Integrated Reports (primarily FY2023–FY2025);
  - Reports containing explicit references to technology, digitalisation, cybersecurity, data privacy, cyber risk management, business continuity or cyber resilience.

This sampling strategy is justified on three reasons. Firstly, the financial services and manufacturing sectors are economic pillars of the nation meaning they are core to understanding cyber resilience in Malaysia. Secondly, the sectors have distinct legal backgrounds (e.g., RMiT vs. general corporate/data-protection laws) which this contrast creates an opportunity to examine how regulatory context may shape differences in maturity. Finally, it ensures qualitative data from those whose reports have tangible and significant evidence of technology or cyber issues discussed in their materials, which keeps the analysis tight.

3.3 Data collection

For each selected firm, the latest Annual and Sustainability Reports were obtained from either corporate websites or Bursa Malaysia. The analysis then focused on sections dealing with technology, digitalisation and cyber resilience, including:

- Risk management and "principal risks" sections;
- Corporate governance and board committee descriptions;
- Sustainability/ESG materiality matrices and "Material Matters" narratives;
- Technology strategy, digital transformation and Industry 4.0 sections;
- Business continuity and disaster recovery discussions;
- Explicit cybersecurity, data privacy, and cyber resilience statements.

Sections covering technology, cybersecurity, cyber risk, data privacy, cyber resilience, digitalisation or Industry 4.0 were filtered into structured tables for each sector. The columns captured the sector, subsector, the company, the original excerpt, the first stage codes used, subcategory/theme and the excerpt's meaning within a cybersecurity resilience context.

3.4 Coding and thematic analysis

The collected data in the form of reports were analysed using thematic analysis. According to Braun and Clarke (2006), thematic analysis allows for a rigorous process of identifying, examining, interpreting and organising recurring meanings found within the qualitative material of the collected data. This methodology is well-suited for document-based inquiries, which prioritise discovering prevalent themes or meanings within the collected evidence, as opposed to merely tallying the frequency of particular terms or concepts. The analysis followed the six-phase process described by Braun and Clarke (2006):

- Familiarisation with the data;
- Generating initial codes;
- Searching for themes;
- Reviewing themes;
- Defining and naming themes;
- Interpreting and producing the report .

The coding and themes were developed through an engagement with the dataset. The codes and themes evolved during the coding process, a process similar to many thematic analyses on corporate annual and sustainability report disclosure.

For instance, Nicolò *et al*. (2022) analysed a large set of integrated reports and combined deductive-inductive coding of specific predefined sustainability categories and themes identified during the reading process, to highlight meaning patterns in sustainability reports. Similarly, Al-Shaer *et al*. (2021) used computational linguistics to identify shared content across a range of sustainability reports, defining forward-looking language, discussion of risk and themes concerning governance as three separate analytical levels that are not easily combined but, when linked, can reveal different types of narratives within corporate reports.

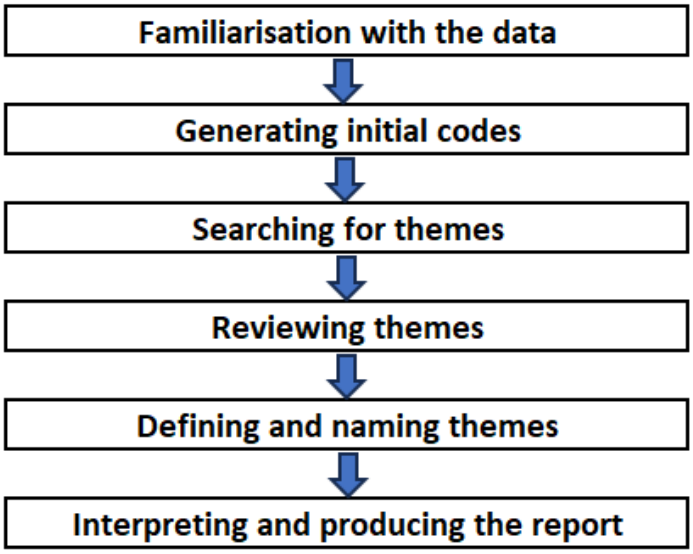
In the present study, the initial coding scheme was constructed deductively based on the literature about cyber resilience, technology governance and risks related to Industry 4.0, using a combination of codes and categories from the financial and manufacturing contexts. However, this initial coding was treated not as a definitive list

but as a provisional starting point. As the analysis progressed, codes were refined inductively. It became apparent that certain risks and governance patterns and those concerned with narratives surrounding digital transformation in firms in Malaysia, recurred across industries with repeated exposure to the annual reports. This hybrid approach of having established rules to follow from the literature but adapting them as we read the data resembles the reflexive nature of thematic analysis as argued by Byrne (2021).

Following established procedures for thematic analysis (Braun and Clarke, 2006), the content of the collected reports analysed as follow:

Figure 1

Thematic analysis six-phase process (Braun & Clarke, 2006)



3.4.1 Phase 1: familiarisation with the data

The analysis began with an immersive reading of the selected reports focusing on sections dealing with digital risk and governance. These sections were read and re-read to identify recurring language, recurring emphases and early indications of how organisations are articulating cyber resilience.

