Computers & Security 165 (2026) 104873

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

Full Length Article

A cyber risk economics model for organization-wide risk management (CYREM-ORM)

Tong Xin[a], Ying He[a,*], Efpraxia D. Zamani[b], Mark Evans[c], Cunjin Luo[d]

[a] Queen Mary University of London, School of Electronic Engineering and Computer Science, London, United Kingdom
[b] Business School, Durham University, Durham DH1 3LB, United Kingdom
[c] School of Computer Science and Informatics, De Montfort University, Leicester, United Kingdom
[d] University of Essex, School of Computer Science and Electronic Engineering, Colchester, United Kingdom

ARTICLE INFO

Keywords:
Cyber threat intelligence
Fair
Cyber risk economics model
CYREM-ORM
Risk management

ABSTRACT

The increasing sophistication of cyber risks has made it challenging for organizations to assess their business impacts. The key challenge is the technical and language “barrier” between cybersecurity teams and business teams who make strategic investment decisions on cybersecurity. This often leads to delays, budget issues that prevent timely responses to cyber incidents. Existing research lacks a transparent, traceable, and reproducible method to communicate cyber risks and their impacts on businesses. We introduce a novel cyber risk economics model for organization-wide risk management (CYREM-ORM) that captures complex cyber risks and expresses them using financial terms. This is achieved by mapping Cyber Threat Intelligence (CTI) to the Factor Analysis of Information Risk (FAIR) model, enriched by cyber cost typologies. CYREM-ORM provides a traceable workflow that links organisation-related CTI to FAIR factor estimation, cost breakdowns, and ultimately to monetary loss amounts and prioritised risk scenarios. This design improves transparency in risk management, helps organisations prioritise mitigations in line with strategic business objectives, and enables stakeholders to assess the rationale behind results when needed. By grounding risk parameters in CTI, the model also facilitates proactive screening of organisation-relevant threats, instead of reactive, control-gap reporting. We evaluate the CYREM-ORM through three complementary case studies: the 2017 Equifax breach case proves its feasibility with historical data and open-source CTI, while the Small and Medium Enterprise (SME) education company and the large retail company cases show its effectiveness in communicating cyber risks at an organizational-wide strategic level within real-world contexts.

1. Introduction

Cybersecurity incidents can severely impact businesses through disruptions, financial losses, and reputational damage (Cavusoglu et al., 2015a). While organizations continue to increase cybersecurity investments (W. W. Li et al., 2023), cybersecurity risks keep rising, as evidenced by IBM's 2025 Data Breach Report (IBM Security, 2025). A major contributing factor is the sophistication of attacks, such as the Advanced Persistent Threat (APT) (Shin and Lowry, 2020). Many organizations struggle to address these threats in their defense strategies as they find it difficult to assess their impact on businesses operations (Benaroch, 2018; Kaspersky.com, 2023; Shin and Lowry, 2020). A key issue is the technical and language ‘barrier’ between the technical and business teams (e.g., business stakeholders and board members), which prevents a shared understanding of the impact of cyber risks. This miscommunication prevents timely cyber risk assessment and strategic level decisions on cyber risk mitigations and investment strategies, which often leads to delays, budget issues that limits effective responses to cybersecurity incidents. According to Kaspersky in 2023 (Kaspersky.com, 2023), 62 % of companies experience cybersecurity incidents caused by such miscommunication. The reports also highlight that this miscommunication is caused by different business priorities and technical jargon (i.e., languages, terms) of these teams.

Cyber threat intelligence (CTI) provides organizations with insights about cyber threats, threat actors, vulnerabilities, and security measures, allowing organizations to ‘know their enemy’, learn lessons from previous cyber incidents and reuse existing security solutions (Merah and Kenaza, 2021; Sun et al., 2023). It supplements traditional risk

[*] Corresponding author.
E-mail address: yinghe@qmul.ac.uk (Y. He).

https://doi.org/10.1016/j.cose.2026.104873
Received 10 July 2025; Received in revised form 8 December 2025; Accepted 24 February 2026
Available online 26 February 2026

assessment by enabling proactive, preventive, and timely identification of organization-specific risks (Ampel et al., 2024). CTI shows promise; however, current research and practice mainly focus on technical sharing mechanics (e.g., data formats and exchange) (Dong et al., 2023), and lack transparent, business-facing methods to translate those threats into financial impact for decision makers (Dekker and Alevizos, 2024; Qamar et al., 2017). As a result, organization-wide risk management and cross-functional collaboration (e.g., with finance) are still under-supported. This intensifies communication barriers, which leads to different risk perceptions and undermines the rationale behind cybersecurity investment decisions and risk mitigation strategies. To the best of our knowledge, there are currently no widely adopted processes that provide transparent, traceable, and reproducible intelligence-to-impact pathways that business teams (e.g. boards) can access when making strategic, organization-wide risk management decisions.

To address this gap, we proposed a novel approach, the Cyber Risk Economics Model for Organization-wide Risk Management (CYREM-ORM), which is inspired by the Cybersecurity Economics Model (CYSEM) (Xin at al., 2024). CYREM-ORM captures complex cyber risks and expresses them in financial terms by mapping CTI into the Factor Analysis of Information Risk (FAIR) model.[1] The FAIR model is selected due to business-centric feature and quantifiable risk factors (Heyburn et al., 2020). CYREM-ORM offers a semi-automatic, interactive assessment workflow: it processes multi-disciplinary data, such as security experts' inputs and industry reports, automatically screened, organization-relevant CTI (e.g., threat actors, TTPs, CVEs related to the organization), and business data for cost components, and produces monetized risk scenarios via Monte Carlo simulation. CYREM-ORM also allows users to rectify data retrieved from CTI sources. It will deliver risk-informed decision support for both technical and non-technical stakeholders, tailored to the criticality of business processes ranked by stakeholders (e.g., less critical systems, such as non-revenue-generating IT infrastructure, may not warrant the same level of cybersecurity investment as core customer-facing applications).

This research makes the following contributions,

- We propose a novel CYREM-ORM that integrates CTI with FAIR, enriched with cyber cost topologies. By translating cyber risks into financial terms, the model helps organizations prioritize cyber risks based on their strategic goals, and business needs, while being transparent, traceable, and reproducible.
- The CYREM-ORM bridges the gap between technical and non-technical stakeholders by providing transparent estimates of financial loss caused by cybersecurity risks and a detailed breakdown of how they were calculated behind those estimates to support organization-wide risk assessment and decisions.
- The CYREM-ORM has a novel CTI-driven algorithm that estimates key FAIR metrics and connects them to cost typologies, which reduces reliance on manual processing and subjective expert judgment during risk quantification and also enables proactive screening of threats relevant to the organization.
- We evaluate CYREM-ORM through three complementary case studies. The 2017 Equifax breach reconstruction case demonstrates the model's feasibility using historical data and open-source CTI, with results that fall within reported loss ranges. The China SME and UK retail cases assess the model's transparency, proactivity and applicability in real organizational settings, and illustrate how financially expressed, CTI-based scenarios can structure risk assessment discussions.

This paper begins with literature review of related work (Section 2). We then present our CYREM-ORM model (Section 3) and evaluate it with three complementary case studies (Section 4). We then discuss our findings and conclude this paper (Section 5 & 6).

2. Theoretical background and related studies

2.1. Cybersecurity risk assessment landscape

Cybersecurity risk assessment plays a critical role in organizational security management by identifying threats, evaluating vulnerabilities, and measuring potential impacts, which aims to help organizations develop prioritization and resource allocation strategies (International Organization for Standardization, 2018). Current popular risk assessment methods can be divided into three types: qualitative, quantitative, and hybrid approaches. Qualitative methods (e.g., NIST SP 800–30) use expert judgment to classify threats and impacts (ROSS, 2025). These are straightforward to implement but may lack accuracy due to subjective nature. Quantitative methods measure risk through financial or numerical indicators (e.g., FAIR) and converts risks into estimated monetary losses to provide a quantitative basis for investment decisions (Freund and Jones, 2014; Jones and Ashenden, 2005). Hybrid methods (such as OCTAVE) combine critical asset assessment with scenario analysis and focus on the integration of organizational knowledge (Alberts and Dorofee, 2003). In recent years, researchers have begun to research on dynamic risk assessment, anomaly detection, and predicting systematic attacks, using machine learning and data-driven models to update risk status in real-time (Shameli-Sendi et al., 2016; J. Wang et al., 2020).

However, organizations still face challenges in organisational risk assessment, particularly cross-department languages barriers. Multiple studies indicate that these barriers between information security departments, IT departments, and business units often lead to inconsistent perceptions of critical asset values and potential threats, which affect risk prioritization and mitigation decisions (Spears and Barki, 2010). This phenomenon of "organizational silence" restricts information flow, causing risk assessment results to deviate from actual exposure surfaces. Furthermore, Kayworth & Whitten (2010) argue that different departments regarding security incident definitions and response standards cause difficulties in executing risk assessment strategies. Therefore, future efforts need to establish cross-department collaboration mechanisms and rebuild this communication within organizations.

2.2. FAIR and its extensions in risk quantification

The Factor Analysis of Information Risk (FAIR) framework quantifies cyber risks in monetary terms by using a structured classification system and statistical methods, which enables transparent risk management among different stakeholders (Bakare, 2020; Freund and Jones, 2014; J. Wang et al., 2020). According to FAIR, total risk (expressed as financial loss) is determined by Loss Event Frequency (LEF) and Loss Magnitude (LM). LEF refers to the probable frequency within a given timeframe that a threat agent will inflict harm upon an asset, driven by Threat Event Frequency (TEF) and Vulnerability (V). TEF is defined as the rate at which threat actors are likely to target assets over a given period, while V is the likelihood that the assets will not resist the threats effectively. TEF is a product of Contact Frequency (CF), the rate at which threat actors encounter assets, and the Probability of Action (PoA), the chance that threat actors will exploit the assets upon contact. V is assessed as the gap between the capability of the threat actors (Threat Capability, TC) and the effectiveness of the controls in place (Resistance Strength, RS). In practical implementations, V is quantified as a numerical probability, sometimes referred to as Vulnerability Level (VL), to enable quantitative risk calculations. LM includes the total expected primary loss magnitude (PLM) and secondary loss magnitude (SLM). The former is the direct losses from an event, such as costs for cybersecurity incident

[1] In FAIR, the term "factor analysis" in its full name refers to a taxonomic decomposition of risk components, rather than psychometric exploratory/confirmatory factor analysis (EFA/CFA).

investigation or asset replacement. The later covers losses from reactions of external stakeholders such as employees, customers, and regulators (see Appendix A for more details).

Recent studies demonstrate how FAIR is operationalized in practice. He et al. (2025) integrates FAIR parameters with Return on Security Investment (ROSI) so that organizations can assess whether specific controls economically "pay off" cybersecurity investment. Seid et al. (2024) apply FAIR in the logistics domain by combining system logs/alerts and semi-structured expert interviews to parameterize scenarios. Methodologically, these applications strengthen FAIR's repeatable taxonomy for turning diverse evidence into money-based risk estimates. FAIR has also been extended to board- and disclosure-oriented use cases. The FAIR Materiality Assessment Model (FAIR-MAM) expands FAIR's LM into a standardized taxonomy of cost components to assess whether an incident is material in financial reporting and to communicate consistent loss estimates to executives and regulators (Nwafor et al., 2025). Similarly, the FAIR Controls Analytics Model (FAIR-CAM) formalizes the influence of controls on both the frequency and magnitude dimensions of risk and enables more defensible statements regarding which controls mitigate specific loss-event pathways (Tucker, 2025).

Collectively, FAIR and its extensions substantially strengthen the economic and governance articulation of cyber risk. However, published standards and commercial implementations often fail to show clear, step-by-step links between specific adversaries, observed TTPs/CVEs, concrete business assets, and the final monetary figures. This limits auditability and reproducibility for internal stakeholders who have to justify these numbers to finance, audit, and regulators. Moreover, existing research typically relies on generic datasets for input data rather than integrating up to date and organization-specific data to ensure its relevance and timeliness.

2.3. CTI and its applications in cybersecurity risk assessment

CTI is defined as information based on knowledge, skills, and experience about both cyber and physical threats, as well as the actors behind these threats, used to stop potential harmful events in the digital world (Ampel et al., 2024). CTI provides decision makers with actionable and valuable insights for early threat detection and promotes collaborative exchange of intelligence against future and existing threats (Gong, 2017; He et al., 2022). Using CTI effectively means sticking to a well-established set of norms and standards that help share updates about network threats (V. G. Li et al., 2019). The Structured Threat Information eXpression (STIX) is the widely accepted and comprehensive format in this regard, designed specifically for CTI exchanges. It is highly recognized for its ability to integrate CTI data and facilitate information sharing (Barnum, 2012). STIX enhances the application of CTI across the cybersecurity community by offering a flexible, scalable, and highly automated framework. It is crucial for analyzing threats, defining indicator patterns for cyber threats, managing response efforts, and maintaining records (Merah and Kenaza, 2021). Our research uses STIX 2.1, which is the de facto standard for structured threat information exchange (Riesco and Villagrá, 2019). This version incorporates core CTI elements, including taxonomies and terminologies and detailed descriptions of objects and properties, while integrating data from sources like the National Vulnerability Database (NVD) and Common Vulnerabilities and Exposures (CVE). Its framework comprises 18 STIX Domain Objects (SDOs), organized hierarchically into classes, subclasses, data types, and object properties, which offers a comprehensive framework for intelligence expression (see Appendix B).

Research on integrating CTI into risk assessment is still in its initial stage and has an imbalanced focus on technical aspect of CTI. Dekker et al. (2024) and Merah & Kenaza (2021) emphasize the dynamic nature of risk assessment models that leverage CTI, proposing methodologies that incorporate real-time data feeds to continuously update threat assessments and security postures. Similarly, Riesco & Villagrá (2019) explore the use of semantic web technologies and ontology to structurally represent and reason about CTI, enhances situational awareness and decision-making. Kure & Islam (2019) and Qamar et al. (2017) further this discussion by demonstrating how CTI can be used within structured frameworks like STIX to improve threat detection and response mechanisms. However, current research primarily focuses on technical implementation, and overlooks two critical aspects: how non-technical stakeholders can understand and use CTI-based risk assessments, and how CTI can support broader organizational processes, such as risk management and cross-departmental collaboration.

A few studies have begun to integrate CTI with FAIR. For example, Kerkdijk et al. (2021) used CTI data to populate the LEF and Vulnerability metrics of FAIR to prioritize different threat groups and reducing subjective judgment. However, it focuses on LEF, rather than translating these threats into specific financial loss scenarios so that senior management can see how much money might be lost. Furthermore, their audience is primarily security teams and industry intelligence-sharing groups, and do not include business decision-makers. Industry guidelines (Tucker, 2025) also standardize how to use observable CTI and historical loss data to populate key FAIR factors and maintain reproducibility. However, it is still at the level of practical guidelines and lacks peer-reviewed empirical validation.

2.4. Commercial cyber risk quantification tools

The business Cyber Risk Quantification (CRQ) platform market is growing rapidly. FAIR-based tools such as RiskLens (the official technology partner of the FAIR Institute) and Risk Cloud Quantify by LogicGate promise to deliver board-ready cyber risk reports in clear financial terms. RiskLens enables end-to-end FAIR implementation through scenario libraries and Monte Carlo simulations (RiskLens, 2023). LogicGate offers customizable Open FAIR breakdowns, which improves traceability and reproducibility (*LogicGate*, n.d.). Other leading board-focused tools like SAFE, Kovrr, and Balbix are known for their timely and actionable executive dashboards. SAFE combines internal controls and monitoring technology with quantitative analysis to provide risk views and ongoing assessments of risk control quality (*SAFE Security*, n.d.). Kovrr focuses on financial quantification of cyber risk for CFOs and insurers (*Kovrr*, n.d.), and is popular in cyber insurance. Balbix automates the entire process from risk exposure analysis to translating it into dollar amounts, and helpe convert technical security posture into board-level narratives (*Balbix*, n.d.).

