From Breach to Bias: Measuring Reputation Value and Trust Recovery After Cyber Incidents in Critical Infrastructure

Bonnie Rushing, Dr. Shouhuai Xu, and Ashley Fairman

University of Colorado Colorado Springs, brushing@uccs.edu, ashley@dicecyber.com

Abstract

Cybersecurity incidents increasingly affect not only operational integrity but also business reputation, especially for companies managing critical infrastructure. This study introduces the Reputation Impact Score (RIS), a novel, repeatable metric that quantifies reputational damage using a combination of financial volatility, investor trust, and sentiment analysis from employees and customers. The RIS model is applied to real-world case studies of high-profile cybersecurity incidents affecting operational technology (OT) companies, including Equifax, SolarWinds, and American Water Works. By integrating open-source financial data and public sentiment ratings, the RIS enables organizations to assess recovery progress and predict potential reputational harm. This work introduces a practical framework to quantify reputational resilience in critical infrastructure firms.

Keywords: Cybersecurity, Reputation Impact Score, Critical Infrastructure Protection, Operational Technology, Stakeholder Sentiment, Psychological Biases

1. Highlights

- Introduces RIS, a new metric for reputational damage after cyber incidents.
- RIS combines stock data and sentiment from employees and customers.
- Supports infrastructure security by analyzing tech and cognitive-based risks.
- Shows how OT firms vary in trust recovery despite similar stock drops.

"The views expressed in this article are those of the author and do not necessarily reflect the official policy or position of the Air Force, the Department of Defense or the U.S. Government."

2. Introduction

As technology becomes deeply embedded in global business operations, political systems, and international relations, safeguarding sensitive data and countering cyber threats has become a top-tier global priority [22]. Business leaders increasingly recognize that cybersecurity incidents extend beyond technical disruptions—they directly impact corporate reputation and, by extension, return on investment (ROI) [17]. Reputation is shaped by

multiple factors, including how stakeholders perceive a company's ability to defend itself against cyber threats and how they respond to them. As incidents grow in frequency and sophistication, reputational damage becomes a critical and compounding risk [23]. This risk is especially acute for companies in the operational technology (OT) sector, where successful cyberattacks may not only harm brand value but also jeopardize US critical infrastructure and national security. For these organizations, proactive cybersecurity strategies are no longer optional—they are essential to organizational survival and public trust [23, 19].

Definition 1 (Cyber attack incidents). *Any malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself [31].*

Definition 2 (Operational Technology (OT)). *OT encompasses a broad range of programmable systems and devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems detect or cause a direct change by monitoring and/or controlling devices, processes, and events. Examples include industrial control systems, building automation systems, transportation systems, physical access control systems, physical environment monitoring systems, and physical environment measurement systems. This technology is essential for critical infrastructure [31, 3, 20].*

For this paper, *OT businesses* refer to any company related to a critical infrastructure sector and relies on OT. These sectors include Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Services and Facilities, Healthcare and Public Health, Information Technology, Nuclear Reactors, Materials, and Waste, Transportation Systems, and Water and Wastewater [6].

OT is vital to operating US critical infrastructures, which are highly interconnected, mutually dependent systems. Most of the nation's critical infrastructure is owned and operated by private entities. Additionally, critical infrastructures are often referred to as a"system of systems" due to the interdependencies between various industrial sectors and the interconnections between business partners [31]. Cyber defense strategies are publicly available online, along with local support across the US; however, it appears that Americans do not prioritize cybersecurity [6, 4, 23, 31].

2.1. Motivation

This paper seeks to understand why Americans often deprioritize cybersecurity and to explore what is at stake for companies impacted by cyberattacks. Although OT security incidents can have wide-ranging consequences—including threats to national security, infrastructure degradation, and risks to human safety—the dominant lens through which these events are evaluated remains financial. In American corporate and public discourse, cybersecurity incidents are often framed in terms of shareholder value, ROI (return on investment), and market volatility. This cost-centric perspective shapes how cyber risks are perceived, managed, and communicated [25]. Prior research has shown that individuals are most influenced by the anticipated costs of cybersecurity measures, display optimism bias in assessing their own vulnerability, and tend to delay action until damage has already occurred [36]. Accordingly, this study emphasizes financial and sentiment-based indicators not to diminish the broader human or national implications, but to reflect the economic realities that drive decision-making and determine whether OT cybersecurity receives the attention it demands.