3.4.2 Phase 2: generating initial codes

Each excerpt was assigned one or more initial codes capturing key ideas. Examples include:

- "Technology and cyber risk as principal risk";
- "Cybersecurity and Data Privacy as material matter";
- "Smart Factory 4.0" and "IoT connectivity and robotics";
- "Zero Trust Framework", "VAPT and red teaming", and "PDPA alignment".

3.4.3 Phase 3: searching for themes

Initial codes were first organised into sub-categories, which served as an intermediate layer between individual codes and higher-level interpretation. These sub-categories were then developed inductively into broader themes by grouping together related ideas, for example:

- Risk framing and materiality;
- Governance structures and policies;
- Frameworks and standards;
- Operational controls and testing;
- Culture, skills and awareness;
- Digitalisation and emerging technologies;
- Impact and outcomes (incidents, metrics, trust).

3.4.4 Phase 4: reviewing potential themes

Themes were then checked carefully against both the coded extracts and the full dataset. This review stage was used to test whether the themes genuinely reflected what the reports disclosed, rather than the researcher’s expectations. In the course of this process, the more detailed sub-categories were consolidated into five broader, overarching themes:

- Governance and oversight;

- Operational capabilities;
- Culture, skills and resilience;
- Cyber resilience and emerging risks;
- Impact and outcomes.

3.4.5 Phase 5: defining and naming themes (Socio-Technical Mapping)

In this phase, the core focus of each theme was clarified by interpreting it through a three-layer socio-technical lens informed by the cyber governance literature. The themes were mapped onto these layers as follow:

- Strategic-framing layer: how organisations frame cyber risk and resilience (e.g. principal/key risk, material environmental, social and governance (ESG) matter, economic stability);
- Structural-governance layer: formal structures, frameworks, policies and regulatory/standards alignment (e.g. board committees, cyber resilience frameworks, references to Bank Negara Malaysia (BNM) policies, the Personal Data Protection Act (PDPA), International Organization for Standardization (ISO) standards, or the National Institute of Standards and Technology (NIST) frameworks references);
- Operational-socio-technical layer: technical controls, testing and incident response, combined with culture, awareness and digital/Industry 4.0 practices.

These layers are summarised in Figure 2, which specifies the focus area and key activities within each level of analysis.

Figure 2

Three-layer socio-technical framework for cyber resilience narratives

Layer	Focus area	Key activities and concerns
1. Strategic-Framing (Macro level)	Vision, direction and legitimacy	How the organisation frames technology, cybersecurity and cyber resilience (e.g. principal risk, material ESG issue, economic stability) and aligns them with external pressures, regulation and societal expectations.

Layer	Focus area	Key activities and concerns
2. Structural-Governance (Meso level)	Rules, institutions and coordination	Formal structures, rules and frameworks that organise cyber resilience (e.g. board and committee mandates, cyber resilience frameworks, policies, standards alignment, coordination across functions and entities).
3. Operational-Socio-Technical (Micro level)	Day-to-day interactions and design	Concrete technical controls, processes and social practices (e.g., security operations centre (SOC) monitoring, vulnerability assessment and penetration testing (VAPT), incident response, operational technology (OT) / Internet of Things (IoT) security, staff training, awareness, culture) where people, processes and technology are jointly optimised.

3.4.6 Phase 6: producing the report

In the final phase, the analysis was woven into a report narrative that links these emergent themes to the three socio-technical layers to offer a more comprehensive and integrated understanding of organisational cyber-resilience postures, using specific excerpts from selected reports to illustrate the way the patterns from coding and theme development appear in firms' own disclosure.

3.5 Cross-sector comparison and trustworthiness

After themes were defined, comparisons were made both within and between the financial and manufacturing sectors. These qualitative comparisons were underpinned by the frequency of features (such as board IT committees, cyber resilience framework, Industry 4.0, VAPT and staff training) in firms' reports.

Trustworthiness was addressed by:

- Using consistent coding categories for both sectors;
- Retaining original excerpts in the matrices to check interpretations;
- Comparing “exemplar” and “minimal” cases within each sector to avoid overgeneralisation.

4 RESULTS

4.1 Sectoral overview: different maturity profiles

Upon reading the two data frames in tandem, it was evident how the two sectors use the concept of cyber resilience in wildly different terms.

In financial sector, tech and cyber risk appear again and again, flagged as a key or primary risk. Privacy and cybersecurity frequently pop up as relevant and material ESG concerns. Banks cite the use of things like official cyber resilience policies, cyber risk strategies, group cyber resilience frameworks, board technology committees and risk committees that are overseeing both tech and cyber risk. These are accompanied by discussions of layered operational capabilities, which can include predictive frameworks, SIRT, Zero Trust, VAPT, red teaming, cyber drills, cyber simulations and cyber insurance, as well as well-executed staff and customer awareness initiatives. In a lot of cases, the banks write about these topics in precisely the same vein throughout the risk section, governance descriptions, sustainability matrices and their operational reviews.