These tools are designed to justify cybersecurity budgets, determine cyber insurance needs, and communicate major cyber risks in business language, which explains why boards of directors have increasingly invested in them. However, these tools still share common limitations in transparency and evidence tracing. For example, RiskLens, SAFE, and Kovrr can provide overall dollar-valued risk exposure and ranked lists of key scenarios, but they do not fully reveal the chain of assumptions behind them. They do not illustrate how they integrate specific threat actors, observed tactics, TTPs, exploited vulnerabilities, business assets, and primary/secondary loss categories to derive each figure. As a result, companies receive only summaries and lack auditability and reproducibility, rendering these tools susceptible to being perceived as "black boxes" during budget reviews. Additionally, Risk Cloud Quantify and Balbix primarily rely on historical baselines or generic scenario libraries. Their integration of adversary-specific and time-sensitive information (who is attacking and how they are attacking) varies considerably, which may lead to incorrect prioritization when the external threat landscape changes.

3. Methodology - CYREM-ORM

This section presents the CYREM-ORM methodology, which integrates STIX-based CTI, the FAIR risk assessment framework, and a comprehensive cyber loss cost typology to quantify the economic impact of targeted cyber threats. Among these components, the cost typology categorizes all possible losses caused by cybersecurity risks into 39 categories, which allows organizations to conduct a comprehensive loss review (Mori et al., 2020a). Specifically, we establish a mapping between key STIX SDOs and FAIR metrics. We then follow the FAIR workflow to assess risk: identify assets; assess TEF and LEF; and apply the 39-category cost typology to determine loss magnitude. For each PLM/SLM we obtain minimum, most-likely, and maximum values and model losses using PERT distributions, which are then aggregated and combined with the LEF Bernoulli distribution in a Monte Carlo simulation to generate an annual loss distribution and risk quantiles (e.g. P50, P90). This design produces distribution-based outputs for CYREM-ORM and reflects parameter uncertainties. Based on traceable CTI and peer-referenced loss ranges, risk assessments become more objective, transparent, and auditable. Fig. 1 shows the framework of CYREM-ORM.

3.1. Mapping STIX-based CTI to FAIR metrics

Inspired by Qamar et al's (2017) work, we match the key STIX SDOs to metrics in the FAIR model that are semantically similar and comparable and can be used in identifying potential threats, exploitable vulnerabilities, affected assets, impacts, etc., which help calculating the financial loss. Fig. 2 illustrates the mapping relationships between the STIX SDOs and the corresponding metrics in FAIR model. In the mapping, we prioritized SDOs that directly contributes to FAIR measurements (shown in grey), which are particularly valuable for quantitative risk assessment. Although other SDOs (shown in white) are not directly involved in calculations, they provide contextual information that supports metric evaluation when analyzed by technical staff considering organizational factors like system architecture.

3.2. Asset identification

For assets identification, organizations typically catalogue all critical data, hardware, software, systems, and facilities that are essential to business operations and could potentially impact the organizations' objectives if compromised (Freund and Jones, 2014).

3.3. TEF assessment

As mentioned in 2.2, TEF is determined by PoA and CF. We use CTI to assess potential threats by identifying relevant threat actors and assess their PoA and CF to the organization. Based on FAIR, CF is categorized into three types: random (i.e., the threat actor randomly encounters the asset), regular (i.e., contact occurs due to threat actor's regular activity), and intentional (i.e., the threat actor seeks out the asset) (Freund and Jones, 2014). We focus exclusively on 'intentional contact' as our model targets organized threats, such as APTs, rather than random or regular incidents. FAIR suggests that PoA can be assessed by assessing the capabilities, intentions, and goals of threat actors (Freund and Jones, 2014). CTI provides this information through Structured Data Objects (SDOs). We map relevant SDOs, such as Threat Actor and Intrusion Set, from CTI databases to organizational characteristics and assets for PoA analysis. Using the 'Threat Actor' SDO as an example: the 'Goal' and 'Motivation' properties reveal what the actor aims to achieve (Piazza et al., 2021). Mismatches between actor motivation or goals and organizational characteristics or assets reduce threat likelihood. The 'Sophistication' and 'Resource Level' properties indicate an actor's capability to execute complex attacks, in which sophistication reflects their skills and expertise, while resource level indicates available attack resources (Piazza et al., 2021). Low technical skills or resources diminish their threat capacity. If the 'Sector' or 'Location' properties match between actors and organizations, the attack risk increases. This CTI-based mapping helps filter and categorize potential threat actors for subsequent assessment.

For the CF assessment of APTs, according to FAIR's recommendations, we extract the actual counts of APTs contacts observed over a defined temporal window (e.g., past 12 months) from organization's system logs (e.g., SIEM (security information and event management) records, historical threat intelligence repositories) (Freund and Jones, 2014), and use feature scaling to normalize the T_n to a value between 0 and 1 for subsequent calculation of the CF variable (Freund and Jones, 2014). The formula is as follows,

$$CF_{T_n} = CF'_{T_n} - CF_{min}/CF_{max} - CF_{min} \tag{1}$$

- CF_{T_n} is the normalized contact frequency for T_n.
- CF'_{T_n} is the observed contact count for T_n.
- CF_{min}, CF_{max} are the minimum and maximum contact counts observed across all APTs under analysis.

If the exact number of contacts is not available, we classify CF into five frequency levels based on the attack patterns of APTs observed or in CTI (see Table 1).

For PoA assessment, the model quantifies the matching degree using CTI SDO vocabularies, which then informs the TEF calculation as the product of this matching. We operationalize threat actor T_n's capability by analyzing its sophistication and resource levels using the Threat Actor Sophistication Vocabulary and Attack Resource Level Vocabulary (Piazza et al., 2021). Sophistication includes seven levels from 'none' to 'strategic'; resource levels span six categories from 'individual' to 'government-backed' resources. We assign numerical values using the formula: value = 1 - (level / total levels) ˆ 2, which appropriately weights higher levels, following NIST SP 800–30 (Ross, 2012). The final capability scores of T_n is the geometric mean[2] of sophistication and resource level values.

$$C_{T_n} = \sqrt{SL_{T_n} \times RL_{T_n}} \tag{2}$$

- C_{T_n} denotes the threat capability of T_n.
- SL_{T_n} denotes the Sophistication level of T_n.
- RL_{T_n} denotes the Resource level of T_n.

Since STIX vocabularies describe threat actor motivations and goals but lack organizational matching levels, we adapt the five-level assessment scale from NIST SP 800–30 (Ross, 2012) to quantify each T_n's relevance to specific organizational contexts. Relevance levels between T_n's motivation and organizational types or purpose are: very high (1.0) for clear alignment, high (0.8) for strong correlation, medium (0.5) for partial overlap, low (0.2) for minimal connection, and very low (0) for no relevance. For T_n with multiple motivations, we aggregate relevance using the Noisy-OR model to ensures that the combined relevance is never lower than the strongest individual match, which means that a highly relevant motivation is not diluted by several weaker ones (Pearl, 2014).

$$M_{T_n} = 1 - \prod_{i=1}^{m} (1 - S(M_i)) \tag{3}$$

- M_{T_n} is the summative degree of $T_n{'s}$ motivation–organization relevance.
- m is the number of motivations for T_n.
- $S(M_i)$ is the relevance score of the i th motivation (M_i) to the organization, $\in [0, 1]$.

Relevance levels between T_n's goals and organization's asset types (e.

[2] We chose geometric mean because it is monotone and less fully compensatory than the arithmetic mean, which better reflects the idea that both sophistication and resource level factors matter (Krejčí & Stoklasa, 2018).

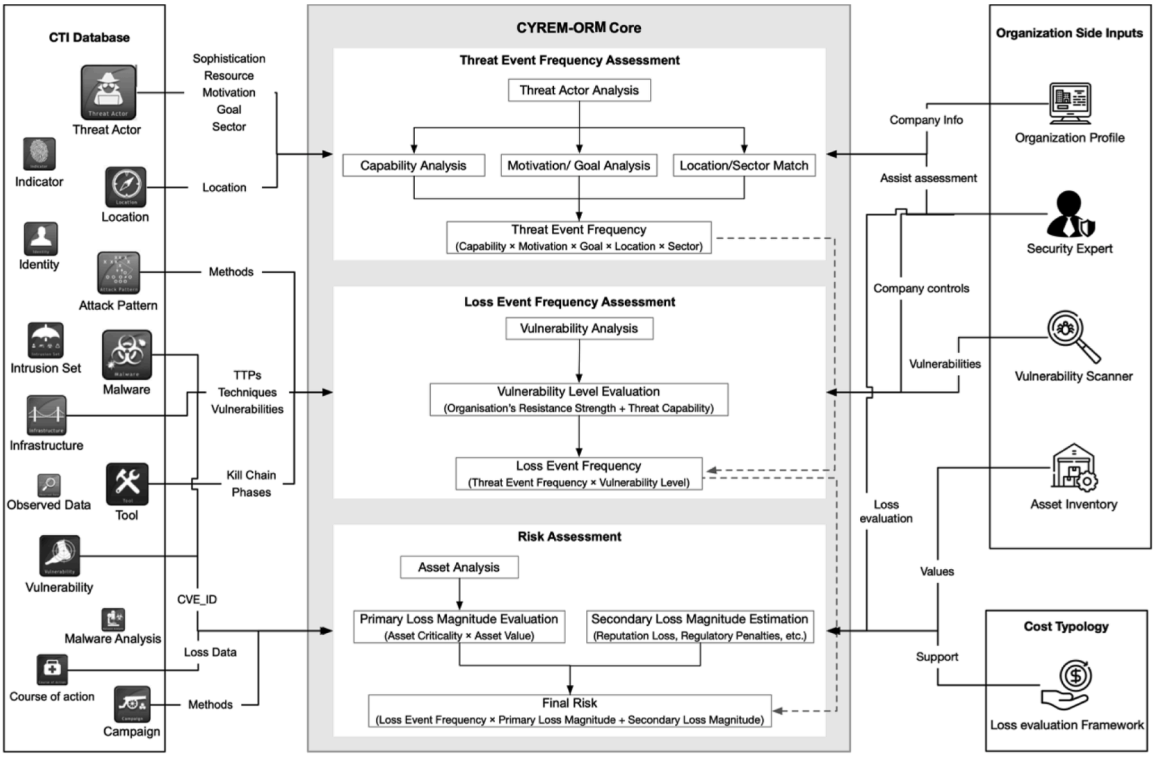

Fig. 1. Framework of CYREM-ORM and its workflow.

g., data, infrastructure, reputation) are assessed as: very high (1.0) for clear alignment, high (0.8) for strong correlation, medium (0.5) for partial overlap, low (0.2) for minimal/indirect connection, and very low (0) for no apparent relevance. If T_n possess multiple goals, we aggregate their match with the organization using the Noisy-OR model.

$$G_{T_n} = 1 - \prod_{j=1}^{n}\left(1 - S\left(G_j\right)\right) \tag{4}$$

- G_{T_n} is the summative degree of $T_n's$ goal–organization relevance.
- n is the number of goals for T_n.
- $S\left(G_j\right)$ is the relevance score of the j-th goal (G_j) to the organization, $\in [0,1]$.

Finally, the organization's geographical location and industry can be mapped with ‘Location’ and ‘Sector’ in STIX respectively. Some T_ns have strong capabilities or general motivations but lack specific historical focus on a particular location or sector. We introduce graded relevance factors that reflect how much overlap exists between the T_n’s known location/sector targets and the organization's profile, to avoid ignoring them completely (Joint Task Force Transformation Initiative, 2012). It allows T_ns with low evidence but high C_{T_n}, M_{T_n} or G_{T_n} to be considered in the analysis with appropriately weighted influence. Please check Table 2 for the details.

This assessment process determines the PoA for each potential T_n.

$$\boldsymbol{PoA}_{T_n} = \boldsymbol{C}_{T_n} \times \boldsymbol{M}_{T_n} \times \boldsymbol{G}_{T_n} \times \boldsymbol{L}_{T_n} \times \boldsymbol{S}_{T_n} \tag{5}$$

Thus, based on FAIR,

$$\boldsymbol{TEF}_{T_n} = \boldsymbol{PoA}_{T_n} \times \boldsymbol{Normallized\ CF}_{T_n} \tag{6}$$

3.4. LEF assessment

LEF refers to the probability of at least one successful loss event caused by T_n occurring within the assessment period (e.g., 12 months). Its assessment is related to V and TEF. Under the FAIR model, V is assessed through TCap and RS. To assess TCap, we first identify exploitable organizational vulnerabilities through systematic scans using network, web application, database, and configuration scanners. We then analyze the CTI database's ‘Vulnerability’ SDO for historical vulnerability data linked to specific T_n. Additionally, analyzing related SDOs (e.g., ‘Campaign’, ‘Infrastructure’, ‘Attack Pattern’) associated with T_n reveals which identified organizational vulnerabilities are exploitable by that aT_n. This process generates a list of potentially risky organizational vulnerabilities specific to each T_n.

$$\boldsymbol{V}_{T_n} = \boldsymbol{V_O} \cap \boldsymbol{V_T} \tag{7}$$

- V_{T_n} is the set of vulnerabilities that are both exploitable by the threat actor and exist within the organization's environment.
- V_T denotes the set of all vulnerabilities that a threat actor could potentially leverage.
- V_O denotes the set of all vulnerabilities that exist within the organization.

Organizational experts assess the difficulty T_n faces in exploiting vulnerabilities by reviewing existing security controls alongside high-risk vulnerabilities and technical details from CTI.

In this process, in addition to analyzing T_n’s sophistication and resource levels, we incorporate other relevant STIX SDOs, such as T_n's ‘Attack pattern’ and ‘Tool’. The attack pattern SDO outlines common methods used by T_n to exploit vulnerabilities, such as SQL injection or cross-site scripting attacks; the tool SDO shows the availability and complexity of the tools used by T_n. This information helps determine the ease or difficulty of threat actors exploiting vulnerabilities from a technological perspective. This analysis helps determine the vulnerability level (VL_{T_n}) by evaluating both the RS_{T_n} and $TCap_{T_n}$. Vulnerability levels use a five-point scale: very high (1.0) for minimal exploitation resistance; high (0.8) for significant exposure despite basic protections; moderate (0.5) for balanced risk requiring skill or persistence; low (0.2)

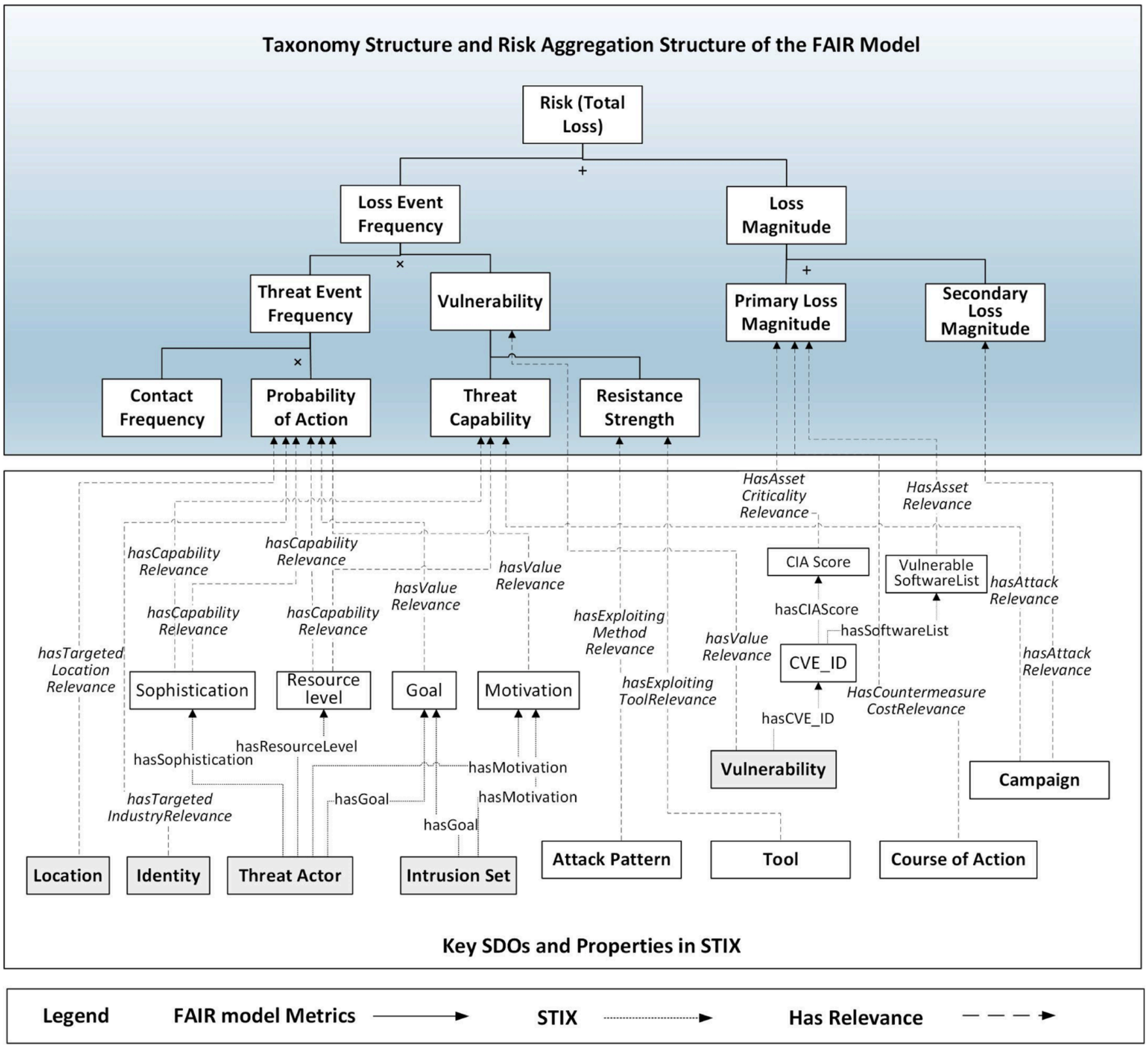

Fig. 2. CYREM-ORM - mapping key SDOs in CTI (expressed using STIX) to metrics in FAIR model.