Harmful impacts of cybersecurity incidents to companies include (i) *business reputation and ROI*, (ii) *national security issues*, and (iii) *widespread consequences for affected OT companies*.

2.1.1. Business Reputation and ROI

Business owners must consider the negative consequences of cyber attacks to their company's reputation and ROI. Reputation is based on the long-term aggregate perception of all stakeholders, which can be positive or negative based on communications and the company's corporate social responsibility (CSR) [17], including ethical concerns and cybersecurity issues [23].

Definition 3 (Return on Investment (ROI)). *ROI represents more than direct financial gain and profitability; it includes intangible assets like business reputation, long-term investor trust, and positive stakeholder perceptions that drive future confidence and success [4, 9].*

2.1.2. National Security Issues

CISA describes 16 critical infrastructure sectors with physical or virtual assets, systems, and networks considered so vital to the US that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. *Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience* advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure [6].

2.1.3. Consequences for Affected OT Companies

OT companies are increasingly exposed to cyberattacks that present a growing national security risk. The consequences of such incidents can be far-reaching, impacting not only business continuity but also public safety and environmental stability. According to the National Institute of Standards and Technology (NIST) [31], compromised OT systems may experience blocked or delayed information flows, resulting in operational disruptions such as loss of visibility or control. Attackers may also execute unauthorized changes to commands, instructions, or alarm thresholds, potentially damaging or disabling critical equipment, creating environmental hazards, or endangering human life. In some cases, false information may be relayed to system operators to either conceal unauthorized actions or deliberately provoke inappropriate responses. Cyberattacks may also involve the modification or corruption of OT software, including the insertion of malware, which can degrade system integrity and safety. Furthermore, attackers could interfere with equipment protection systems—posing serious risks to expensive, mission-critical infrastructure—or compromise safety systems in ways that directly threaten human life. These risks underscore the urgency of strengthening both technical defenses and organizational awareness within the OT sector.

Adversaries are pre-positioned within US infrastructure networks. For example, the People's Republic of China (PRC) state-sponsored cyber actors have already compromised US OT companies, including water systems. The nefarious actors employ "Living-off-the-Land" techniques, maintaining anonymity and moving within IT environments [6]. This threat is far-reaching, especially for small businesses. Small and privately owned facilities make up

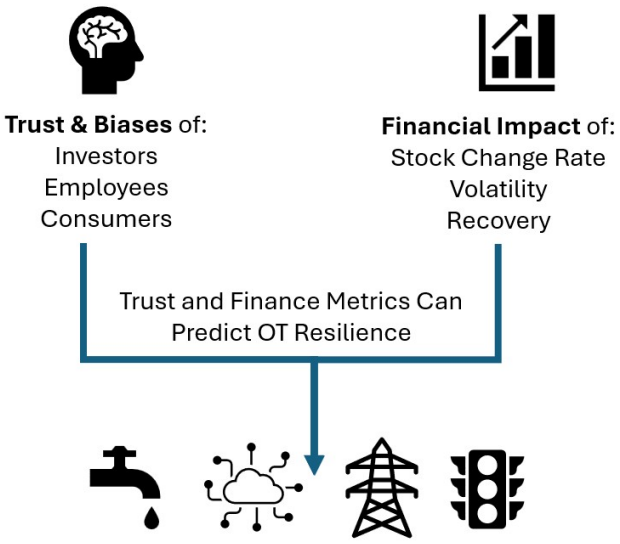

Figure 1: Graphical Abstract: Summarizes Interdisciplinary Approach to Operational Technology (OT) Resilience with Two Pillars, Trust and Biases and Financial Impact

most of the US critical infrastructure and are being specifically targeted by cyber attackers. For example, malicious actors may seek to disrupt, deny, degrade, or destroy critical operations by locking out authorized users, shutting down infrastructure without notification, and inserting malicious settings or code to corrupt operations [6].