Manufacturing firms commonly emphasise technologies such as automation, IoT, AI, robotics, 3D printing, smart factories, hybrid cloud and next-gen automotive and semiconductor products. Among these manufacturers, a number openly characterise cybersecurity and data privacy as significant considerations or core strategic areas. A subset of firms even details more robust cybersecurity structures and governance, such as DRB-HICOM's Cybersecurity Committee, cyber rating platform, and liability insurance. However, a majority of firms frame cyber risks broadly within either IT or operational risk and have relatively simple internal mechanisms with little specific connection to their Industry 4.0 descriptions. Their cyber resilience statements usually fall short in detail, consistency and linkage to the extensive digital transformation accounts elsewhere in these reports.

4.2 Financial sector: characteristics of cyber resilience maturity

4.2.1 Strategic-framing layer

Technology and cybersecurity risk sits at the highest level in the bank's risk hierarchy. AmBank positioned it as one of its "Principal Risks." Bank Islam, RHB, Maybank and Public Bank all used equivalent language such as "Key Risk" and "Principal Risk". Thus, this consistent language suggests cyber resilience sits at the highest level on board-level concern for the industry, as credit, market and liquidity risks do.

Cybersecurity fits well into material ESG issues. AmBank stating that *"Cybersecurity and Data Privacy falls under the most material category for business and stakeholders"*. Meanwhile, CIMB classified it among its "Material ESG Matters" suggesting its importance to the business, the environment and social factors, aligning with the definition of materiality as impacts on long-term value creation and reporting.

Furthermore, banks tied security directly to trust, which is intrinsically linked with the notion of the organization being held accountable ethically for the safety of its customers. For example, Maybank stated that one of the reasons for investing heavily in cybersecurity was to fulfill customer and stakeholder trust: *"managing risks ethically and effectively, building resilience against challenges."* Public Bank also actively promoted its awareness initiatives. To support this, PB has rolled out a nationwide "PB Scam Rangers" and states *"cyber security fraud experts who travel throughout Malaysia to educate the public and share updates on the latest scam trends"*. In doing so, the bank extended to the community, seeing public awareness as an essential part of the company's sense of resilience and ethical responsibility.

4.2.2 Structural-governance layer

The core difference between the financial and manufacturing firms, was the strength and precision of their internal governance framework. Rather than make broad, vague statements, financial firms explicitly referenced governance documents like policies and committees with clear objectives, providing specifics.

AmBank noted three main components of cyber governance: *"Cyber Risk Strategy," "multi-layered Cyber Risk Management Framework"* and a stand-alone *"Cyber Resilience Policy."* Bank Islam cited an impressive suite of instruments, referring to a *"Group Cyber Resilience Framework, a Group Technology and Cyber Risk Policy, Cybersecurity Testing Guidelines and Digital Security Key Management Guidelines,"* all *"aligned with the latest regulatory requirements and best practices."* Bank Muamalat, meanwhile, highlighted its alignment with government regulations, stating *"the establishment and operationalisation of the Technology Risk Management Framework (TRMF) and the Cyber Resilience Framework (CRF)… in line with BNM's Risk Management in Technology (RMiT) policy."*

Furthermore, the nature of board-level oversight was consistently detailed. For example, Maybank disclosed the function of its Board Technology Committee as *"tasked with shaping technology strategy and ensuring operational resilience, cybersecurity, and IT governance, including vendor risk and talent aspects"*. Hong Leong Bank, operating through two committee structures, stated that BARMC and GBITC were tasked with *"ensuring that management meets the expectations on technology and cyber security risk management as set out in BNM policy document on Risk Management in Technology."*

Bank Negara Malaysia's Risk Management in Technology (RMiT) seemed to be the most influential regulation, serving as the primary reference point for developing, justifying and describing the governance structures across banks and insurers. As an illustration, Public Bank acknowledged that its Technology Risk Management Framework (TRMF) *"developed based on BNM's RMiT"*. Bank Rakyat reported that its IT team had *"implemented improved threat monitoring, automated incident response capabilities, and compliance enhancements to meet regulatory standards, particularly in alignment with Bank Negara Malaysia's Risk Management in Technology (RMiT) guidelines."*

4.2.3 Operational-socio-technical layer

At the operational level, what the disclosures showed seemed to be broadly in line with what was claimed under its governance structures. Financial institutions are

described as doing far more than just having firewalls and then panicking after something happens.