Table 1
Contact frequency levels for APTs.

	Level
If $\boldsymbol{T_n}$ contact the target daily or near-daily, or evidence of extremely high frequency of action.	1
If $\boldsymbol{T_n}$ contact the target weekly but not daily, or evidence of high frequency of action.	0.8
If $\boldsymbol{T_n}$ contact the target monthly or seasonly, or evidence of medium frequency of action.	0.5
If $\boldsymbol{T_n}$ rarely contact the target, or evidence of low frequency of action.	0.2
If $\boldsymbol{T_n}$'s contact is only a one-time or isolated incident.	0

Table 2
Assessment scale for location and sector match.

Sector Match ($\mathbf{S}_{\mathbf{T_n}}$) / Location Match ($\mathbf{L}_{\mathbf{T_n}}$)	Level
If the organization's location/sector is among $\boldsymbol{T_n}$'s primary target locations/ sectors.	1
If the organization's location/sector is in $\boldsymbol{T_n}$'s known secondary target regions/sectors.	0.8
If $\boldsymbol{T_n}$ has no location/sector preference but has high motives and/or goals to reach the organization.	0.5
If the organization is outside $\boldsymbol{T_n}$'s typical operational area but still reachable.	0.2
If the organization is outside $\boldsymbol{T_n}$'s typical operational area and could not reachable.	0

for limited opportunities due to effective controls; and very low (0) for negligible exposure from rigorous defenses or lack of exploitable vectors. To enable quantitative simulation, we transform the LEF point estimate obtained from above (i.e., the product of TEF and VL) into a Bernoulli distribution by using it as the rate parameter, which enables more objective risk analysis.

$$\boldsymbol{LEF_{T_n}} \sim Bernoulli\left(\boldsymbol{TEF_{T_n}} \times \boldsymbol{VL_{V_{T_n}}}\right) \quad (8)$$

- LEF_{T_n} presents the probability that at least one successful loss event occurs during the assessment period because of Tn.
- $\boldsymbol{VL_{V_{T_n}}}$ denotes the organization's vulnerability level for Tn.

3.5. PLM and SLM assessment

PLM and SLM assessment require collaboration between technical and financial experts using STIX SDOs to identify vulnerable assets potentially affected by specific attacks. For example, through SDOs such as 'Attack Pattern', 'Malware', 'Report' of the confirmed threat actors T_n, it is possible to identify which assets may be impacted by T_n, successful attacks via specific vulnerabilities V_{T_n}, and historical loss amount in similar fields. It can also reveal potential direct damages such as data loss, service disruptions, or system harm. The vulnerability SDO's CVE_ID includes CVSS base score, which helps assess potential impacts on the confidentiality, integrity, and availability of information assets.

We assess LM by first using CTI information to determine the most likely value (mode) for each loss sub-item (i.e., PLM and sub-items of SLM) by cost category. We then reference industry reports and public data on comparable organizations' risk events (Carter, 2014; Patton, 1999) to set each loss type's [a,b] interval based on industry metrics (e.g., loss or revenue percentage, refund rate percentage). Since real-world assessments of asset values and recovery costs inherently contain interval uncertainty, we model each loss sub-item as a PERT distribution, i.e., $\mathrm{LM}_{\mathrm{T_n}} \sim \mathrm{PERT}(\mathrm{a}_{\mathrm{T_n}},\ \mathrm{m}_{\mathrm{T_n}}, \mathrm{b}_{\mathrm{T_n}})$. Finally, we aggregate all loss sub-items to obtain the total loss magnitude.

To assess the most likely value (mode) of PLM, we consider both asset criticality and value (e.g., physical costs, countermeasure costs, etc.) of the affected assets (Yaqoob et al., 2019). Criticality here refers to the asset priority; assets with higher criticality values are deemed more essential to protect. The average CVSS base scores of vulnerabilities linked to an asset serves as indicators of its criticality, highlighting how the vulnerability impacts the confidentiality, integrity, and availability of that asset. Additionally, the 'Course of Action' SDO provides mitigation recommendations, which helps estimate countermeasure and recovery costs.

$$\begin{aligned} \boldsymbol{a}_{T_n}^{PLM} &= \sum_{k=1}^{N} \left(\overline{\boldsymbol{CVSS}_{V_{T_n}}} \times \boldsymbol{AV}_k^a\right) \\ \boldsymbol{m}_{T_n}^{PLM} &= \sum_{k=1}^{N} \left(\overline{\boldsymbol{CVSS}_{V_{T_n}}} \times \boldsymbol{AV}_k^m\right) \\ \boldsymbol{b}_{T_n}^{PLM} &= \sum_{k=1}^{N} \left(\overline{\boldsymbol{CVSS}_{V_{T_n}}} \times \boldsymbol{AV}_k^b\right) \end{aligned} \tag{9}$$

- $\boldsymbol{m}_{T_n}^{PLM}$ denotes the most likely value (mode) of PLM.
- $\boldsymbol{a}_{T_n}^{PLM}$ denotes the minimum loss estimate of PLM based on the peer cases.
- $\boldsymbol{b}_{T_n}^{PLM}$ denotes the maximum loss estimate of PLM based on the peer cases.
- $\overline{CVSS_{V_{T_n}}}$ denotes the criticality of the k-th asset.
- $\boldsymbol{AV}_k^a,\ \boldsymbol{AV}_k^m,\ \boldsymbol{AV}_k^b$ denotes the minimum, most likely and maximum value of the k-th asset, seperately.

Therefore, the PERT distribution of PLM is,

$$\boldsymbol{PLM}_{T_n} \sim PERT\left(\boldsymbol{a}_{T_n}^{PLM}, \boldsymbol{m}_{T_n}^{PLM}, \boldsymbol{b}_{T_n}^{PLM}\right) \tag{10}$$

SLM primarily includes reputational impact, legal litigation, compliance fines, and customer churn costs (Mori et al., 2020a). Values can be sourced from internal organizational data (historical litigation records, compliance/audit reports, IT cost statements) or external CTI sources (data breach analysis reports, GDPR/CCPA penalty databases, industry reports, financial analyses). When direct data is unavailable, secondary losses can be inferred from primary loss characteristics and associated STIX SDOs. For example, campaign SDO related to a threat actor elaborate on the broader targets and impacts of coordinated attacks, which helps us assess the wider business and operational impacts beyond direct damages, such as reputational damage and regulatory fines resulting from significant data breaches.

We adopted the same assessment method as PLM, and performed PERT modeling on each component of SLM and summarized them to obtain the SLM interval.

$$\boldsymbol{SLM}_{T_n,s} \sim PERT\left(\boldsymbol{a}_{T_n,s}^{SLM}, \boldsymbol{m}_{T_n,s}^{SLM}, \boldsymbol{b}_{T_n,s}^{SLM}\right) \tag{11}$$

- s denotes the sub-item of SLM.
- $a_{T_n,s}^{SLM}$ denotes the minimum loss estimate of the sub-item of SLM based on the peer cases.
- $m_{T_n,s}^{SLM}$ denotes the most likely loss estimate of the sub-item of SLM based on the peer cases.
- $b_{T_n,s}^{SLM}$ denotes the maximum loss estimate of the sub-item of SLM based on the peer cases.

Thus,

$$\boldsymbol{SLM}_{T_n} = \sum_{s \epsilon S} \boldsymbol{SLM}_{T_n,s} \tag{12}$$

3.6. Monte Carlo-based risk assessment

To propagate the uncertainty of previous metrics (e.g., LEF, PLM, SLM) into the final risk output, we use a Monte Carlo simulation. Specifically, in each simulation run, the model first uses LEF to decide whether a loss event driven by $\mathrm{T_n}$ occurs in that year (yes or no), by drawing a Bernoulli outcome. If an event occurs, the model then samples each PLM and SLM sub-item from its PERT distribution and sums them to obtain a realization of the total loss magnitude for $\mathrm{T_n}$. The simulated annual loss contributed by $\mathrm{T_n}$ in $\mathrm{i^{th}}$ run is,

$$\boldsymbol{R}_{T_n}^{i} = \boldsymbol{LEF}_{T_n}^{i} \times \left(\boldsymbol{PLM}_{T_n}^{i} + \boldsymbol{SLM}_{T_n}^{i}\right) \tag{13}$$

Repeating this procedure for a large number of iterations generates an empirical distribution of annual loss. From this distribution, CYREM-ORM reports standard risk metrics such as expected annual loss and key percentiles (e.g., P50, P90).

4. Evaluation of CYREM-ORM - multiple case studies

In this section, we evaluate CYREM-ORM through three complementary case studies to demonstrate its effectiveness and practical applicability in different organizational contexts. The first case study examines the 2017 Equifax data breach (P. Wang and Johnson, 2018). The second and third case studies apply the model to an SME education consulting company and a large retail company respectively, which assesses the real-world utility of CYREM-ORM in two different industrial settings. Accessing company data in relation to data breaches and cybersecurity is exceptionally challenging, since companies rarely share such sensitive data, even in anonymized form. To overcome this challenge, our research uses a combination of methodological approaches.

For the Equifax case, we use a document analysis method (Bowen, 2009) combine with semi-synthetic data (Stojanović et al., 2020). The data integrates publicly available information from available reports with expert-generated mock data through expert judgement research method (Hughes, 1996; Otway and von Winterfeldt, 1992) where detailed information is lacking. Specifically, we invited three domain experts with 8–15 years of experience in cybersecurity risk assessment and incident analysis. Each expert independently simulated the missing variables in the Equifax case based on the same known facts and information from public reports, according to their professional judgment. Finally, we aggregated the data and took the median/mean value of each variable to minimize individual bias.

For the two industrial cases (the large retail company and the SME education consulting company), we adopt multiple instrumental case studies approach combined with summative ex post reviews. Instrumental case study uses a specific case to provide insight and refinement into a broader phenomenon beyond the individual case itself (Kekeya, 2021). It allows us to examine how CYREM-ORM can be applied in real-world industrial settings by analyzing the experience of specific organizations in detail. The summative ex post reviews with participants in the cases can help us gain deeper understanding of how the model can effectively bridge the language gap between technical and business stakeholders. Additionally, to support the case studies of the large retail company and the SME education consulting company, we developed an interactive system to be used as a training tool and platform for the application of CYREM-ORM. The system consists of three main components: (1) the composition of the model, theoretical background, and concepts of key elements, (2) demonstration cases that illustrate how to apply the model, and (3) an interactive interface that enables industrial practitioners to conduct risk assessments.

The three cases offer complementary insight: the Equifax case demonstrates CYREM-ORM's effectiveness with historical data and open-source CTI, to validate the model's analytical accuracy. The SME case assesses CYREM-ORM's accessibility and cost-effectiveness for resource-constrained organizations with limited cybersecurity expertise. The large retail company case evaluates CYREM-ORM's capability to translate technical cyber risks into financial terms and facilitate cross-departmental risk management. The following subsections (4.1 - 4.3) present each case in detail.

4.1. *Case study 1 - CYREM-ORM evaluation using the 2017 Equifax data breach*

The Equifax data breach case study shows how CYREM-ORM can be applied to translate the cyber risks to financial implications. This case was selected since it represents a well-documented major data breach with publicly available financial impact data. Additionally, it allows us to evaluate and compare our model's results based on known outcomes. Our analysis is based on the document analysis method, most of the data is from official reports and public disclosures related to the breach (Daswani and Elbayadi, 2021; P. Wang and Johnson, 2018).

Equifax is one of the largest credit reporting agencies in the United States. In this major data breach, the personal information of about 147 million consumers was leaked. The main reason for the leak was that Equifax failed to promptly patch the CVE-2017–5638 vulnerability in Apache Struts[3] (Daswani and Elbayadi, 2021). The data breach caused serious financial losses to the company, ranging from $1.38 - $2 billion (Jai Vijayan, 2020; Mark Meltzer, 2020). Appendix C detailed the cost statistics and sources.

Assets Identification of Equifax. The analysis focuses on Equifax's key assets, which includes consumer data and credit reports, intellectual property, and IT infrastructure.

TEF assessment. Using STIX SDO mapping, FIN7 is selected as a representative targeted threat actor for Equifax because it is a financially-motivated, spear-phishing-driven intrusion set active since 2013 (Anvilogic, 2023), and also matches Equifax's sector and location profile. As discussed earlier, CYREM-ORM focuses on deliberate, organized threats, we treat CF as intentional contact. Given FIN7′s history of frequently targeting U.S. financial companies (Anvilogic, 2023), we assign CF = 1.0, which is the highest FAIR intentional contact level. PoA is calculated by multiplying the scores for capability, motivation, goal, location, and sector (Eq. (5)). Capability ($\mathrm{C_{FIN7}}$) is computed as the geometric mean of sophistication and resource-level values (Eq. (2)). With FIN7′s sophistication level ($\mathrm{SL_{FIN7}}$) rated as advanced (0.673) and its resource level ($\mathrm{RL_{FIN7}}$) as organization-backed (0.889), $\mathrm{C_{FIN7}}$ is computed as $\sqrt{0.673 \times 0.889} \approx 0.774$. Next, motivation is determined using Noisy-OR aggregation. Given the primary and secondary motivations of FIN7 are financial gain (very high relevance, 1.0) and notoriety (moderate relevance, 0.5), M_{FIN7}= 1 - (1 - 1.0) (1 - 0.5) = 1 (Eq. (3)). The goal of FIN7 is data theft (very high relevance, 1.0), G_{FIN7} = 1 - (1 - 1.0) = 1 (Eq. (4)). FIN7 targets at U.S. and financial or retail sector, where Equifax is located and belongs to. According to Table 2, $\mathrm{L_{FIN7}} = 1$; $\mathrm{S_{FIN7}} = 1$. According to Eq. (5), the $\mathrm{PoA_{FIN7}} = 0.774 \times 1 \times 1 \times 1 \times 1 = 0.774$ (Eq. (5)). Thus, $\mathrm{LEF_{FIN7}} = 0.774 \times 1 = 0.774$ (Eq. (6)).

LEF assessment. In this stage, we identify the vulnerabilities $\mathrm{V_{T_n}}$ present in Equifax (V_O) and that T_n have exploited or could exploit (V_T) (Eq. (7)). Scans of Equifax's systems identified two vulnerabilities: CVE-2017–0144 and CVE-2017–5638. By examining FIN7′s relevant SDOs (e.g., attack patterns, infrastructure, malware) from the CTI database, we found that FIN7 has previously exploited CVE-2017–5638 and shows high capability to exploit CVE-2017–0144. Equifax's weaknesses in patch management, network segmentation, and web application security (Wang and Johnson, 2018) increase exploitation likelihood for both vulnerabilities. Based on these factors, we rated FIN7′s threat capability (Tcap) as high and vulnerability likelihood ($\mathrm{VL_{FIN7}}$) as 0.8. Thus, the LEF point estimate is $0.774 \times 0.8 = 0.619$. Then, LEF is transformed into a Bernoulli event variable: $\mathrm{LEF_{FIN7}} \sim$ Bernoulli ($p = 0.619$), which represents the probability that at least one successful FIN7-driven loss event occurs within one year.