2.2. Research Question

Based on the potential for infrastructure and security disasters posted by adversarial cyber actors, we aim to build upon growing literature in the fields of political science, cybersecurity, economics, business management, and psychology. This cross-disciplinary approach enables our team to approach this issue with a diverse perspective, poised to answer unique questions in a novel manner.

We consider the motivating issues of business reputation and ROI, national security issues, and consequences for affected OT companies. This combination of impacts leads to our research question (RQ), which follows.

- *RQ: How can reputational risk after cyberattacks be quantified in operational technology companies using open-source sentiment and financial data?*

2.3. Contributions

This paper makes a novel contribution by presenting a mathematical formula for measuring the reputational impacts on companies and analyzing their resilience following historical incidents. In the unique case study, we focus on companies related to OT. Our paper takes a multidisciplinary research approach, incorporating methods and concepts from business management, economics, cybersecurity, political science, and psychology. Figure 1 visualizes this interdisciplinary approach.

2.4. Related Studies

We organize related studies as follows: (i) approaches to measuring business reputation value, and (ii) studies on OT cybersecurity incidents.

2.4.1. Approaches to Measuring Business Reputation and ROI

The evaluation of business reputation has attracted significant attention across multiple disciplines, including economics, finance, network science, sociology, and risk management. Reputation is increasingly recognized as a form of intangible capital that affects firm value, investor confidence, and crisis resilience.

In economics and finance, reputation has been studied as a strategic asset that influences consumer choice, pricing power, and market valuation [18]. Feldman et al. describe reputation as a composite of stakeholder evaluations that reflect both cognitive and affective dimensions, shaped by interactions across internal and external actors such as employees, customers, investors, and communities [8]. Empirical studies have shown that data breaches can lead to quantifiable losses in firm value, reputational capital, and executive compensation [35, 25].

More broadly, network science approaches conceptualize reputation as a dynamic process influenced by information flow, social trust networks, and collective opinion formation. Recent studies have emphasized how online platforms, peer ratings, and public reviews serve as distributed reputation systems that can amplify or buffer reputational shocks [1, 2]. The EPL (Europhysics Letters) review (2023) highlights the mathematical modeling of reputation propagation in complex networks, where trust relationships and information diffusion mechanisms jointly shape public perception [2]. Similarly, the Physics of Life Review (2023) synthesizes interdisciplinary advances in reputation modeling, integrating cognitive science, opinion dynamics, and systemic risk frameworks [12]. These network-driven models provide a theoretical foundation for understanding how both financial data and sentiment signals co-evolve following crises.

From a risk management perspective, reputation has also been framed as a component of enterprise risk, where reputational loss can trigger secondary financial, legal, and regulatory consequences [27]. Studies in organizational behavior suggest that proactive reputation management, crisis communication, and transparent governance are essential to preserving stakeholder trust during and after cybersecurity incidents [5]. Coombs' Situational Crisis Communication Theory (SCCT) remains highly influential, emphasizing the role of crisis attribution, emotional framing, and strategic messaging in minimizing reputational damage [5].

Despite growing literature on reputation metrics, there remains no universally accepted formula that integrates both financial and sentiment factors into a unified measurement model. Existing tools often focus on either subjective surveys or isolated financial indicators, limiting their predictive and comparative power across organizations. This gap motivates the development of the Reputation Impact Score (RIS), which seeks to combine market response (stock change rate), investor confidence (volatility and recovery), and multi-stakeholder sentiment (employees and customers) into a repeatable and adaptable metric.

2.4.2. Studies on Cybersecurity Incidents Affecting Critical Infrastructure

The operational technology (OT) sector, which includes water systems, power grids, manufacturing facilities, and transportation networks, remains uniquely vulnerable to cyber threats due to the convergence of legacy systems, complex interdependencies, and growing digitalization. As Nkongolo explains, the protection of critical infrastructure has become a top-tier national security priority, with governments like Estonia implementing proactive cyber defense strategies following large-scale attacks such as the 2007 Estonian cyber campaign [22]. These early incidents highlighted how state-sponsored actors can leverage cyber tools to disrupt infrastructure and destabilize public trust.