Many of them described having tested their systems using exercises or simulations and finding weaknesses that they went on to fix. AmBank is claimed to have *'Above Average'* scores in the *"Cyber Simulation Exercise conducted by BNM"* and *"significant reductions in high-risk VAPT findings."* Bank Islam claimed it runs *"red teaming, cyber drills, and compromise assessments, rigorously testing incident response processes against emerging threats"* and that RHB also played a part in "*BNM RE4CT 2024,"* an *"industry-wide cyber resilience exercise."*

Many described dedicated teams and specialised centres, such as AmBank had a *"dedicated Security Incident Response Team (SIRT) to manage the full cyber risk lifecycle from identification to recovery"* or CIMB Bank its dedicated *"a dedicated Cyber Security Defence Centre and Threat Monitoring & Intelligence unit."*. RHB operated *"a Security Operation Centre and Cyber Emergency Response Team."*

Dedicated teams and specialised centres were also a recurring feature. AmBank had a *"dedicated Security Incident Response Team (SIRT) to manage the full cyber risk lifecycle from identification to recovery."* CIMB maintained *"a dedicated Cyber Security Defence Centre and Threat Monitoring & Intelligence unit"*. Meanwhile, RHB operated *"a Security Operation Centre and Cyber Emergency Response Team."*

There was also considerable mention of the importance of people to security, like Hong Leong Bank, requiring all employees to take an *"annual e-learning on cyber security and cyber risk management"* with *"a minimum score of 80%"* to pass, supplemented by *"phishing simulation exercises."* AmBank's Digital Academy has trained 767 employees on cybersecurity and AI and CIMB summarized this well *"We believe our people are an integral part of our cyber defence."*

It was also striking that many banks described moving towards implementing Zero Trust, like Bank Islam, which stated it has been implemented *"as a key component of our Cybersecurity Roadmap and Blueprint."* Bank Muamalat has also *"established the Zero Trust maturity model"* and Maybank utilizes *"advanced technology like zero-trust architecture, multi-factor authentication and rigorous employee training"*.

Taking these points together, these operational disclosures paint the picture of an industry with multilayered abilities, ranging from prevention to detection to response and

recovery, supported by dedicated staff teams and with the additional backing of testing against third-party scenarios and of training employees. To say what percentage of these actions have actually been executed properly would require examining the internal operations of those firms in the financial sector, something that cannot be assessed from public disclosures alone, but the similarities among them show they follow a similar template for what mature cyber resilience is expected to look like.

4.3 Manufacturing sector: industry 4.0 exposure and cyber resilience

4.3.1 Strategic-framing layer

Some manufacturing firms made ambitious statements about the technology involved. PECCA for instance, described its new plant as *"a future-ready hub for high-value manufacturing"* driven by *"system integration, IoT connectivity, and autonomous robotics"*. EG Industries described a *"Smart Factory 4.0"* producing *"5G optical modules, EV chargers and AI-related devices"*. APM detailed how *"automation, internet of things or IoT, and artificial intelligence or AI"* were reshaping operations.

For a couple of exceptions, "Cybersecurity and Data Privacy" were listed as a material matter by Jetson. MBM Resources directly linked cyber risk to *"financial losses, reputational damage and operational disruptions"*. Many more manufacturers listed cybersecurity, often only as a brief point under much larger categories such as "IT Risk" or "Operational Risk" without the prominent classification of "Principal Risk" or "Material Matter" that was standard for the banks examined.

This asymmetry was common across a large section of the manufacturers. These companies highlighted in considerable detail their digital ambitions, but did not mirror this when discussing the cyber-resilience implications that such technologies posed. This is referred to as the "digital ambition and resilience articulation gap" in this study. Manufacturers were keen to position themselves as at the cutting edge of technology, but did not articulate with comparable clarity or perhaps preparedness the risks and processes they had in place for cybersecurity risks tied to technology integration.

4.3.2 Structural-governance layer

The governance landscape in the manufacturing sample was far more varied.

DRB-HICOM reported that *"aligned its governance framework with the Malaysia Cyber Security Act 2024,"* established *"a dedicated Cybersecurity Committee with technically competent members under Board and Senior Management oversight,"* introduced *"a group-wide Cybersecurity Liability Insurance Programme"* and deployed *"a cybersecurity ratings platform for continuous posture monitoring."* These might not be far from what banks might report for governance, except that DRB-HICOM claims these are self-initiated based on management leadership.

Several other firms fall in a middle position. Jetson, for example, reported *"strengthening its cybersecurity framework by aligning practices with the Personal Data Protection Act (PDPA) 2010."* Globaltec Formation described *"a comprehensive cybersecurity framework integrated into operations, compliant with regulatory requirements in all regions."* V.S. Industry was *"ISMS ISO 27001 certified"* which represents a meaningful commitment to standards-based information security governance, although it remains a voluntary standard rather than a mandatory sector rule.

Lastly, some firms only mentioned general IT policies or list “Technology & Innovation” as one of several items overseen by a broad risk committee, such as Sapura Industrial, which referred to technology-related risks within the scope of the Group Risk Management Committee, but did not detail any dedicated structures, specific frameworks or particular regulatory benchmarks like banks had highlighted.

The most noticeable structural difference causing this variation is the absence of an RMiT equivalent sector-specific regulator, as financial institutions continuously referenced Bank Negara Malaysia's requirements, which provide direction and benchmarking to their cyber governance practices. Manufacturing institutions typically referenced the PDPA which, as argued earlier, relates primarily to data protection, not technology risk management or, in DRB-HICOM's case, the new Cyber Security Act 2024, leading to greater heterogeneity.