PLM, SLM assessment. We then assess the potential primary and secondary losses if FIN7 were to exploit CVE-2017–5638 vulnerability against Equifax.

For PLM assessment: the PLM of FIN7 attack is divided into two major components based on the cost typology: incident response (IR) cost and business interruption (BI) cost. We use ‘Report’ and ‘Vulnerability’ SDOs, combined with industry data breach reports and Equifax's own financial data (Equifax Inc., 2016), to assess the parameters a, m, and b of PLM's PERT distribution. The IR cost estimates the direct costs related to handling the breach. We use net cost anchors from major data breaches of related fields before 2017 (e.g., Commonwealth of Massachusetts, 2022; *Target cyber attack: A Columbia University case study.*, 2022; The Home Depot, 2016), which showed costs in the range of $1.33 ∼ $4.05 per record. We model the Equifax exposure ratio as 5 %–25 % of its 820 million consumer records. This exposure ratio is from the evidence that many large consumer-facing data breach incidents affected roughly 5 %−25 % of customers, such as Experian, Orange and Home Depot (Commonwealth of Massachusetts, 2022; Joshua Melvin, 2014; The Home Depot, 2016). According to Eq (9), the IR costs for FIN7 are modeled as PERT ($1.33 \times 5\,\% \times 820 \times 9.05$, 170.73×9.05, $4.05 \times 25\,\% \times 820 \times 9.05$) $ million, i.e., PERT (493.5, 1545, 7514) $ million. The BI cost refers to the loss from downtime and operational disruption. Based on industry research prior to 2017 or from similar fields (Coveware, 2020; Datto, 2016; IBM, 2016; Intermedia, 2016), the duration of business disruptions caused by cybersecurity incidents ranged from several days (ransomware shutdown) to several weeks (complex systems recovery) and even one to three months (data breach containment period). Based on the evidence listed above and considering the combined impact of system outages, operational degradation, and recovery efforts, business disruptions are estimated to result in a loss equivalent to 0.5–2.5 months of profit. Based on Equifax's 2016 monthly profits (Equifax Inc., 2016) and Eq (9), FIN7′s BI costs have a PERT distribution of (184, 552.5, 921) $ million (see Appendix C.2 for details). Thus, PLMFIN7 is the sum of BI and IR costs, which is PERT (677.5, 2097.5, 8435) $ million (Eq (10)).

For SLM assessment, the reputation damage (i.e., the damage to Equifax's brand and customer trust, indirectly affected by the breach of personal data), and regulatory compliance and legal fees (i.e., costs arising from legal actions, fines, and settlements due to non-compliance with data protection laws) are considered as potential main secondary losses (Mori et al., 2020b). To estimate legal expenses, we use analogical anchoring to big data breach cases in highly regulated US industries prior 2017 (Daswani and Elbayadi, 2021; Target Corporation, 2016; *Target cyber attack: A Columbia University case study.*, 2022) and the industry reports (IBM, 2016; Verizon, 2016). These sources indicate that the average settlement cost per breached data record was $0.3 to $2.9. Settlements with banks, financial institutions and credit card companies are from $125 million to $160 million. As mentioned previously, 5 % ∼25 % of the 820 million customers were affected by the data breach. Based on the per-record legal and settlement anchors with this affected

[3] A popular open-source web application software.

base, we obtain an individual-level legal component PERT distribution, PERT (12.3, 209, 594.5) $ million (Appendix C.2). The estimated settlement amount for institutions (banks, card issuers, and regulators) is PERT (125, 142.5, 160) $ million. Thus, the three-point PERT parameters for the legal expenses are the sum of the individual and institutional components, which is PERT (137.3, 351.5, 754.5) $ million. Similarly, we model Equifax's reputational loss as 0.4 % - 2.5 % of its 2016 revenue using a PERT distribution (Appendix C.2). Thus, based on Equifax's 2016 annual profit of $489 M, we obtain the estimated reputation damage loss, which is PERT (2, 5,14.7) $ million. Therefore, $\mathrm{SLM}_{\mathrm{FIN7}} \sim$ PERT (139.3, 356.5, 769.2) $ million (Eq (11) & 12).

Monte Carlo simulation and risk results. To capture parameter uncertainty and obtain a full loss distribution, we implement a Monte Carlo simulation for the Equifax-FIN7 scenario. Following best practice in quantitative cyber risk studies (Erola et al., 2022; Franco et al., 2024), we run $N = 10^5$ iterations. In each iteration, we first draw a Bernoulli LEF indicator, $\mathrm{LEF}_{\mathrm{FIN7}} \sim$ Bernoulli (0.619). Conditional on $\mathrm{LEF}_{\mathrm{FIN7}} = 1$, we then sample $\mathrm{PLM}_{\mathrm{FIN7}}$ and $\mathrm{SLM}_{\mathrm{FIN7}}$ from their PERT distributions and compute the conditional $\mathrm{LM}_{\mathrm{FIN7}} = \mathrm{PLM}_{\mathrm{FIN7}} + \mathrm{SLM}_{\mathrm{FIN7}}$. The annual loss for the Equifax-FIN7 scenario is then $\mathrm{R}_{\mathrm{FIN7}} = \mathrm{LEF}_{\mathrm{FIN7}} \times \mathrm{LM}_{\mathrm{FIN7}}$. We summarize the resulting simulated distributions using the expected value, standard deviation, and empirical quantiles such as P50, P90, P95 (see Appendix C.4).

The Monte Carlo results indicate that the conditional loss (if there is a FIN7 breach) has a median (P50) of about $3.12 billion, while the annual loss distribution (including the loss-event probability) has an expected value of $2.04 billion and a P50 of $2.05 billion (Appendix C.3). The realized Equifax loss range of $1.7–2.0 billion falls within the central region of the simulated annual loss distribution, which suggested that CYREM-ORM provides a reasonable pre-breach risk estimates for this breach scenario. Fig. 3(a) shows the histogram of simulated annual loss values with the P50 and P95 markers. Fig. 3(b) provides the corresponding empirical cumulative distribution function (CDF), which is useful for directly reading capital-at-risk at different confidence levels.

Overall, the Equifax-FIN7 case operationalizes CYREM-ORM in a transparent way: CTI in STIX format is first used to identify FIN7 and quantify TEF (CF and PoA). LEF is then derived by combining FIN7's threat capability with Equifax-specific vulnerability likelihoods and converted into a Bernoulli loss event. Conditional PLM (IR + BI) and SLM (legal + reputational losses) are parameterized with PERT distributions anchored in mega-breach benchmarks prior 2017 and Equifax's 2016 financial report. Finally, Monte Carlo simulation propagates these inputs into a full annual loss distribution, which can provide valuable insights for decision-making in financial organizations.

4.2. Case study 2 - CYREM-ORM evaluation in a large UK retail company

4.2.1. Case background and context

This case study examines the application of CYREM-ORM in a major UK online retail company with an average annual revenue of approximately £1.5 billion and over 10 million active customers globally. We chose this retail company due to its wealth of customer data, complex digital infrastructure and complex stakeholder landscape provided a real-world business setting to validate the CYREM-ORM.

The case study was facilitated through direct access to organizational resources and stakeholders. The Chief Information Security Office (CISO), who help coordinated the industrial case study has expertise in both cybersecurity and cybersecurity investment decision-making, which ensure high-quality guidance throughout the application process. It enables us to use the realistic cyber threat data and company's financial indicators that allows us to test the effectiveness of the model in a real business environment. Table 3 summarizes the processes of the case study.

4.2.2. Case application process

The case study was conducted through three phases, lasted for about one month. In Phase 1, we introduced CYREM-ORM through a training session. This session covered CYREM-ORM's theory and core concepts, highlights how CTI integrates with the FAIR model. Using one demonstrative case, we trained users on the model's operation and application to ensure they understood both theory and application before conducting risk assessments. In Phase 2, we applied the CYREM-ORM using realistic organizational data (with data masking: such as masking partial data of the server names, and perturbation, such as slightly modify numerical data points, e.g. adjusting loss figures by a small percentage) (Little, 1993). The CISO of the retail company coordinated this application. The retail company first provided their business details and key assets. Using this information, we populated the system with relevant threat profiles and vulnerabilities from CTI databases that could affect their business environment. Given the sensitivity of the company's systems and assessment data, we handed the interactive system to the company to independently populate the organizational data required as inputs for the CYREM-ORM. This approach ensures data confidentiality while allows the retail company to directly interact with the CYREM-ORM and populate data such as system vulnerabilities, and asset assessments. In Phase 3, we reviewed the populated data and model results together with the company through two interviews. Using retail industry benchmarks, we first discussed how they made their assessments and, with their agreement, adjust the data to better match their risk reality. In the second interview, we collected feedback on how transparent CYREM-ORM was to use, how useful the outputs were, and how well on its transparency which could help explain cyber risk in financial terms to senior stakeholders. This process combined structured data collection with flexibility to uncover real-world implementation issues and improvement needs.

4.2.3. CYREM-ORM application process

Assets Identification. The retail company's key assets include

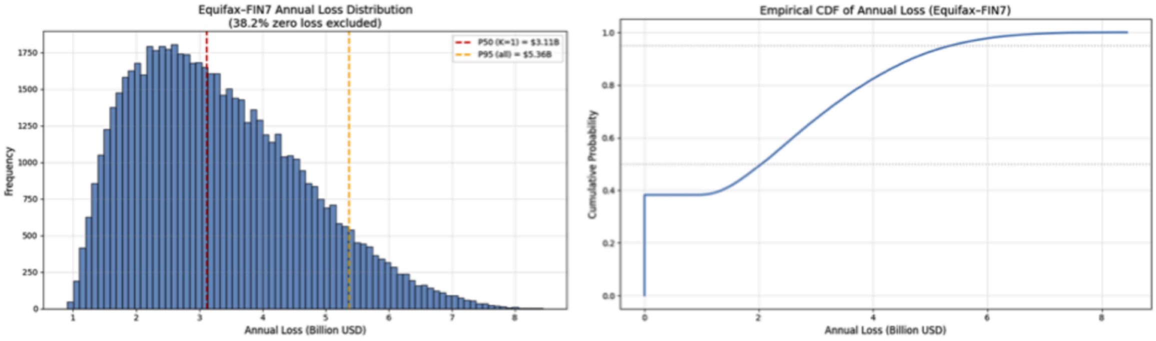

Figure 3(a). Equifax - FIN7 annual risk distribution

Figure 3(b). Equifax - FIN7 empirical CDF of annual risk

Fig. 3. Monte Carlo results of Equifax-FIN7 scenario.

Table 3
An instrumental case study of CYREM-ORM application in a large retail company.

Context: 62 % of companies have experienced cybersecurity incidents caused by poor management between departments about cybersecurity risks. We designed CYREM-ORM to help improve their cyber risk assessment and communication.

Objective: To understand how CYREM-ORM can be applied in a retail organization setting to translate technical cyber risks into financial terms and facilitate cross-departmental risk communication.
Study design: Single instrumental case study with three phases
The case: A major UK online retail company
Data collection:
Phase 1 (Training Phase):
- Conducted a semi-structured interview to understand the risk assessment method using in the company.
- Conducted comprehensive training on the CYREM-ORM model, includes theoretical basis and key concepts explanation, practical training through cases.

Phase 2 (Application Phase):
- Started to apply CYREM-ORM using organizational data.
- The retail company provided basic information such as industry, business operations, and key assets.
- Pre-filled relevant threat actor profiles and vulnerability information based on company characteristics.
- Handed over the interactive system to the company to independently fill in the organizational data.

Phase 3 (Evaluation Phase):
- Reviewed the populated data and model results, made necessary fine-tuning based on retail industry benchmarks (in Review 1).
- Obtained company feedback on the evaluation process (in Review 2).

Key findings:
1. The model shows a consistent perceived improvement across the relevance, traceability, actionability, auditability and proactive dimensions.
2. The model requires continuous threat intelligence updates to maintain current information. Moving to the board level requires higher-level summaries and automated data imports to reduce ongoing explanation and maintenance work.

customer data, e-commerce platforms, and supply chain systems that are important for operations and maintaining customer trust.

TEF assessment. CYREM-ORM uses the CTI database to identify threat actors targeting the company. We found that Magecart is a key threat, which attacks e-commerce sites to steal payment card data and has hit over 70,000 websites (Sansec Forensics Team, 2024). For $CF_{Magecart}$, the value is set to 1 (see Table 1). Magecart exhibits expert-level skills ($SL_{Magecart} = 0.714$) and team-level resources ($RL_{Magecart} = 0.667$), giving a capability score of $C_{Magecart} = \sqrt{0.714 \times 0.667} \approx 0.69$ (Eq. (2)). Magecart's ‘financial-gain’ motive makes it very likely to target the company, $M_{Magecart} = 1 - (1 - 1.0) = 1$ (Eq. (3)). Their objectives are payment data theft and card-skimming, with the former considered of highest relevance and the latter of high relevance by the interviewee, giving $G_{Magecart} = 1 - (1 - 1.0)\ (1 - 0.8) = 1$ (Eq. (4)). Since the company's location and industry match Magecart's typical targets, $L_{Magecart} = 1$ and $S_{Magecart} = 1$ (see Table 1). Based on these parameters, the Probability of Action is calculated as $PoA_{Magecart} = 0.69 \times 1 \times 1 \times 1 \times 1 = 0.69$. Thus, the Threat Event Frequency is $TEF_{Magecart} = 0.69 \times 1 = 0.69$ (Eq. (6)).

LEF assessment. Security scans found four vulnerabilities in the retail company's e-commerce platform. Analysis showed that Magecart, a known hacking group, had exploited similar vulnerabilities before. One vulnerability stood out: CVE-2019–11,043, a PHP-FPM flaw that allows attackers to run malicious code on the e-commerce server. This is especially risky for the company because it could expose payment data and is hard to fix without stopping business operations. The security team rated this as a critical threat ($VL_{Magecart} = 1.0$). Thus, the LEF point estimate is $0.69 \times 1 = 0.69$. We transform LEF point estimate into a Bernoulli event variable: $LEF_{Magecart} \sim$ Bernoulli ($p = 0.69$) (Eq. (8)).

PLM and SLM assessment. The PLM in this case is the cost of repairing, replacing and hardening the two core e-commerce web servers affected by CVE-2019–11,043 (CVSS score = 9.8). This cost belongs to the technical costs of detection and upgrade and post-event response (Heyburn et al., 2020). Based on the CISO’s assessment, the servers would require approximately £20 M for rebuild and security enhancement. Business interruption costs (including e-commerce platform downtime and lost sales revenue during remediation) were estimated at £3 M. To reflect uncertainty about the expert judgement, we model PLM as a PERT distribution, treat £20M+£3 M as the mode parameter (m), and anchor the minimum (a) and maximum (b) using industry evidence. Specifically, we anchor the total loss using comparable UK retail companies’ data breach incidents, then apply IBM's five-year benchmark (2021–2025), which reported the proportion of the detection/post-event response costs in total data breach loss, to estimate the lower and upper bounds of PLM. According to the review (see Appendix D.1), the total loss of a data breach is 1.8 %–4.3 % of the annual revenue. Using this range as a benchmark (see Appendix D.1), we took the total loss between £27 M (1.8 % × £1.5 billion) and £64.5 M (4.3 % × £1.5 billion). Based on the IBM's five-year benchmark (2021–2025) (Appendix D.2), the detection & escalation cost and technical handling part in the post-breach response cost are around 35 %–59 % of the total data breach loss. Thus, based on Eq (9), we obtained the PERT distribution of $PLM_{Magecart}$, which is PERT (35 % × £27 M × 9.8, 9.8 × £23 M, 59 % × £64.5 M × 9.8), i.e., PERT (93, 225, 373) £ million (Eq.9 and Eq.10).