International events, such as the 2017 *WannaCry* ransomware attack, further demonstrated the global reach of cyber incidents, as organizations across the healthcare, energy, transportation, and financial sectors were simultaneously compromised [22]. Such incidents underscore how OT-targeted attacks not only affect system functionality but also generate significant public concern, erode confidence in government institutions, and trigger cascading economic consequences.

In the United States, high-profile data breaches, such as the 2017 Equifax incident, offer insight into the cognitive and behavioral dimensions of public responses to cybersecurity events. Zou et al. found that individuals' protective behaviors after the breach were often shaped by psychological biases, such as optimism bias (underestimating personal risk), financial cost aversion, and delayed action until tangible harm occurred [36]. This highlights how public sentiment surrounding cyber incidents reflects not only technical damage but also risk perceptions, financial anxieties, and emotional reactions, factors central to the reputation dynamics captured by the RIS framework.

Scholars have increasingly emphasized that the reputational consequences of cyber incidents extend far beyond immediate technical remediation. As highlighted by Shedd and colleagues, trust restoration following cyber incidents involves a complex interplay between technical controls, executive leadership, public communication, and investor confidence [29]. Moreover, empirical analyses of data breaches suggest that firms experiencing repeated incidents suffer disproportionately higher valuation losses, reputational erosion, and market penalties compared to first-time breaches [35]. These cumulative reputational effects reflect both stakeholder sentiment and perceived organizational competence in managing crises.

Recent national security assessments have further documented how state actors employ cyber operations as components of broader political warfare strategies. For example, Chinese-sponsored campaigns, such as *Volt Typhoon*, deliberately target critical infrastructure not only to disrupt potential military operations but also to erode public trust in the resilience of essential services [33, 13]. These operations emphasize the reputational dimension of modern cyber conflicts, where the erosion of confidence can itself constitute a form of strategic advantage for adversaries.

Despite growing attention to OT vulnerabilities, few existing studies offer quantifiable frameworks for assessing how cyber incidents translate into reputational outcomes that combine financial, organizational, and psychological indicators. This gap highlights the need for integrative metrics, such as the RIS model, which explicitly considers investor trust, market volatility, employee sentiment, and customer confidence as key dimensions of post-incident reputation assessment.

2.4.3. Summary

The RIS model builds on an interdisciplinary foundation spanning cybersecurity, behavioral science, finance, and crisis communication. Prior studies on incident consequences have largely focused on technical or financial impacts, such as stock volatility or executive compensation following incidents [35]. However, recent research emphasizes the role of stakeholder sentiment and perception in shaping post-incident outcomes [25, 7]. Feldman's work on strategic reputation highlights trust as a long-term asset influenced by both internal and external stakeholder evaluations [8], while Zou et al. examine how psychological biases and perceived costs affect individuals' responses to cyber threats [36]. To interpret RIS score categories and reputational meaning, this study draws conceptually from Coombs' situational crisis communication theory (SCCT), which links organizational response strategies to stakeholder attribution and trust outcomes [5]. This interdisciplinary approach forms the foundation for our methodology.

3. Methodology

Our methodology includes secondary data analysis, which combines qualitative insights with quantitative analysis to provide a holistic understanding of reputation impact. This method utilizes multiple data sources, including financial data, social media, and other open-source intelligence, to enhance the validity and reliability of the findings. This study approach enables the identification of industry-specific trends and generalizable patterns.

Expected Outcomes:

1. Identification of key factors influencing business reputation and ROI following cyber attacks.

2. Development of a reputation impact score (RIS) model (tailored for OT businesses in the case study).

3. Strategic recommendations for crisis communication and reputation management (tailored for OT businesses in the case study).

3.1. Metrics

This paper's methodology uses the following concepts and metrics.