4.3.3 Operational-socio-technical layer

Most manufacturers described relatively basic but service-oriented controls. MBM Resources listed *"regularly updating and upgrading the firewall and antivirus system, implementation of cyber security awareness programmes for employees, implementation of Disaster Recovery Plan and regular data backup activities."* Jetson noted *"updating antivirus protections, maintaining secure firewall configurations, and reinforcing internal controls."* Globaltec Formation referenced *"updated firewalls/antivirus and restricted internet access"*.

Such controls are necessary basic requirements, but they fall short of the layered, intensely tested security architectures employed by banks, which include Security Operations Centres (SOC), Security Incident Response Teams (SIRT), red-teaming efforts, Zero Trust roadmaps and participation in BNM-led cyber simulation. The disparity is both quantitative and qualitative, with financial institutions typically referring to capabilities designed to look forward and stress-test under assault, while manufacturers largely focus on preventing known threats from gaining entry.

Notable was DRB HICOM's disclosures with its mention of *"annual VAPT and DR simulations, IT Security Awareness Campaigns for all staff, mobile security devices, patching regimes and completion of a Business Continuity Management System."* EG Industries reported *"zero data breach incidents"* and connects its data security posture to long-term resilience. However, public reporting alone cannot verify the completeness of such a claim.

More concerningly, OT-specific (operational technology) cybersecurity largely disappeared from the manufacturing discussions. Manufacturers described IoT-enabled production lines, robots, SCADA and cyber-physical manufacturing in technology discussions, yet rarely outlined how controls adapted OT systems as differentiated from IT systems. The implications of Industry 4.0 convergence of OT and IT and a resulting myriad of risks did not see significant exploration of operational resilience, supply-chain contagion risks or specific cyber-physical incidents.

Employee awareness likewise represented another area where manufacturing reports often fell short. UMW Holdings briefly alluded to efforts to *"continuously improving awareness on cyber security among employees,"* while MCE Holdings

disclosed its directors receive training. In contrast, a bank might describe mandatory, yearly e-learning courses with a passing score requirement, frequent phishing simulation campaigns or the existence of exclusive digital academies, without a corresponding discernible level of commitment described in the manufacturing sample. This does not necessarily mean such programs do not exist in practice but suggests they are not a focal point of the current cyber resilience discussion of manufacturing companies.

4.4 Cross-sector comparison

There are five patterns found based on cross sector analysis:

- Language: The language of the financial sector shows depth in specific terminology such as "Cyber Resilience Framework," "Zero Trust maturity model," "Security Incident Response Team," "red teaming," and "compromise assessments." Financial language points to the establishment of mature cyber resilience practices. However, manufacturing reports were more descriptive, with general statements such as "cybersecurity measures," "firewall and antivirus updates," and "IT policies."
- Narrative integration: The concept of cyber resilience emerges as an all-encompassing notion in the financial sector, as it is covered in various guises: risk taxonomies, ESG materiality matrices, board mandates, operational reviews and customer initiatives, all linked together and weaving into the general organisational discourse of risk management and resilience. By contrast, the manufacturing reports scattered related cybersecurity-linked content and rarely was it linked back to other sections of the document, cyber risk sometimes came up only in IT risk subsection, but not with any particular connection to wider digital-transformation narratives and strategic priorities.
- Regulatory anchoring: The RMiT framework for financial services gives firms an important reference point-the language and the regulator as justification for investing in governance and testing. This served simultaneously as a way to achieve compliance and an excuse for the comprehensive nature of the governance measures reported by the banks. However, manufacturers lack an equivalent in

their sector. Whilst the PDPA and the newly implemented Cyber Security Act 2024 legislation do provide important foundations, they do not stipulate the detailed, sector-specific technology risk governance that the RMiT outlines, contributing to the lack of a unifying framework in manufacturing.

- The Industry 4.0 paradox. While Manufacturers often talk about having the most sophisticated environments in this dataset: smart factories, 5G production lines, robots, autonomous production lines, etc., how they are preparing for the associated cyber resilience implications is often either implicit or briefly touched upon. The firms are adopting technology faster than they communicate how they manage their related cyber risk implications due to OT/IT convergence, the potential vulnerabilities associated with their supply chain and cyber physical attack scenarios.
- Outliers and agency. Exemplary firms exist in both sectors to point to maturity as not simply being the result of regulation, for instance, AmBank and Bank Islam both go further than the bare RMiT in their frameworks, testing procedures and staff awareness levels, while DRB-HICOM has developed a sophisticated suite of governance and operational capabilities on the manufacturing side without any prescribed standard for its sector, these firms highlight the significance of leadership and governance structures, arguing that regulation is a significant structuring factor, but does not define the extent to which and manner in which firms develop and articulate their cybersecurity resilience posture.