For SLM, the retail company identified four categories of secondary losses from the breach. Reputational damage is the largest impact at £30 M, due to potential harm to the brand and customer trust. Regulatory fines (GDPR and PCI-DSS violations) are estimated as £8.7 M. Legal fees and potential lawsuits are around £1 M. Customer defection from people losing confidence in the platform's security is estimated at £2 M. Thus, the mode of the SLM is the sum of these losses, £41.7 M. Based on the IBM's five-year benchmark (2021–2025) (Appendix D.2), the regulatory penalties and legal costs, and the lost business cost (such as revenue loss due reputation damage) are around 41 %–65 % of the total data breach loss (£27M-£64.5 M). Therefore, PERT distribution of $SLM_{Magecart}$ is PERT (41 % × £27 M, £41.7 M, 65 % × £64.5 M), i.e., PERT (11, 41.7, 42) £ million (See Appendix D.3 for detailed calculation processes).

Monte Carlo simulation and risk results. We run a $N = 10^5$ iterations’ Monte Carlo simulation for the Retail-Magecart scenario. In each iteration, we first draw a Bernoulli LEF indicator, $LEF_{Magecart} \sim$ Bernoulli (0.69). Conditional on $LEF_{Magecart} = 1$, we sample $PLM_{Magecart}$ and $SLM_{Magecart}$ from their PERT distributions, and compute the conditional $LM_{Magecart}$. The annual loss is $R_{Magecart} = LEF_{Magecart} \times LM_{Magecart}$. The Monte Carlo results show a conditional median loss (P50) of about £0.26 billion when a Magecart-driven breach occurs (Appendix D.4). Around 31 % of simulated years result in zero loss because no breach occurs, while the remaining years are between roughly £200–400 M. The annual loss distribution (combine the LEF and LM) has a P50 of about £0.26 billion and a P95 of roughly £0.34 billion, which provides a clear risk envelope for this scenario. Fig. 4 shows the histogram of simulated annual loss values and the CDF.

4.2.4. CYREM-ORM feedback and qualitative comparative assessment

We conducted a side-by-side qualitative comparison to assess the feasibility of the CYREM-ORM in the business scenario and its role in organizational cybersecurity investment decisions. Through a semi-

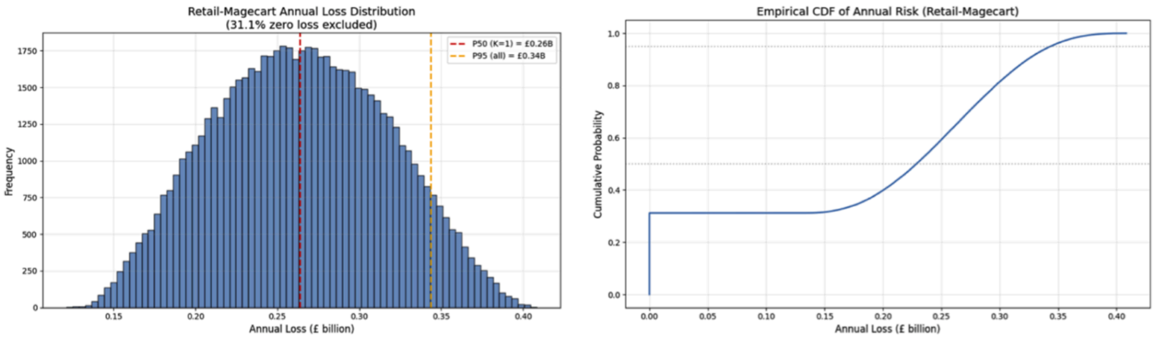

Figure 4(a). Retail - Magecart annual risk distribution

Figure 4(b). Retail - Magecart empirical CDF of annual risk

Fig. 4. Monte Carlo results of Retail-Magecart scenario.

structured interview with their CISO who is responsible for the company's internal cybersecurity risk assessment and reporting to the board of directors. We compared the organization's existing risk assessment method (baseline) and the method model provides in terms of transparency and proactive aspects of risk assessment. Specifically, we use six dimensions to evaluate the model. Among those, five dimensions assess how the model improves the organization's cybersecurity risk assessment in terms of transparency. These dimensions capture aspects that are critical to decision makers and can be supported by evidence:1) relevance (whether model outputs match the organization's assets and vulnerabilities, and are useful); 2) timeliness (whether outputs reflect recently active APTs/TTPs/CVEs and can be updated continuously); 3) actionability (whether outputs provide decision makers with risk ranking and guidance); 4) traceability (whether each financial loss can be traced back to APTs/TTPs/CVEs - assets - PLM/SLM components and assumptions); 5) auditability (whether the model has clear parameters, source dictionaries, and calculation trails for financial and internal audit verification). Together, these five dimensions form a complete definition of transparency. The sixth dimension evaluates the model's proactive capability, specifically whether the CYREM-ORM can provide early warning of future threats to the organization, rather than only responding to known attacks. These six dimensions come from two recognized sources: threat intelligence quality attributes (relevance, timeliness, actionability, and proactiveness) (ENISA, 2025) and risk governance attributes (traceability and auditability) (Al Fikri et al., 2019; NIST, 2012).

To assess and qualitatively compare the impact of the model on the transparency and proactivity, we used the semi-structured interview and related materials (corporate risk registers, annual budget schedules, CTI acquisition methods, etc.) about the original risk assessment method as a reference, pairing them with two post-interviews and model outputs (threats, losses, risks, source dictionaries). We extracted the original contents from interviews across the six dimensions and conducted triangulation (Carter, 2014; Patton, 1999), presents "baseline interview excerpts/post-interview excerpts/key changes" side-by-side in Table 4. The baseline focuses on parent risk and negotiated budget, while the model emphasizes financialized threat-related outputs, traceable computational chains, continuous CTI updates and reduced black-box judgments.

As shown in Table 4, compared to the baseline, the model shows a perceived improvement across the four dimensions of relevance, traceability, actionability, and auditability. The model now ties threats to specific monetary amounts and rankings, and traces those amounts back through attackers, techniques, and CVEs down to individual assets. This creates a clear risk path, which shows the monetary losses of specific risks rather than relying on black-box judgment. However, from the feedback, two conditions are needed to expand these gains. First, the model needs continuous threat intelligence updates to stay current. Second, moving to the board level requires higher-level summaries and automated data imports to reduce ongoing explanation and maintenance. Overall, users shifted from making subjective, unexplained calls to using a process they could explain, verify and for budget conversations.

Table 4
Comparative evidence for transparency and proactivity: baseline vs post-model.

Dimensions	Interview Excerpt (Baseline)	Interview Excerpt (feedback of CYREM-ORM)	Key Changes brought by CYREM-ORM
Relevance	"We have a corporate risk register… we capture a parent risk… reviewed by our PLC board and our executives."	"It provides a specific financial and threat-based output that links posture to risk."	Shift from parent-level risk to a threat-driven, monetization-based narrative, matching the organization's context.
Timeliness	"We start budgeting in December for the next year… submit a wish list to build and run budget…"	"It would need to be continuously refreshed from threat intelligence sources."	Their current baseline method is based on an annual pace; CYREM-ORM enables continuous CTI updates to maintain recentness.
Actionability	"We set a plan and a budget… the decision was ultimately made by the CFO."	"Shows the financial risk exposure… making it easier to justify priorities."	Shift from negotiated budgeting to risk prioritization; reporting anchored to monetary exposure.
Traceability	"That risk is quantified by myself… (to ensure) an accurate reflection of risk exposure."	"With the tool, the transparency improves… I can show the calculations and justify why those three are needed."	From individual judgement to a traceable computational path (threat - asset - PLM/ SLM - monetary risks).
Auditability	"We have independent financial audits annually… internal information security audits."	"People don't see a black box anymore."	The model support independent verification of finance and internal audit with parameter-source dictionaries and calculation trajectories.
Proactive	"We introduced vulnerability scanning… providers will let us know if there's an emerging threat…"	"Helpful… to implement extra security controls in response to emerging threat actors."	Shift from passively waiting for procedural prompts to proactive control based on intelligence signals.

4.3. Case study 3 - CYREM-ORM evaluation in an education consulting SME

4.3.1. Case background and context

Case 3 evaluates CYREM-ORM in a SME education consulting company based in China. The company’s main business is international education and career services. The company has 38 employees, with an average annual revenue of nearly RMB 10 million (around $1.4 million), and a profit margin of 60–70 %. The company has an information system developed and supported by a third party. This company was selected as a representative of the SMEs for several reasons: 1) it handle a large amount of sensitive personally identifiable information (PII) (i.e. student financial data, academic transcripts, passport data), and data exchanges with overseas educational institutions, which increases its attack surface; 2) it has limited legal awareness despite processing cross-border data (China-EU-US) under multiple privacy frameworks (GDPR, FERPA); 3) it relies on outsourced IT services and third-party developed systems like the reality for most SMEs globally, which may lead to security oversight gaps; 4) it has limited cybersecurity budget and lacks technical expertise to assess outsourced security services, which creates knowledge asymmetry.

4.3.2. Case application process

Case 3 was conducted over a two-week period with three phases. Phase 1 offers a training session with the SME management team (managing director, financial staff) and outsourced IT personnel. We designed role-specific training materials: accessible explanations with a simplified example of CYREM-ORM's theoretical foundation for the SME management team, and more technically focused explanations of the framework's underlying principles for outsourced IT personnel. Phase 2 is the data collection process. We applied CYREM-ORM using realistic organizational data, coordinated jointly by the SME management team and outsourced IT personnel. The SME management team first provided details including client data types, regulatory compliance requirements, and critical business assets (e.g. database, communication servers). Based on this information, we pre-populated relevant threat profiles that target education organizations and SMEs from multiple CTI databases, such as sector-specific threat intelligence feeds and recent breach reports from similar organizations. Given the sensitivity of the company's systems and data, the SME management team and outsourced IT personnel independently populate the organizational data required as inputs for CYREM-ORM. Phase 3 evaluated the results and obtained feedback from the SME management team and outsourced IT personnel. We first reviewed the population data and results of CYREM-ORM with the participants, learned about their evaluation process, and discussed how the inputs and outputs fit with their actual situation. We then conducted structured interviews with both the SME management team and outsourced IT personnel to collect feedback. The evaluation focused on two dimensions: CYREM-ORM's accessibility for SMEs with limited cybersecurity expertise, and its feasibility and cost-effectiveness in enabling CTI-driven risk management. Feedback from the case study showed CYREM-ORM's potential and limitations across these dimensions, which are critical to determine the model's applicability in SME environments where cybersecurity is outsourced (see Table 5 for details).

4.3.3. Model application process

Assets Identification. The SME’s key assets include customer (student) personal identifiable information, overseas institutional contact information and their partnerships agreements, system platform and backend databases, etc.

TEF assessment. A key identified T_n is Vice Society (VS), which primarily targets the education and healthcare sectors in ransomware attacks to steal data and extract ransom (*Vice Society*, 2023). Based on the system logs and VS’s characters, the interviewees consider CF_{VS}=0.5. CTI shows VS has the “Intermediate” sophistication level (SL_{vs} = 0.429) and “team” level supported resources (RL_{vs}= 0.667), resulting in $C_{VS} = \sqrt{0.429 \times 0.667} \approx 0.54$ (Eq. (1)). VS's main motive is ‘financial-gain’, which is rated by the interviewee as highly likely to target this SME, giving $M_{vs} = 1 - (1 - 0.8) = 1$ (Eq. (2)). Its extortion goal has high relevance, giving $G_{vs} = 1 - (1 - 0.8) = 1$ (Eq. (3)). VS is known to attack on healthcare, educational and manufacturing organizations. Since this SME falls within its target scope, S_{vs}= 1. Although VS mainly target companies in U.S. and Europe (*Vice Society*, 2023), its motivation

Table 5
An instrumental case study of CYREM-ORM Application in an education SME.

Context: Most SMEs lack cybersecurity expertise and rely heavily on outsourced IT services, which make them vulnerable to targeted attacks. The designed CYREM-ORM is to provide proactive CTI-driven risk assessment for resource-constrained SMEs.

Objective: To understand how CYREM-ORM can be applied in an SME setting to enable proactive threat management and translate technical cyber risks into financial terms for management decision-making.
Study design: Single instrumental case study with three phases
The case: An education SME
Data collection:
Phase 1 (Training Phase):
- Conducted two training sessions (total 2 h) with three participants (managing director, financial staff, outsourced IT personnel).
- Provided accessible explanations and examples of CYREM-ORM for the managing director and the financial staff.
- Provided technically focused explanations of CYREM-ORM for outsourced IT personnel.

Phase 2 (Application Phase):
- Used realistic organizational data with appropriate confidentiality measures to apply the CYREM-ORM.
- The SME supplied necessary business details and critical assets.
- Pre-populated relevant threat profiles targeting education organizations and SMEs from CTI databases.
- Handed over the interactive system to the SME to enable outsourced IT personnel and management team to collaboratively populate organizational data inputs.

Phase 3 (Evaluation Phase):
- Reviewed the populated data and model results with participants.
- Assessed alignment between inputs/outputs and actual organizational situation.

Key findings:
1. CYREM-ORM can translate technical cybersecurity risks into financial terms that non-technical management can understand and prioritize.
2. CYREM-ORM shows accessibility for SMEs with limited cybersecurity expertise through automated CTI mapping and step-by-step guidance.
3. CYREM-ORM shows cost-effectiveness potential by enabling SMEs to focus limited security budgets on high-impact areas.
4. CYREM-ORM cannot directly apply countermeasures in outsourced environments, which lead to delayed responses.
5. CYREM-ORM does not integrate with SIEM/SOC systems, limiting real-time monitoring and automated updates.
6. The model does not consider ongoing maintenance costs or long-term dynamics in outsourcing partnerships.

Main limitations: The application focused on a single educational SME, which may limit generalizability to other sectors. However, the study provides valuable insights into CYREM-ORM's applicability for resource-constrained organizations and suggests potential for broader SME adoption with appropriate system integrations to reduce dependence on cybersecurity expertise.

and goal are considered highly relevance to the SME by the interviewee, resulting in $L_{vs} = 0.5$ (Table 1). Based on these parameters, the Threat Event Frequency is calculated as $TEF_{VS} = 0.54 \times 1 \times 1 \times 1 \times 0.5 \times 0.5 \approx 0.14$ (Eq. (6)).

LEF assessment. Security scans found three critical vulnerabilities in the SME education company's systems: CVE-2021–34,527, CVE-2020–0796, and CVE-2018–13,379. A threat actor (VS) has previously exploited CVE-2021–34,527 and CVE-2018–13,379 to deploy ransomware like Zeppelin and HelloKitty (*Vice Society*, 2023). These two vulnerabilities are problematic because they enable attackers to gain admin access and run code on domain controllers that store student data, risking exposure of personal information. SMEs typically lack proper patch management and network isolation, making them vulnerable. The outsourced IT personnel rated it as very highly vulnerable ($VL_{VS} = 1.0$) of the company. Thus, the LEF point estimate here is $0.14 \times 1 = 0.14$. LEF is then transformed into a Bernoulli event variable: $LEF_{FIN7} \sim$ Bernoulli ($p = 0.14$).

PLM and SLM assessment. We assess the PLM and SLM that would result if VS successfully exploited CVE-2021–1675 (7.8) and CVE-2021–34,527 (8.8) in the SME. Based on the knowledge of the outsourced IT personnel, these vulnerabilities primarily affect the company’s main application server and domain controller, which manage student data and university communications, with asset values of approximately 20–40k CNY. The criticality score is calculated as $(8.8 + 7.8) / 2 = 8.3$. According to Eq (9), the PERT distribution of PLM_{VS} is PERT (20×8.3, 30×8.3, 40×8.3), i.e., PERT (166, 249, 332) k CNY (Eq.10). For the education consulting SME, SLM primarily consist of regulatory penalties. Fines from regulators are a major secondary loss. Based on recent cases in China targeting training institutions as the lower bound, the outsourced IT personnel’s estimate as the mode, and the 5 % annual revenue cap stipulated in China's Personal Information Protection Law for violations as the upper bound (Franco et al., 2024), we model regulatory penalties as PERT (10, 80, 500) k CNY, which can be seen as SLM_{VS}.

Monte Carlo simulation and risk results. We run a $N = 10^5$ iterations’ Monte Carlo simulation for the SME-VS scenario using the same process as in case study 2. Monte Carlo simulations show that, assuming a successful attack from VS ($K = 1$), the P50 is approximately 38k CNY. Approximately 86 % of the years will result in zero loss, and P50 for the remaining years with positive losses is also around 38k CNY, the P95 is approximately 55k CNY (see Fig. 5 and Appendix E for details).