Definition 4 (Business Reputation). *Constituents' global perception or evaluation of a company's performance and attributes. It is a collective phenomenon comprising cognitive (thoughts) and affective (e.g., moods, feelings, attitudes) dimensions and develops over time [8].*

A positive business reputation is a strategic resource that enhances credibility and fosters trust among key stakeholders. As Feldman notes, a strong reputation yields a range of benefits that extend across operational, financial, and organizational dimensions [8]. It improves consumer perceptions of product and service quality, enabling companies to charge premium prices and generate positive word-of-mouth. Internally, it enhances a firm's ability to attract and retain qualified personnel while also boosting employee morale and productivity. A strong reputation can also serve as a buffer during crises, reducing the negative impact

of public scrutiny, competitive attacks, or operational disruptions. In the global market, a strong reputation facilitates international expansion by easing entry into new markets and forging strategic alliances. Financially, it attracts more investors, increases market value, reduces perceived organizational risk, and enables access to capital under more favorable terms. Altogether, a strong reputation differentiates a company from its competitors and strengthens its position in the marketplace.

These benefits underscore the significance of reputation and trust in achieving competitiveness. All stakeholders' needs must be met, including cybersecurity expectations; otherwise, the business reputation will decline [8]. In this paper, we introduce a metric to measure business Reputation Impact Scores.

Reputation Impact Score (RIS): Definitions and Interpretation

Definition 5 (Reputation Impact Score (RIS)). *A quantitative measure of a company's reputation health after an incident. It combines financial resilience (Investor Trust), market response (Stock Change Rate), and sentiment data (employee and customer confidence) to assess how well a company retains public trust.*

The RIS formula is our team's original synthesis, combining conceptual inspirations and empirical justifications drawn from prior work on investor trust, volatility factors [7], and sentiment-based modeling [8, 25]. It adapts established concepts from financial breach impact literature [35] and volatility-based trust decay modeling [7]. Our unique contribution lies in the integration of quantitative sentiment data from multiple stakeholders—specifically, employees and customers—making this methodology both repeatable and scalable for future investigators seeking to assess post-breach reputational impact.

It is essential to distinguish the temporal nature of the data sources used in the RIS framework. The financial indicators—such as stock change rate, volatility, and recovery magnitude—are time-bound metrics that reflect market behavior during the period immediately surrounding the breach event. In contrast, stakeholder sentiment data, drawn from employee reviews (e.g., Glassdoor) and customer reviews (e.g., Trustpilot), represent longer-term perceptions. These sentiment scores may reflect an organization's sustained reputation and culture and are not necessarily a direct result of a single incident. By combining these temporally distinct components, RIS captures both the immediate financial impact of a breach and the more enduring reputational landscape in which an organization operates.

RIS Formula

$$\text{RIS} = (S \times T) + E + C \tag{1}$$

Where:

- *S (Stock Change Rate)* – Percentage change in stock value post-incident. A negative value indicates a drop.
- *T (Investor Trust)* – Financial resilience score normalized between 0 and 1. Calculated as:

$$T = \max\left(0, 1 - \frac{\text{Stock Volatility}}{\text{Stock Volatility} + \text{Stock Recovery Magnitude}}\right) \tag{2}$$

- *E (Employee Sentiment)* – Workforce confidence, gathered from platforms like Glassdoor. Normalized to 0–1 (e.g., 3.5/5 stars = 0.70).
- *C (Customer Sentiment)* – Customer trust, measured from platforms like Trustpilot, Yelp, or Google Reviews. Normalized to 0–1 (e.g., 4.5/5 = 0.90).

Supporting Definitions:

- *Stock Volatility* – Standard deviation of stock price fluctuations within a defined post-breach period.
- *Stock Recovery Magnitude* – Amount by which stock price rebounds from its lowest point after the breach.

Worked Example Case:

$$\text{RIS} = (-0.12 \times 0.85) + 0.75 + 0.66 = -0.102 + 1.41 = \textit{1.308} \tag{3}$$

A RIS of *1.308* suggests that while the company has been impacted by the incident, it shows resilience—likely due to strong employee and customer sentiment.

Score Ranges Interpretation. RIS provides an intuitive score (positive score = recovery; negative score = severe damage). We developed Table 1 as a foundation for measuring RIS, inspired by methodologies from corporate reputation management, financial assessments, and crisis recovery models [5]. Higher scores show strong trust and recovery while lower scores indicate reputational risk.