5 DISCUSSION

5.1 How firms conceptualise, govern and operationalise cyber resilience (RQ1)

The analysis highlights that for financial institutions cyber resilience is not just a technical solution or some clause within an IT security policy. They have instead framed cyber risk as a strategic risk and an urgent ESG issue, elevating it into the realm of core business strategy, governance and external communications. This framework actually does have some traction and, crucially, has led to complex, regulation-compliant governance structures. In practice, governance frameworks have produced reasonably

sophisticated practices. These include red-team exercises and large-scale, sector-level drills that pull people into an organization and place them at the heart of the response mechanism than a vulnerability. These include cyber squads within teams that also conduct some red-team drills and sector-level cyber exercises that also pull in the relevant participants. They have instituted ongoing staff training programs that treat employees as a critical element of the defense mechanism than the weakness.

Manufacturing shows a patchier trend. A select number of standout performers, DRB-HICOM, have successfully achieved higher levels of maturity. Their examples include having dedicated cybersecurity committees, buying cybersecurity insurance, running regular VAPT tests and disaster simulations and consciously adapting to new cybersecurity legislation. The rest of the industry still appears to regard cybersecurity largely at a macro or high level, with levels of governance differing greatly from business to business. Some manufacturers still rely on the most rudimentary controls-antivirus software, firewalls and data backups-as their principal defence mechanisms. Together, these create what could aptly be labelled a resilience gap. On one hand, many manufacturers are hurtling towards Industry 4.0, attaching IoT sensors to their production lines, introducing industrial robots and running prototypes for their smart factories. On the other hand, their reported security structures and general comments on cyber risk seem to fall short of these new and increasingly ambitious plans. In other words, the drive to digitalise seems to have outpaced efforts to think about and document resilience to cyber threats. For many of them, the security strategies that protect their increasingly digital assets may need to be more holistic, acknowledging the interconnected nature of IT and OT systems and the possibility of cyber-physical failure than viewing cyber risk as exclusively an IT concern independent of operations (El-Breshy *et al*., 2024; Ribeiro *et al*., 2021).

Evidence implies financial firms are moving towards a cohesive socio-technical approach to cyber resilience, while most manufacturers remain at an earlier stage, with basic controls and fragmented narratives that, failing to match their digital aspirations.

5.2 The role of regulation and frameworks in driving maturity (RQ2)

The sector divide appears heavily rooted in regulatory influence. Within the Malaysian financial system, Bank Negara Malaysia's RMiT is not just another piece of documentation that needs to be fulfilled; it is the organising logic behind the way top management, the risk department and technical teams conceptualise technology risk and cyber resilience. With RMiT, firms have an organised language and recognised level of maturity they can strive to carry out, resulting in a consistent strategy versus one consisting of siloed initiatives. This supports the study by Carrillo (2023), argument that prescriptive regulation can go beyond simply forcing compliance and actually shape how organisations conceptualise and prioritise resilience.

However, the manufacturing sector faces a much less prescriptive regulatory landscape. It mainly falls under general regulations like PDPA, the recent cybersecurity law and standards they choose voluntarily, but lacks a manufacturing-specific framework comparable to RMiT for financial sector in outlining expectations about technology risk. In such an environment, maturity levels are often determined by specific business leaders, particular client demands or pressure from global supply-chain partners, not by a sector-level baseline that everyone follows. Top-performing firms in the manufacturing sector have demonstrated it is possible to achieve a higher level of maturity without any specific push, yet, by comparison to other sectors, having a better regulatory framework for cybersecurity seems the most effective method to lift the overall bar for the manufacturing sector as a whole.

6 IMPLICATIONS

The report advocates for continued investment in cyber resilience for banks and insurance companies. The researchers point to AI, cloud-based services and ecosystem partners as additional sources of risk that have been introduced into financial services by these technologies.

The paper stresses the importance of aligning the strategy with manufacturing firms as they're at the forefront of Industry 4.0. The authors suggest establishing boards

with responsibility for cybersecurity within risk committees and setting controls for operational technology and key supply chain partners.

Policymakers can benefit from the analysis by applying principles such as those outlined in financial regulation about expectations for cyber governance, testing and auditing and the cyber incident reporting framework, which can raise the floor of cyber resilience for critical manufacturing. The Cybersecurity Act 2024 establishes the legal foundation, but the impact of this measure on the manufacturing industry will depend on the specific regulatory and practical guidance issued concerning OT and IT interoperability, supply chain challenges and the issues faced by SMEs.

7 LIMITATIONS AND FUTURE RESEARCH

This research focuses on public statements, not internal reality. Corporations might conceal their technical competencies to avoid exposing them to competition or threats from rivals or governments, whereas others could exaggerate them to encourage public trust. Both annual reports and those focusing on corporate social responsibility inherently promote a self-image and the conclusions should be understood with this qualification. Furthermore, the chosen data set consists of publicly traded companies, with a requirement that they should have disclosed enough information to be assessed on their technological and cyber maturity. Small and medium-sized enterprises (SMEs) operating privately and comprising the bulk of the manufacturing sector in Malaysia are beyond the reach of this analysis and may have different patterns of maturity in this respect.