4.3.4. *CYREM-ORM applicability to SME scenarios*

We used two prior interviews with SME management team and outsourced IT personal respectively was used as a baseline to compare the two aspects (collaborativeness and sustainability) of the value the model might bring to SMEs; and presented the evidence (see Table 6) observed when using the model. Collaborativeness assesses whether non-security managers and outsourced staff can collaboratively use the model to complete and reproduce an assessment with minimal guidance. Sustainability refers to whether the SME can continuously use the data and conduct the risk assessment at low cost.

Table 6
Comparative evidence for transparency and proactivity: baseline vs post-model.

Dimensions	Interview excerpt from management (baseline)	Interview excerpt from security personnel (baseline)	Evidence observed
Collaborativeness	“Our company doesn’t have its own IT department… we rely heavily on outsourced IT…” “but I expect them to explain in plain language.”	“I review logs, … vulnerability scans… we prepare a report and summarize their security status.”	After training both parties, they took about 40 min to collaborate and complete the first risk assessment using the model. During the trial, the facilitator provided assistance three times. After the trial, both parties stated that the model helped them define their roles during collaboration.
Sustainability	“We rely on outsourced… I sign budgets and communicate with outsourcing providers.”	“I wish … improve communication efficiency… engage us earlier in projects and budget planning.”	The company's management team felt the model has the potential to reduce the time spent on risk assessments and decrease dependence on third-party services.

In this trial, both the SME management team and outsourced IT personnel noted the model clarified their roles, which shows the model’s collaborativeness. Management felt the model could reduce risk assessment time and third-party dependence (sustainability). However, the outsourced IT personnel pointed out that, the use of the model is limited by manpower and data collection. If it can be integrated with their existing security monitoring system and automate real-time threat monitoring, it will further reduce reliance on experts and decrease outsourcing costs. The SME management team expressed interest regarding the overall cost of model adoption and the extent to which it can replace third-party services, which indicates that a period of observation is necessary to fully assess these aspects.

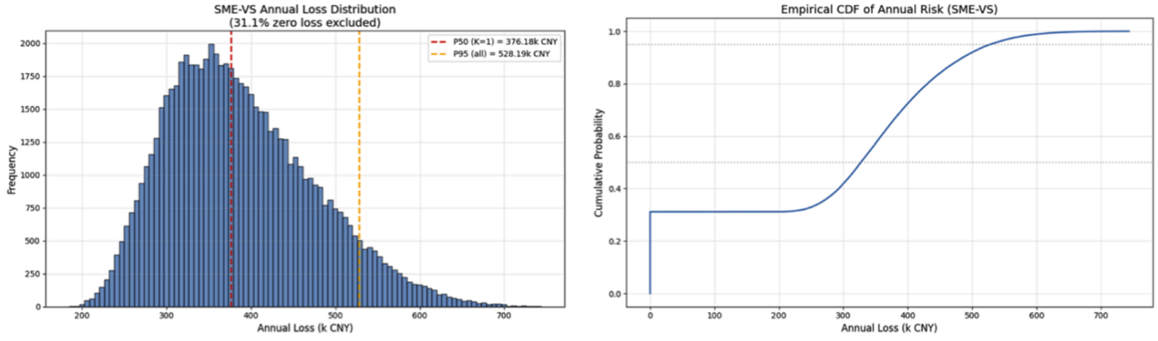

Figure 5(a). SME - VS annual risk distribution

Figure 5(b). SME - VS empirical CDF of annual risk

Fig. 5. Monte Carlo results of SME-VS scenario.

5. Discussion

This study introduces CYREM-ORM, a cyber risk economics model for organization-wide risk management that translates technical CTI and control information into financial terms through transparent, traceable pathways. By integrating STIX-based CTI with the FAIR framework and the cost typology, CYREM-ORM not only expresses complex threats and vulnerabilities as distributional monetary loss estimates, but also supports proactive screening and ranking of organization-specific risk scenarios in line with their business goals. The model's use of CTI to estimate event frequency and to apply Monte Carlo simulation reduces dependence on subjective expert opinions and generic risk scenarios, and allows stakeholders to see how specific threat actors, attack methods, vulnerabilities, affected assets, and cost factors combine to produce final loss estimates. Across three case studies, the 2017 Equifax breach analyzation demonstrates that CYREM-ORM can produce realistic pre-breach risk estimates that fall within observed loss ranges, while the large UK retail and Chinese SME application show perceived improvements in relevance, timeliness, actionability, traceability, auditability, and proactiveness compared with their baseline practices. These findings suggest that CYREM-ORM strengthens organization-wide cyber risk management by making CTI-based risk assessments more transparent.

5.1. Contributions

First, CYREM-ORM contributes a transparent intelligence-to-impact workflow that makes CTI-based monetary risk estimates more interpretable for both technical and business stakeholders. Previous research shows that organizations struggle with cross-department communication in risk assessment. Meanwhile, CTI research and practice have largely focused on technical sharing mechanics (e.g., formats, exchange protocols) and on improving detection and response, but have offered limited business-facing methods that clearly explain how concrete threats translate into financial exposure for decision makers, nor provides traceable steps that boards can verify (Dekker and Alevizos, 2024; Qamar et al., 2017). FAIR and its extensions improve the economic articulation of cyber risk, but published standards and commercial tools often hide the connections between adversaries, attack methods, vulnerabilities, and the final monetary estimates. This "black box" problem undermines trust and makes results hard to verify or replicate. CYREM-ORM resolves this by connecting CTI data (STIX format) to risk factors (TEF, LEF, PLM, SLM), breaking down losses by cost type, and calculating potential losses through Monte Carlo simulation. Every scenario's monetary loss can be traced back to the threat actors, techniques, vulnerabilities, assets, and cost components that produced it, with documented parameters and calculation steps. In the retail and SME cases, decision makers highlighted improved relevance, traceability and auditability of the risk assessment process when using the model. These cases demonstrate CYREM-ORM provides a transparent, verifiable bridge between threat analysis and financial risk stories to break the language barriers.

Second, the CYREM-ORM shifts organizations from passive to proactive risk assessments as it is continuously fed with up-to-date CTI, which greatly expands organizations' strategic perspective when conducting organizational wide risk assessment at a strategic level. Many organizations plan their cybersecurity budgets based solely on past incidents, without considering evolving threats (Merah and Kenaza, 2021; Sun et al., 2023). Compliance-focused companies often use outdated prevention methods and fixed risk management strategies which struggle to keep up with the rapid changing threat environment and growing attack surfaces, which can lead to flawed risk assessments (Kotsias et al., 2023). Even with advanced cyber defenses, organizations struggle to build strong protections because they do not fully understand how threats evolve and the lack experience handling complex attacks such as APTs (Ahmad et al., 2021). Organizations requires risk assessment methods that can adapt quickly to new threats. The CYREM-ORM uses CTI to filter and prioritize threat actors whose sector, location, motivation, goals and observed CVEs match the focal organization, and to parameterize TEF and vulnerability based on observed campaigns and contact patterns. This design allows risk scenarios to be refreshed as new CTI arrives (Kotsias et al., 2023; Shin and Lowry, 2020; Skopik, 2017), and allows organizations to respond to emerging threats by deploying appropriate security measures and making informed investment decisions (Ettinger, 2019).

Third, the CYREM-ORM advances the semi-automation of CTI-driven cyber risk quantification by structuring which FAIR parameters can be populated from structured CTI vocabularies and cost typologies, and which still require expert judgement. Current threat intelligence and automation tools focus mostly on detecting and connecting threats, while FAIR risk analysis typically requires many expert meetings and broad industry data. CYREM-ORM bridges this gap by mapping STIX SDOs to FAIR variables, quantifying rules for threat-actor properties, and proving a reusable loss typology. This setup allows threat data and system logs to feed the model automatically, so stakeholders only need to identify critical assets and estimate potential costs. In the SME case, managers and IT experts handled business details while the model processed threat data and showed that CYREM-ORM offers a practical blueprint for semi-automated, CTI-driven risk assessments in resource-constrained settings.

Fourth, the study offers an empirical, multi-case illustration of CYREM-ORM and complements conceptual research on CTI-enabled FAIR applications and commercial CRQ tools. Existing research on integrating CTI into risk assessment is still at an early stage and imbalanced towards technical aspects; few studies examine how CTI-based assessments are understood and used by non-technical stakeholders or embedded in broader risk management processes. Early CTI- and FAIR-related work (e.g., using CTI to populate LEF and vulnerability) mainly targets cyber security teams. It does not extend to full financial loss scenarios for senior management. Moreover, there is no peer-reviewed research evaluating how industry guidelines or commercial CRQ tools use CTI to populate FAIR. Our semi-synthetic reconstruction of the 2017 Equifax breach shows that CYREM-ORM can produce annual loss estimates that match reported losses and provides retrospective reality checks. The retail and SME case studies then apply CYREM-ORM in two distinct settings. Through interviews and evaluation across six dimensions (i.e., relevance, timeliness, usefulness, traceability, auditability, proactiveness), we document clear gains in transparency and threat-informed risk discussion compared to their current practices. While these cases are exploratory and focused on specific contexts, they provide a valuable foundation for future evaluations of CTI-FAIR-based cyber risk models, including comparisons with established frameworks and commercial tools.

5.2. Limitations and future directions

This research acknowledges several areas for further development. First, the effectiveness of CYREM-ORM relies on the quality of CTI, including its accuracy, timeliness, availability, and completeness. While imperfect CTI could influence risk assessment results, ongoing advances in CTI and commercial products in recently years are expected to provide increasingly robust data for CYREM-ORM.

In addition, although our current study includes an illustrative backtest using the Equifax case, further systematic robustness and benchmarking analyses would help quantify the model's sensitivity to key assumptions and compare its results with other solutions. Future work could incorporate parameter-sensitivity exercises and comparative evaluations to provide deeper insights into CYREM-ORM's stability, reliability, and its loss estimation compared with commercial solutions.

Finally, CYREM-ORM demonstrates strong potential for practical implementation. Future research could explore automated systems, particularly by leveraging artificial intelligence in CTI collection and analysis (Dekker and Alevizos, 2024). Such developments could offer accessible, cost-effective solutions for organizations, especially SMEs with limited cybersecurity resources. We will also consider integration with mature cybersecurity systems such as SIEM (Security Information and Event Management) (Cinque et al., 2018) and Security Operations Centre (SOC) (Onwubiko, 2015).

6. Conclusion

This research has introduced the novel CYREM-ORM, a CTI-driven cyber risk economics model that connects STIX-based intelligence, FAIR and a cost typology into a structured pipeline that translates threat intelligence into monetary impacts. By expressing threats as probability distributions of financial losses, the CYREM-ORM improves the transparency of cyber risk discussions and enables organizations to identify relevant threat actors and estimate key risk parameters more effectively. Three case studies demonstrate the model's practical value in terms of relevance, traceability, and actionability within real organizational settings. While further testing and refinement are required, CYREM-ORM provides a practical and transparent foundation for connecting threat intelligence, quantitative financial analysis, and organizational risk management.

Ethical statement

The research was conducted in accordance with established ethical guidelines for academic research. The study received ethical approval from the institution’s research ethics committee (Reference NO QMERC20.565.DSEECS23.070), and all data collection and storage procedures complied with GDPR and relevant data protection regulations. The participating organizations were fully informed about the research objectives and data usage and provided written consent for participation.

Funding

This work is supported by the funding from the Economic and Social Research Council (ESRC), UK Research and Innovation (Grant No ES W/005964/1, Grant No ES W/005964/2).

CRediT authorship contribution statement

Tong Xin: Writing – original draft, Validation, Software, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Ying He:** Writing – review & editing, Writing – original draft, Validation, Supervision, Resources, Project administration, Methodology, Investigation, Funding acquisition, Formal analysis, Conceptualization. **Efpraxia D. Zamani:** Writing – review & editing, Validation, Methodology, Formal analysis, Conceptualization. **Mark Evans:** Writing – review & editing, Investigation, Data curation, Conceptualization. **Cunjin Luo:** Writing – review & editing, Validation, Resources, Methodology, Formal analysis, Conceptualization.

Declaration of competing interest

We declare that there are no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix

A. The taxonomy structure and calculations of FAIR model
Fig. A.

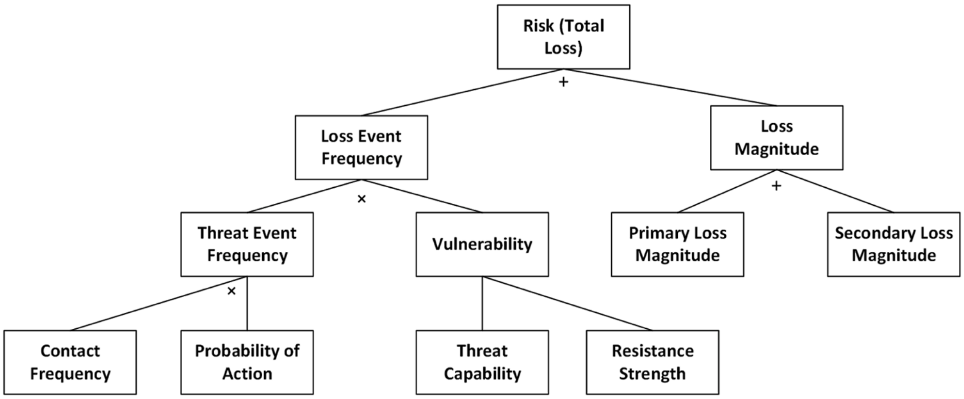

Fig. A. . The taxonomy structure and risk aggregation calculations of the FAIR model.

Table A, Table B, Table C1, Table C4, Table D2, Table D4, Table E2

Table A
. The FAIR model’s risk aggregation calculations.

Equations
Loss Event Frequency = Threat Event Frequency × Vulnerability
Threat Event Frequency = Contact Frequency × Probability of Action
Vulnerability = Resistance Strength × Threat Capability
Loss Magnitude = Primary Loss Magnitude + Secondary Loss Magnitude
Risk = Loss Event Frequency × Loss Magnitude

B. STIX domain objects

Table B
. STIX domain objects and their descriptions.

SDO	Description
Attack Pattern	A type of TTP that describe ways that adversaries attempt to compromise targets.
Campaign	A series of coordinated attacks targeting specific entities over a defined period.
Course of Action	An intelligence producer's advice to a consumer on potential actions in response to that intelligence.
Grouping	Explicitly states that the referenced STIX Objects share a context.
Identity	Actual individuals, organizations, or groups (e.g., ACME, Inc.) as well as classes of individuals, organizations, systems, or groups (e.g., the finance sector).
Indicator	Contains a pattern that can be used to detect suspicious or malicious cyber activity.
Intrusion Set	A grouped set of adversarial behaviors and resources with common properties that is believed to be orchestrated by a single organization.
Infrastructure	Describes a type of TTP involving systems, software services, and related physical or virtual resources designed to fulfill a specific purpose.
Location	Represents a geographic location.
Malware	A type of TTP that represents malicious code.
Malware Analysis	The metadata and results of a particular static or dynamic analysis performed on a malware instance or family.
Note	Provides additional context and analysis not included in the related STIX Objects, Marking Definition objects, or Language Content objects.
Observed Data	Conveys information about cyber security related entities such as files, systems, and networks using the STIX Cyber-observable Objects (SCOs).
Opinion	Evaluating the accuracy of information in a STIX Object created by another entity.
Report	Collections of threat intelligence that concentrate on specific topics.
Threat Actor	Actual individuals, groups, organizations believed to be operating with malicious intent.
Tool	Legitimate software that can be used by threat actors to perform attacks.
Vulnerability	A mistake in software that can be directly used by a hacker to gain access to a system or network.

C. Supplement data of Case Study 1(Equifax Case)

C.1 Brief summary of 2017 Equifax breach.

Equifax is one of the largest credit reporting agencies in U.S. It collects and aggregates information on over 800 million individual consumers. The company's primary services include services include credit reporting and scoring, as well as marketing and fraud prevention services. The data breach exposed the personal information of approximately 147 million consumers. The breach was primarily caused by the vulnerability CVE-2017–5638 in Apache Struts, a popular open-source software used for building web applications (Jai Vijayan, 2020; Mark Meltzer, 2020). Equifax failed to patch this known vulnerability in a timely manner.