Future research could address the issues raised above through several pathways. For instance, semi-structured interviews with CISOs, CROs and managers in IT and OT would help clarify how the structures presented in reports work in real life. Examining manufacturers currently struggling to reconcile OT and IT could help highlight how to build the necessary resilience of cyber-physical systems. Research on corporate reports compiled before and after the enactment of the Cybersecurity Act 2024 could also show how regulatory measures affect and transform how businesses communicate cyber resilience over time.

8 CONCLUSION

This study conducted a thematic analysis of 40 corporate reports, divided equally between Malaysia's financial and manufacturing industries, interpreted through the lens of a three-layer socio-technical framework to identify patterns in their reported levels of cyber-resilience maturity. The analysis revealed that the financial sector provides a more consistent narrative of resilience maturity, naming established frameworks, having formal board-level governance structures, describing sophisticated testing capabilities, integrating environmental, social and governance principles into cyber strategies and mirroring Bank Negara Malaysia's Cyber Resilience Framework and Risk Management in Technology (RMiT) guideline. In contrast, companies in the manufacturing industry frequently detail ambitious Industry 4.0 transformations but give a less detailed and more variable depiction of their security measures, exposing a "digital ambition and resilience articulation gap" in a sector increasingly reliant on digital technology and interconnected cyber-physical systems.

The role of regulation is shown as a key driver behind the maturity uniformity identified within the financial industry. The experience of DRB-HICOM demonstrates the continuing relevance of organisational autonomy and leadership: firms can progress beyond regulatory dictates when they so choose. As digitalization in manufacturing progresses and the gulf between the technology deployed and the protection implemented shrinks, this transition is no longer just a compliance issue but represents a major strategic and societal problem.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to the Universiti Teknikal Malaysia Melaka (UTeM) for supporting this study.

ETHICAL CONSIDERATIONS

The data supporting this study are derived from publicly available Annual Reports and Sustainability Reports published by the sampled firms through Bursa Malaysia and corporate websites.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

FUNDING DECLARATION

This research received no external funding.

REFERENCES

Al-Shaer, H., Albitar, K., & Hussainey, K. (2021). *Creating sustainability reports that matter: an investigation of factors behind the narratives*. https://doi.org/10.1108/jaar-05-2021-0136

Ayodele, O. F., & Adelaja, A. O. (2024). Advancing Cybersecurity Governance: Adaptive Resilience and Strategic Third-Party Risk Management in Financial Services. *World Journal of Advanced Research and Reviews*, *24*(2), 293–302. https://doi.org/10.30574/wjarr.2024.24.2.3312

Beattie, V., McInnes, B., & Fearnley, S. (2004). *A methodology for analysing and evaluating narratives in annual reports: a comprehensive descriptive profile and metrics for disclosure quality attributes*. https://doi.org/10.1016/j.accfor.2004.07.001

Biró, G. (2025). *Cybersecurity and financial stability:Interconnections, risks and regulatory approaches*. https://doi.org/10.33908/ef.2025.3.1

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101.

Burrell, D. N., & Nobles, C. (2022). Discovering the Emergence of Technical Sociology in Human Capital Systems and Technology-Driven Organizations. *International Journal of Human Capital and Information Technology Professionals*, *13*(1), 1–15. https://doi.org/10.4018/ijhcitp.300324

Byrne, D. (2021). *A worked example of Braun and Clarke's approach to reflexive thematic analysis*. https://doi.org/10.1007/S11135-021-01182-Y

Campbell, S., Greenwood, M., Prior, S., Shearer, T., Walkem, K., Young, S., Bywaters, D., & Walker, K. (2020). *Purposive sampling: complex or simple? Research case examples*. https://doi.org/10.1177/1744987120927206

Carrillo, E. F. P. (2023). Cybersecurity in European Financial Institutions: New Grounds for Corporate Governance Reform. *European Business Law Review*, *34*(Issue 7), 1133–1166. https://doi.org/10.54648/eulr2023052

Cavelty, M. D., Eriksen, C., & Scharte, B. (2023). *Making cyber security more resilient: adding social considerations to technological fixes*. https://doi.org/10.1080/13669877.2023.2208146

Cora, H., & Mikail, E. H. (2026). CYBERSECURITY, SOVEREIGNTY, AND INTERNATIONAL LAW: NORMATIVE CHALLENGES IN THE DIGITAL AGE. *Veredas Do Direito*, *23*, e234381. https://doi.org/10.18623/rvd.v23.4381

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

El-Breshy, S., Elhabashy, A. E., Fors, H., & Harfoush, A. (2024). Resiliency of manufacturing systems in the Industry 4.0 era – a systematic literature review. *Journal of Manufacturing Technology Management*, *35*(4), 624–654. https://doi.org/10.1108/jmtm-04-2022-0171

Fairburn, N., Shelton, A., Ackroyd, F., & Selfe, R. (2021). Beyond Murphys Law: Applying Wider Human Factors Behavioural Science Approaches in Cyber-Security Resilience. In *Lecture Notes in Computer Science* (pp. 123–138). Springer International Publishing. https://doi.org/10.1007/978-3-030-77392-2_9

Ghobakhloo, M., Iranmanesh, M., Foroughi, B., Tseng, M.-L., Nikbin, D., & Khanfar, A. A. A. (2023). Industry 4.0 digital transformation and opportunities for supply chain resilience: a comprehensive review and a strategic roadmap. *Production Planning & Control*, *36*(1), 61–91. https://doi.org/10.1080/09537287.2023.2252376

Hasnan, S. (2023). Impacts of Information technology and Risk Management on Cybersecurity Governance: Empirical Study on Malaysian Financial Institutions. *Economic Affairs*, *68*(3). https://doi.org/10.46852/0424-2513.3.2023.17

Heikkila, M., Rattya, A., Pieska, S., & Jamsa, J. (2016, December). Security challenges in small- and medium-sized manufacturing enterprises. *2016 International Symposium on Small-Scale Intelligent Manufacturing Systems (SIMS)*. https://doi.org/10.1109/sims.2016.7802895

Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019). Towards an Improved Understanding of Human Factors in Cybersecurity. *2019 IEEE 5th International*

Conference on Collaboration and Internet Computing (CIC), 338–345. https://doi.org/10.1109/cic48465.2019.00047

Junior, C. R., Becker, I., & Johnson, S. (2023). Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity. *ArXiv.Org*. https://doi.org/10.48550/ARXIV.2309.17186

Leo, M. (2020). *Operational Resilience Disclosures by Banks: Analysis of Annual Reports*. https://doi.org/10.3390/risks8040128

Ling, Y., Hamid, N. A. A., & Chuan, L. (2020). *Is Malaysia ready for Industry 4.0? Issues and Challenges in Manufacturing Industry*. https://doi.org/10.30880/ijie.2020.12.07.016

Ludin, E., Mohd, M., & Fauzi, F. (2025). *Enhancing Cybersecurity Programs in Small and Medium Enterprises (SMEs): A Systematic Literature Review*. https://doi.org/10.14569/ijacsa.2025.0160943

Mahdy, E. M. (2026). INSURANCE AGAINST CYBER RISKS: COMPARATIVE STUDY. *Veredas Do Direito*, *23*(3), e234297. https://doi.org/10.18623/rvd.v23.n3.4297

Malatji, M., Solms, S. V, & Marnewick, A. (2019). *Socio-technical systems cybersecurity framework*. https://doi.org/10.1108/ICS-03-2018-0031

Nicolò, G., Zanellato, G., Tiron-Tudor, A., & Polcini, P. T. (2022). *Revealing the corporate contribution to sustainable development goals through integrated reporting: a worldwide perspective*. https://doi.org/10.1108/srj-09-2021-0373

Nyimbili, F., & Nyimbili, L. (2024). *Types of Purposive Sampling Techniques with Their Examples and Application in Qualitative Research Studies*. https://doi.org/10.37745/bjmas.2022.0419

Palinkas, L., Horwitz, S., Green, C. A., Wisdom, J., Duan, N., & Hoagwood, K. (2015). *Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research*. https://doi.org/10.1007/s10488-013-0528-y

Pasmore, W., Francis, C., Haldeman, J., & Shani, A. (1982). *Sociotechnical Systems: A North American Reflection on Empirical Studies of the Seventies*. https://doi.org/10.1177/001872678203501207

Pollini, A., Callari, T., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2021). *Leveraging human factors in cybersecurity: an integrated methodological approach*. https://doi.org/10.1007/s10111-021-00683-y

Ribeiro, D., Almeida, A., Azevedo, A., & Ferreira, F. (2021). Resilience in Industry 4.0 Digital Infrastructures and Platforms. In *Advances in Transdisciplinary Engineering*. IOS Press. https://doi.org/10.3233/atde210067

Subbarao, A., & Zéghal, D. (1997). *Human Resources Information Disclosure in Annual Reports: An International Comparison*. https://doi.org/10.1108/EB029039

Tope Oladele Jooda, Adeyemo Taiwo Samson, & Adeyemi Adewunmi Olalemi. (2023). Strengthening cyber resilience in financial institutions: A strategic approach to threat mitigation and risk management. *World Journal of Advanced Research and Reviews*, *20*(3), 2217–2247. https://doi.org/10.30574/wjarr.2023.20.3.2460

Walker, G., Stanton, N., Salmon, P., & Jenkins, D. (2008). *A review of sociotechnical systems theory: a classic concept for new command and control paradigms*. https://doi.org/10.1080/14639220701635470

Wallang, M., Shariffuddin, M., & Mokhtar, M. (2022). *CYBER SECURITY IN SMALL AND MEDIUM ENTERPRISES (SMEs)*. https://doi.org/10.32890/jgd2022.18.1.5

Wong, A., & Kee, D. (2022). *Driving Factors of Industry 4.0 Readiness among Manufacturing SMEs in Malaysia*. https://doi.org/10.3390/info13120552