Table C1
. 2017 Equifax breach losses and costs.

Category	Amount (USD)
Regulatory Settlement	$575M-$700 M (Federal Trade Commission, 2019)
Consumer Restitution Fund	$380.5 M (Security Magazine, 2020)
Litigation Settlement	$149 M (K. LaCroix, 2020)
Information Security Investments	$1B (pledged over 5 years) (Jai Vijayan, 2020)
UK FCA Fine	£11.16 M (~$14.5 M) (Wikipedia contributors, n.d.)
Total Estimated Cost (2019)	>$1.7B (Federal Trade Commission, 2019)

C.2 Expert assessment of the semi-synthetic Equifax case.

For the Equifax case, we combined a document analysis method (Bowen, 2009) with semi-synthetic data construction (Stojanović et al., 2020). Publicly available information was first collected from regulatory filings, official investigation reports, financial disclosures, and reputable breach and CTI reports describing the FIN7 campaign, the exploitation of CVE-2017–5638, and Equifax’s pre-breach financial position. Where these documents did not provide sufficient numerical detail for CYREM-ORM, we complemented them with structured expert judgement following established procedures for expert-based risk assessment (Hughes, 1996; Otway and von Winterfeldt, 1992). We invited three domain experts with 8–15 years of experience in cybersecurity risk assessment and incident analysis. Each expert received the same data that includes the verified facts from public sources, together with our CYREM-ORM cost typology and CTI-based threat description. After three responses had been submitted, we aggregated the inputs by taking the median for each variable.

Table C.2 summarizes the individual ratings and the aggregated values used in CYREM-ORM. Ratings of CF and VL were based on normalized 0-1 scales defined in Section 3. For business disruption in PLM, experts assess it based on sources (Coveware, 2020; Datto, 2016; IBM, 2016; Intermedia, 2016).

Table C2
. Parameters assessed by experts in Equifax-FIN7 scenario.

Variable	Component	Expert 1	Expert 2	Expert 3	Aggregated value
TEF	CF_{FIN7}	1.0	1.0	1.0	1.0
	M_{FIN7} - financial gain	1.0	1.0	1.0	1.0
	M_{FIN7} - notoriety	0.8	0.5	0.5	0.5
	G_{FIN7} - data theft	0.8	1.0	1.0	1.0
LEF	VL_{FIN7}	0.8	1.0	0.8	0.8
PLM (Business disruption)	Minimum months of profit lost	0.5	0.5	0.25	0.5
	Most likely months of profit lost	1.5	1.5	1.0	1.5
	Maximum months of profit lost	2.5	2.5	2.0	2.5

C.3 Supplement Data for PLM/SLM evaluation.

Equifax operated one of the largest consumer credit databases worldwide before 2017, and had over 820 million consumers. Its net profit in 2016 was $488.8 million, approximately $40.7 million per month. These baselines are used to rescale industry loss ratios to the Equifax context. For the

FIN7 case study, PLM is decomposed into incident response (IR) and business interruption (BI). The interval bounds a and b of each PERT distribution are anchored to pre-2017 breach evidence and industry reports, while the mode m is aligned with Equifax's financial scale and commonly accepted industry containment/downtime ranges. Table C.3 summarizes PERT parameters and their main anchors.

Table C3
. PERT parameters for PLM and SLM in the Equifax-FIN7 scenario.

Component	PERT (a, m,b)	Calculation basis for a,m,b	Resources
Incident response cost	*a* = $493.5M	*a* = $1.33/record × (5 % × 820 M) × 9.05 ≈ $493.5M: in Experian 2015 data breach cost $20 M directly responding to this incident, affected 15 million customers, ≈$1.33/record.	(Commonwealth of Massachusetts, 2022; Marty Frappolli, 2015).
	m = $1545M	*m* = ($170 *M* + $0.73 M) × 9.05 ≈ $1545M: the average cost for data breach investigation and forensics in the US was $0.73 million in 2016, future system repair and security hardening costs $170 M (about twice the annual security budget of $85 M).	(Daswani and Elbayadi, 2021; Target Corporation, 2016; Target cyberattack: A Columbia University case study., 2022; The Home Depot, 2016; IBM, 2016)
	b = $7514M	*b* = $4.05/record × (25 % × 820 M) × 9.05≈$7514M: upper bound reflects a higher per-record direct response cost for a highly regulated, high-sensitivity PII environment. In Target (2013), net breach-related expenses not covered by insurance of $162 M for about 40 M cards, ≈ $4.05/record.	(Target Corporation, 2016; IBM, 2016)
Business interruption	*a* = $184M	*a* = $40.7 *M* × 0.5 month × 9.05 ≈ $184 M, which is the minimum (0.5 month) of Equifax's profit. Since industry surveys in 2016 found that ransomware-affected organizations lost access to critical data for at least two days, and one-third experienced five or more days of downtime. Coveware (2020) reports that larger organizations typically experience 1~3 weeks of downtime from ransomware attacks, with full recovery often taking several weeks.	(Coveware, 2020; Datto, 2016; Intermedia, 2016)
	M≈ $552.5M	*m* = $40.7 *M* × 1.5 month × 9.05 ≈ $552.5 M, which is the medium (1.5 month) of Equifax's profit. The window of opportunity for containing and resolving malicious data breaches is approximately one to three months.	(IBM, 2016; Verizon, 2016)
	b = $921M	*b* = $40.7 *M* × 2.5 month × 9.05 ≈ $921 M, which is the maximum (2.5 month) of Equifax's profit. The window of opportunity for containing and resolving malicious data breaches is approximately one to three months.	(Target Corporation, 2016; IBM, 2016)
Regulatory compliance and legal fees	*a* = $137.3M	*a* = $12.3 *M* + $125 *M* = $137.3 M. In Target 2013, 40–110 M customers received the total $10 M settlement fee, thus payment to the individual is $0.3/record × 5 % × 820 = $12.3 M. Target's total payments to banks and card organizations are approximately $125 M.	(Kelli Young, 2021; *Target cyber attack: A Columbia University case study.*, 2022)
	m = $351.5M	*m* = $209 *M* + $142.5 *M* = $351.5 M. In Anthem (2015), ~$1.46/record of settlement fee per person. In Capital One (2019), ~ $1.8–1.9/record of settlement fee per person. We use the median value of them, $1.7/record × 15 % × 820 = $209 M. We choose the median value of these organizations' payments to banks and card organizations, which is approximately $142.5 M.	(California Department of Insurance, n.d.; Capital One, 2022; Steve Alder, 2018)
	b = $754.5M	*b* = $594.5 *M* + $160 *M* = $754.5 M. In the Office of Personnel Management data breach, ~$63 M for ~21.5 M victims, around $2.9/record. Thus, $2.9/record × 25 % × 820 = $594.5 M. Home Depot total payments to banks and card organizations are approximately $160 M.	(The Home Depot, 2016; Top Class Actions, 2017)
Reputational Damage	*a* = $2M	*a* = $488.8 *M* × 0.4 % ≈ $2 M. The lower bound (0.4 %) is anchored in relatively small credit agency incidents (e.g., Experian 2015), where non-recurring breach-related costs well below 1 % of annual revenue.	(Commonwealth of Massachusetts, 2022)
	≈ $5M	*m* = $488.8 *M* × 1 % ≈ $5 M. The mode (1 %) reflects data-intensive consumer service breaches, such as the 2015 TalkTalk attack, where the breach led to a ~1 % year-on-year revenue decline, primarily driven by customer churn and reduced usage.	(Dan Cancian, 2016; Paul Sandle, 2016).
	b ≈ $14.7M	*b* = $488.8 *M* × 3 % ≈ $14.7 M. The upper bound (3 %) is from Capital One (2019), customer confidence after the data breach took a hit, which is expected to reduce Capital One's revenues by 3 % in 2019, 2020 and 2021 with respect to the base model, similar with major retail breaches like Target 2013.	(Capital One, 2022; Kelli Young, 2021; *Target cyber attack: A Columbia University case study.*, 2022)

Table C4
. Equifax-FIN7 Monte Carlo simulation details.

Index	Conditional LM (LEF = 1) [$M]	Annual risk (with LEF) [$M]
Mean	3307.71	2038.98
Std	1332.65	1914.1
P50	3117.58	2045.55
P90	5183.13	4679.99
P95	5788.46	5362.02

D. Supplement Data of Case Study 2 (UK Retail Case)

For the UK Retail Case Study, we anchor the total breach impact using comparable UK incidents which shows in the Table D.1. The 2015 TalkTalk breach, the 2025 M&S cyberattack, and the 2025 Co-op incident imply total incident costs in the range of ≈1.8–3.3 % of annual revenue for serious but non-existential events. Rescaling these percentages to our focal retailer yields a plausible total loss range of ≈£27–49.5 m. A complementary per-customer view, using peer incidents with ≈£10-£30 cost per affected customer and assuming 10–20 % of the 10 m customer base is materially impacted, leads to a similar range of ≈£10–60 m.

Table D1
. PERT parameters for PLM and SLM in the Retail-Magecart scenario.

Example company & incident	Field & annual avenue & customer size	Disclosed rough total losses from incidents	Losses as a percentage of revenue	Sources
TalkTalk, 2015	A UK telecommunications operator, with approximately £1.8 billion annual revenue in 2015, around 4 million customers.	approximately £77 M.	£77M/£1.8 billion ≈ 4.3 %	(Dan Cancian, 2016; Paul Sandle, 2016; Sean Farrell, 2016)
Marks & Spencer, 2025	A large UK-based integrated retailer with annual revenue in the range of approximately £14 billion and around 30 million customers.	The cyberattack is expected to result in a profit and operating loss of around £300 M.	£300M/£14 billion ≈ 2.1 %	(Sarah Butler, 2025)
Co-op Group, 2025	A UK-based cooperative retail group with revenue of approximately £11.3 billion and 6.2–6.5 million members in 2024.	A sales loss of £206 M and an operating profit impact of approximately £80M-£120 M, for a total economic shock of ≈£200M-300 M.	£200M-£300M/£11.3 billion ≈ 1.8 %–2.6 %	(Lauren Almeida, 2025)

Table D2
. IBM's five-year benchmark (Year 2021–2025).

Year	Total cost	Detection & Escalation	Notification	Post-breach response	Lost business
2021	4.24	1.24 (29 %)	0.27 (6 %)	1.14 (27 %)	1.59 (38 %)
2022	4.35	1.44 (33 %)	0.31 (7 %)	1.18 (27 %)	1.42 (33 %)
2023	4.45	1.58 (36 %)	0.37 (8 %)	1.20 (27 %)	1.30 (29 %)
2024	4.88	1.63 (33 %)	0.43 (9 %)	1.35 (28 %)	1.47 (30 %)
2025	4.44	1.47 (33 %)	0.39 (9 %)	1.20 (27 %)	1.38 (31 %)

Table D.3 reports statistics separately for the conditional $\mathrm{LM}_{\mathrm{Magecart}}$ and for the annual risk $\mathrm{R}_{\mathrm{Magecart}}$. It listed the “Value” established for each “Component” in the CYREM-ORM. It also lists the “Sources”, where these values are from. The CYREM-ORM processes multi-disciplinary data that is a combination of CTI, and the retail company’s inputs for the calculating process.

Table D3
. Details of CYREM-ORM application in Case Study 2.

Step	Component	Value	Source
Assets identification	Key assets	Critical assets for business operations (e.g., customer data; E-commerce platform; supply chain system, etc.)	Retail Company
TEF evaluation	Sophistication level (SL)	0.714 (Expert)	CYREM-ORM CTI
	Resource level (RL)	0.667	CYREM-ORM CTI
	Capability (C)	$\sqrt{0.714 \times 0.667} \approx 0.69$	CYREM-ORM Calculated
	Motivation (M)	$M = 1$ - (1 - 1.0) = 1	Retail Company & CYREM-ORM CTI
	Goal (G)	$G = 1$ - (1 - 1.0) (1 - 0.8) = 1	Retail Company & CYREM-ORM CTI
	Location match (ML)	1.0 (UK-based target)	Retail Company & CYREM-ORM CTI
	Sector match (MS)	1.0 (Retail sector target)	Retail Company & CYREM-ORM CTI
	PoA	$0.69 \times 1 \times 1 \times 1 \times 1 = 0.69$	CYREM-ORM Calculated
	TEF	$0.69 \times 1 = 0.69$	CYREM-ORM Calculated
LEF evaluation	Identified Vulnerabilities (Vo)	CVE–2024–20,720; CVE–2016–4010; CVE–2024–34,102; CVE-2019–11,043	System Scan Results
	Exploitable Vulnerabilities (Vt)	CVE–2018–9206; CVE–2017–7391; CVE–2019–11,043; CVE-2019–16,535	CYREM-ORM CTI
	Vulnerable vulnerability	CVE-2019–11,043	Analysis
	Vulnerability level	1.0	Retail Company
	Final LEF	$0.69 \times 1 \times 1 \times 1 \times 1 = 0.69$	CYREM-ORM Calculated
Loss Magnitude	CVSS score	9.8	CYREM-ORM CTI
	Impacted asset value	£23M	Retail Company
	Primary Loss (PLM)	$a = 35\,\% \times £27\,M \times 9.8 = £93$ m $= £23\,M \times 9.8 = £225$M (two web servers +BI cost) $b = 59\,\% \times £64.5\,M \times 9.8 = £373$M	CTI (industry reports) CYREM-ORM Calculated
	Reputation Loss (m)	£30M	Retail Company
	Regulatory Penalties (m)	£8.7M	Retail Company
	Business Disruption (m)	£3M	Retail Company
	Legal Costs (m)	£1M	Retail Company
	Customer Loss (m)	£2M	Retail Company
	Secondary loss (SLM)	$a = 41\,\% \times £27\,M = £11$ m = £44.7 M $b = 65\,\% \times £64.5\,M = £42$M	CTI (industry reports) CYREM-ORM Calculated
Risk assessment	Total Risk (R)	P50 = £260 M; P95= £340M	CYREM-ORM Calculated

Table D4
. Retail-Magecart Monte Carlo Summary.

Index	Conditional LM (LEF = 1) [£M]	Annual risk (with LEF) [£M]
Mean	264.2	181.93
Std	53.06	130.03
P50	263.7	228.66
P90	335.49	323.98
P95	352.46	343.69

D.5 Semi-structured interviews for Case Study 2 (UK Retail Case).

To assess and qualitatively compare the impact of CYREM-ORM on transparency and proactivity, we conducted two semi-structured interviews in the large UK retail company before and after the CYREM-ORM trial. The pre-model interview was conducted with their CISO who led risk assessment processes. This interview focused on establish the baseline by identifying the company's current risk assessment practices and governance processes. The interview lasted around one hour and was audio-recorded and transcribed for analysis.

The interview questions include:

1. How do you identify and quantify cyber security risks?

Probes: How risks are captured and assessed; what information or sources are used; how results are reviewed and validated.

2. How are decisions on cyber security coordinated across teams and management?

Probes: Who participates in decisions; how information flows between technical and business teams; how decisions are finalized and communicated.

3. How do you plan and prioritize cyber security investments?

Probes: How budget items are linked to risks; how priorities are set; how trade-offs between internal and external solutions are made.

4. What challenges do you face in assessing risks or making investment decisions?

Probes: Difficulties caused by limited resources, time, or understanding; strategies used to overcome these challenges.

5. How do you handle cyber security incidents and evaluate their impacts?

Probes: How incidents are detected and reported; who is involved in assessing impacts; how financial, operational, or reputational losses are estimated and acted upon.

6. How do you evaluate the effectiveness of your cyber security investments?

Probes: What indicators or metrics are used; how results are communicated to management; how lessons learned inform future investments.

After the CYREM-ORM trial, we conducted the post-model interview and asked the participant to reflect on their experience using the model and to compare it with their baseline approach along the six dimensions reported in Table 4 (dimensions addressed: relevance, timeliness, actionability, traceability, auditability, proactiveness). The interview lasted around one hour and was audio-recorded and transcribed for analysis.

The interview questions include:

1. How does the tool influence the way you identify and quantify cyber risks?

Probes: connections between risks (traceability); clarity of possible actions (actionability); how others can review your assessment (auditability)

2. How does the tool influence your budgeting or planning process?

Probes: linking budget to risks (traceability); speed of review cycles (timeliness); clarity (auditability); choosing what to act on (actionability)

3. How does the tool influence how you work with threat information?

Probes: relevance of threat (relevance); threat updates (timeliness); ability to act ahead of threats (proactiveness)

4. How does the tool influence how you judge and manage residual risk?

Probes: understand how residual risk is derived (traceability); plann mitigation (actionability); transparency for review (auditability)

5. How does the tool influence your communication with senior leadership?

Probes: show risk-business links (traceability); allow managers to verify assumptions (auditability); clarify actions or trade-offs (actionability)

6. How does the tool influence your ability to link risks to financial impacts?

Probes: justify spending (auditability); understand which risks drive which costs (traceability); decide cost-related actions (actionability)

For each dimension, we coded baseline, post-interview excerpts and related data (risk registers, budget schedules). The results reported in Table 4 are drawn from this coding and illustrate how participants perceived shifts from a parent-risk and negotiated-budget narrative towards threat-driven, monetized, and more traceable risk assessments.

E. Supplement Data of Case Study 3 (SME case)

Table E.1 shows the “Value” established for each “Component” in the CYREM-ORM and the "Sources" where these values are derived from. The CYREM-ORM processes multi-disciplinary data that is a combination of CTI, and the retail company’s inputs for the calculating process.

Table E1
. Details of CYREM-ORM application in Case Study 3.

Step	Component	Value	Source
Assets identification	Key assets	Critical assets for business operations (e.g., customer data; E-commerce platform; supply chain system, etc.)	SME
TEF evaluation	Sophistication level (SL)	0.429	CYREM-ORM CTI
	Resource level (RL)	0.667	CYREM-ORM CTI
	Capability (C)	$\sqrt{0.429 \times 0.667} \approx 0.54$	CYREM-ORM Calculated
	Motivation (M)	1 - (1 - 0.8) = 1	SME & CYREM-ORM CTI
	Goal (G)	1 - (1 - 0.8) = 1	SME & CYREM-ORM CTI
	Location match (ML)	0.5	SME & CYREM-ORM CTI
	Sector match (MS)	1.0	SME & CYREM-ORM CTI
	TEF	0.14	CYREM-ORM Calculated
LEF evaluation	Identified Vulnerabilities (Vo)	CVE–2021–34,527; CVE–2020–0796; CVE-2018–13,379	System Scan Results
	Exploitable Vulnerabilities (Vt)	CVE–2021–34,527; CVE–2021–1675; CVE–2020–1472; CVE-2018–13,379	CYREM-ORM CTI
	Vulnerable vulnerability	CVE–2018–13,379; CVE-2021–34,527	Analysis
	Vulnerability level	1.0	SME
	Final LEF	0.14	CYREM-ORM Calculated
Loss Magnitude	CVSS score	(8.8 + 7.8)/2 = 8.3	CYREM-ORM CTI
	Impacted asset value	20~40k CNY (main application server and domain controller)	SME
	Primary Loss (PLM)	$a = 20 \times 8.3 = 166$k CNY $m = 30 \times 8.3 = 249$ k CNY $b = 40 \times 8.3 = 332$k CNY	CYREM-ORM Calculated
	Secondary loss (SLM)	$a = 10$k CNY $m = 80$k CNY $b = 10$ M CNY $\times$ 5 % = 500k CNY	CTI (industry reports) CYREM-ORM Calculated
Risk assessment	Total Risk (R)	P50 = 38k CNY; P95= 55k CNY	CYREM-ORM Calculated

Table E2
. SME-VS Monte Carlo Summary.

Index	Conditional LM (LEF = 1) [k CNY]	Annual risk (with LEF) [k CNY]
Mean	387.38	54.18
Std	87.29	138.18
P50	375.80	0.00
P90	509.23	328.46
P95	548.39	410.79

Data availability

Data will be made available on request.

References

Ahmad, A., Maynard, S.B., Desouza, K.C., Kotsias, J., Whitty, M.T., Baskerville, R.L., 2021. How can organizations develop situation awareness for incident response: a case study of management practice. Comput. Secur. 101, 102122.

Al Fikri, M., Putra, F.A., Suryanto, Y., Ramli, K., 2019. Risk assessment using NIST SP 800-30 revision 1 and ISO 27005 combination technique in profit-based organization: case study of ZZZ information system application in ABC agency. Procedia Comput. Sci. 161, 1206–1215.

Alberts, C.J., Dorofee, A.J., 2003. Managing Information Security Risks: the OCTAVE Approach. Addison-Wesley Professional.

Ampel, B.M., Samtani, S., Zhu, H., Chen, H., 2024. Creating proactive cyber threat intelligence with hacker exploit labels: a deep transfer learning approach. MIS Q. 48 (1).

Anvilogic. (2023). FIN7’s growth and evolution: from financial gains to ransomware collaborations.

Bakare, A.A., 2020. A Methodology for Cyberthreat Ranking: InCorporating the NIST Cybersecurity Framework into FAIR Model. University of Cincinnati.

Barnum, S., 2012. Standardizing cyber threat intelligence information with the structured threat information expression (stix). Mitre Corp. 11, 1–22.

Benaroch, M., 2018. Real options models for proactive uncertainty-reducing mitigations and applications in cybersecurity investment decision making. Inf. Syst. Res. 29 (2), 315–340.

Bowen, G.A., 2009. Document analysis as a qualitative research method. Qual. Res. J. 9 (2), 27–40.

Carter, N. (2014). The use of triangulation in qualitative research. Number 5/September 2014, 41(5), 545–547.

Cavusoglu, H., Cavusoglu, H., Son, J.-Y., Benbasat, I., 2015. Institutional pressures in security management: direct and indirect influences on organizational investment in information security control resources. Inf. Manag. 52 (4), 385–400.

Cinque, M., Cotroneo, D., Pecchia, A., 2018. Challenges and directions in security information and event management (SIEM). In: 2018 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW), pp. 95–99.

Commonwealth of Massachusetts. (2022). Experian 2015 data breach: administrative Order of Determination.

Coveware. (2020). Ransomware costs double in Q4 as Ryuk, Sodinokibi proliferate.

Daswani, N., Elbayadi, M., 2021. Big breaches: cybersecurity lessons for everyone. Big Breaches. https://doi.org/10.1007/978-1-4842-6655-7_4.

Datto, I. (2016). Datto’s state of the channel ransomware report 2016.

Dekker, M., Alevizos, L., 2024. A threat-intelligence driven methodology to incorporate uncertainty in cyber risk analysis and enhance decision-making. Secur. Privacy 7 (1), e333.

Dong, F., Wang, L., Nie, X., Shao, F., Wang, H., Li, D., Luo, X., Xiao, X., 2023. {DISTDET}: a {cost-effective} distributed Cyber threat detection system. 32nd USENIX Secur. Sympos. (USENIX Secur. 23) 6575–6592.

ENISA. (2025). Enisa cybersecurity threat landscape methodology. https://doi.org/10.2824/1888892.

Erola, A., Agrafiotis, I., Nurse, J.R.C., Axon, L., Goldsmith, M., Creese, S., 2022. A system to calculate cyber value-at-risk. Comput. Secur. 113, 102545.

Ettinger, J., 2019. Cyber Intelligence Tradecraft Report: The State of Cyber Intelligence Practices in the United States. Retrieved from Carnegie Mellon University. https://resources.sei.cmu.edu/library/asset-view.cfm.

Franco, M.F., Künzler, F., Von der Assen, J., Feng, C., Stiller, B., 2024. RCVaR: an economic approach to estimate cyberattacks costs using data from industry reports. Comput. Secur. 139, 103737.

Freund, J., Jones, J., 2014. Measuring and Managing Information Risk: a FAIR Approach. Butterworth-Heinemann.

Gong, N.X., 2017. Barriers and Impacts to Adopting Interoperability Standards for Cyber Threat Intelligence Sharing: a Mixed Methods Study. Robert Morris University.

He, Y., Inglut, E., Luo, C., 2022. Malware incident response (IR) informed by cyber threat intelligence (CTI). Sci. China. Inf. Sci. 65 (7), 179105.

He, Y., Xin, T., Luo, C., 2025. Enhancing cybersecurity investment with FAIR-ROSI: a responsible cybersecurity approach to digital society. Inf. Syst. Front. 1–16.

Heyburn, H., Whitehead, A., Zanobetti, L., Shah, J.N., Furnell, S., 2020. Analysis of the full costs of cyber security breaches. Ipsos MORI Rep.

Hughes, R.T., 1996. Expert judgement as an estimating method. Inf. Softw. Technol. 38 (2), 67–75.

IBM. (2016). 2016 Cost of data breach Study: global analysis.

IBM Security, 2025. Cost of a data breach Report 2025. https://www.ibm.com/reports/data-breach.

Intermedia, 2016. Report identifies ransomware's biggest cost to be business downtime. Intermedia.

International Organization for Standardization, 2018. Information Technology — Security Techniques — Information Security Risk Management (ISO/IEC 27005: 2018). ISO/IEC.

Joint Task Force Transformation Initiative. (2012). Guide for conducting risk assessments (NIST Special Publication 800-30, Revision 1). https://doi.org/10.6028/NIST.SP.800-30r1.

Jones, A., Ashenden, D., 2005. Risk Management for Computer Security: Protecting your Network and Information Assets. Butterworth-Heinemann.

Kaspersky.com, 2023. Fluent in Infosec: are c-level executives and IT security managers on the same page? https://www.kaspersky.com/blog/speak-fluent-infosec-2023/.

Kayworth, T., Whitten, D., 2010. Effective information security requires a balance of social and technology factors. MIS Q. Execut. 9 (3).

Kekeya, J., 2021. Qualitative case study research design: the commonalities and differences between collective, intrinsic and instrumental case studies. Contemp. PNG Stud. 36, 28–37.

Kerkdijk, R., Tesink, S., Fransen, F., Falconieri, F., 2021. Evidence-based prioritization of cybersecurity threats. ISACA J. 6.

Kotsias, J., Ahmad, A., Scheepers, R., 2023. Adopting and integrating cyber-threat intelligence in a commercial organisation. Euro. J. Inf. Syst. 32 (1), 35–51. https://doi.org/10.1080/0960085X.2022.2088414.

Krejčí, J., Stoklasa, J., 2018. Aggregation in the analytic hierarchy process: why weighted geometric mean should be used instead of weighted arithmetic mean. Expert. Syst. Appl. 114, 97–106.

Kure, H., Islam, S., 2019. Cyber threat intelligence for improving cybersecurity and risk management in critical infrastructure. J. Univ. Comput. Sci. 25 (11), 1478–1502.

Li, V.G., Dunn, M., Pearce, P., McCoy, D., Voelker, G.M., Savage, S., 2019. Reading the tea leaves: a comparative analysis of threat intelligence. In: 28th USENIX Security Symposium (USENIX Security 19), pp. 851–867.

Li, W.W., Leung, A.C.M., Yue, W.T., 2023. Where is IT in information security? The interrelationship among IT investment, security awareness, and data breaches. MIS Q. 47 (1), 317–342.

Little, R.J.A., 1993. Statistical analysis of masked data. J. Off. Stat. 9 (2), 407.

Meltzer, Mark, 2020. Equifax says data breach has cost it nearly $2 billion so far. Atlanta Bus. Chronicle.

Melvin, Joshua, 2014. Orange: Hackers Nab Data from 800,000 Clients. February 3. The Local France.

Merah, Y., Kenaza, T., 2021. Ontology-based cyber risk monitoring using cyber threat Intelligence. In: ACM International Conference Proceeding Series. https://doi.org/10.1145/3465481.3470024.

Mori, I., Heyburn, H., Whitehead, A., Zanobetti, L., Shah, J.N., & Furnell, S. (2020). Analysis of the full costs of cyber security breaches Analysis of the full costs of cyber security breaches literature review annex.

NIST. (2012). NIST Special publication 800-30 revision 1. https://doi.org/10.6028/NIST.SP.800-30r1.

Nwafor, C.N., Nwafor, O., Brahma, S., Acharyya, M., 2025. A hybrid FAIR and XGBoost framework for cyber-risk intelligence and expected loss prediction. Expert. Syst. Appl., 129920

Onwubiko, C., 2015. Cyber security operations centre: security monitoring for protecting business and supporting cyber defense strategy. In: 2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cybersa), pp. 1–10.

Otway, H., von Winterfeldt, D., 1992. Expert judgment in risk analysis and management: process, context, and pitfalls. Risk Anal. 12 (1), 83–93.

Patton, M.Q., 1999. Enhancing the quality and credibility of qualitative analysis. Health Serv. Res. 34 (5 Pt 2), 1189.

Pearl, J., 2014. Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference. Elsevier.

Piazza, R., Darley, T., Jordan, B., 2021. Stix V2.1. OASIS Standard. June 2021.

Qamar, S., Anwar, Z., Rahman, M.A., Al-Shaer, E., Chu, B.T., 2017. Data-driven analytics for cyber-threat intelligence and information sharing. Comput. Secur. 67, 35–58. https://doi.org/10.1016/j.cose.2017.02.005.

Riesco, R., Villagrá, V.A., 2019. Leveraging cyber threat intelligence for a dynamic risk framework: automation by using a semantic reasoner and a new combination of standards (STIXTM, SWRL and OWL). Int. J. Inf. Secur. 18 (6), 715–739. https://doi.org/10.1007/s10207-019-00433-2.

RiskLens, 2023. Cyber Risk Quantification. June 5. RiskLens.

Ross, R., 2012. Guide for conducting risk assessments. Special Publication (NIST SP). National Institute of Standards and Technology, Gaithersburg, MD. https://doi.org/10.6028/NIST.SP.800-30r1.

ROSS, S.J., 2025. NIST CSF 2.0 and the cybersecurity hierarchy. ISACA J. 1.

Sansec Forensics Team, 2024. What is Magecart? April Sansec.

Seid, E., Satheesh, S., Popov, O., Blix, F., 2024. FAIR: cyber security risk quantification in logistics sector. Procedia Comput. Sci. 237, 783–792.

Shameli-Sendi, A., Aghababaei-Barzegar, R., Cheriet, M., 2016. Taxonomy of information security risk assessment (ISRA). Comput. Secur. 57, 14–30.

Shin, B., Lowry, P.B., 2020. A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability'that needs to be fostered in information security practitioners and how this can be accomplished. Comput. Secur. 92, 101761.

Skopik, F., 2017. Collaborative Cyber Threat Intelligence: Detecting and Responding to Advanced Cyber Attacks at the National Level. CRC Press.

Spears, J.L., Barki, H., 2010. User participation in information systems security risk management. MIS Quarterly 503–522.

Stojanović, B., Hofer-Schmitz, K., Kleb, U., 2020. APT datasets and attack modeling for automated detection methods: a review. Comput. Secur. 92, 101734.

Sun, N., Ding, M., Jiang, J., Xu, W., Mo, X., Tai, Y., Zhang, J., 2023. Cyber threat intelligence mining for proactive cybersecurity defense: a survey and new perspectives. IEEE Commun. Surv. Tutor. 25 (3), 1748–1774. https://doi.org/10.1109/COMST.2023.3273282.

Target Corporation. (2016). 2015 annual report.

Target Cyber Attack: A Columbia University Case Study. (2022).

The Home Depot, Inc. (2016). 2016 annual report.

Tucker, T., 2025. Analyst's guide to cyber risk data sources what data to use to measure, monitor, and manage cyber risk. www.FAIRInstitute.org.

Verizon. (2016). 2016 data breach investigations report.

Vice Society. (2023, August 1). Wikipedia.

Vijayan, Jai, 2020. 2017 Data breach will cost Equifax at least $1.38 billion. Dark Read.

Wang, P., Johnson, C., 2018. Cybersecurity incident handling: a case study of the Equifax data breach. Issues Inf. Syst. 19 (3).

Xin, Tong, He, Ying, Zamani, Efpraxia, Luo, C., 2024. Poster: cyber security economics model (CYSEM). In: ACM SIGSAC Conference on Computer and Communications Security (CCS '24).

Yaqoob, T., Arshad, A., Abbas, H., Amjad, M.F., Shafqat, N., 2019. Framework for calculating return on security investment (ROSI) for security-oriented organizations. Fut. Gener. Comput. Syst. 95, 754–763.