Table 1: Reputation Impact Score (RIS) Interpretation Guidelines. The table defines RIS score ranges used to classify reputational resilience after a cyber incident. Higher scores reflect stronger stakeholder trust and recovery, while lower scores indicate increasing levels of reputational risk.

Reputation Impact Score (RIS)	**Meaning**
$\geq$ **1.5 (High)**	**Strong reputation resilience**, minimal long-term damage
$1.0 - 1.5$ **(Moderate)**	**Moderate recovery**, company is recovering from impact but concerns remain
$0.5 - 1.0$ **(Low)**	**Reputation risk**, requires strong recovery efforts
< 0.5 **(Very Low)**	**Severe reputation damage**, loss of stakeholder trust

3.2. Data Collection and Calculation Process

Our methodology employs Open Source Intelligence (OSINT) collection to gather real-world data on cybersecurity incidents, financial performance, and stakeholder sentiment. The integration of diverse OSINT sources allows us to quantify reputational impacts while ensuring the method remains transparent, repeatable, and adaptable across different sectors. This approach supports both research reproducibility and practical application by business leaders, risk managers, and cybersecurity policymakers.

Overview of Data Sources. We collect historical data from publicly accessible OSINT repositories, including:

- Financial markets and investor platforms (e.g., Google Finance, Yahoo Finance, Nasdaq historical data, company investor relations portals).
- Public cybersecurity incident databases (e.g., CISA advisories, MITRE ATT&CK, Have I Been Pwned, Shodan).
- Publicly available sentiment platforms (e.g., Glassdoor for employee sentiment; Trustpilot, Yelp, and Google Reviews for customer sentiment).
- News outlets, press releases, regulatory filings (e.g., SEC disclosures), and legal settlement reports.

A consolidated OSINT search framework is employed using online tools such as `https://osintframework.com/` to identify appropriate data sources for each company and incident.

Data Collection Steps.

1. *Cybersecurity Incident Identification:* Incidents are first identified using structured cybersecurity advisories (e.g., CISA alerts), publicly disclosed breach reports, and regulatory filings. For each company, we document incident dates, scope of compromise, attribution (if available), and response actions.
2. *Financial Market Data Collection:* Historical stock price data is gathered for each organization using sources such as Google Finance or the Python library *yfinance*, enabling daily resolution around the incident window. We collect stock prices covering at least 30 days before and after the incident to calculate stock change rate, volatility (standard deviation), and recovery magnitude.
3. *Employee Sentiment Collection:* Glassdoor reviews are aggregated to compute average star ratings for employee satisfaction. We document the total number of reviews available during the sampling period to assess confidence levels. Where possible, qualitative review content may be cross-validated for consistency.
4. *Customer Sentiment Collection:* Customer reviews are extracted from platforms such as Trustpilot, Yelp, and Google Reviews. For each platform, we record the average rating and review count to establish customer sentiment benchmarks. When multiple platforms are available, weighted averages may be applied, though equal weighting was used in this initial model for simplicity.

Sample Size and Review Volume Considerations. In each sentiment collection step, the sample size of available reviews is recorded to account for possible data sparsity. Smaller firms with limited online presence may exhibit higher volatility in sentiment scores due to smaller sample sizes. As part of model transparency, we acknowledge this limitation and propose that future research explore weighting sentiment scores based on sample volume, time window, and natural language processing (NLP) of review text for richer sentiment extraction [24].

Time-Series Alignment. To integrate financial and sentiment data, we establish a timeline surrounding each incident with aligned data points for stock price movements, volatility calculations, and public sentiment snapshots. While financial data is time-sensitive and reacts immediately to incident disclosures, sentiment data often reflects longer-term stakeholder perceptions that may lag or persist following the incident window.

Calculation and Visualization. The RIS model is then applied to compute reputation scores for each case study based on the collected OSINT data. Results are plotted into comparative tables and bar charts to visualize how different metrics interact across companies. These visualizations support both individual case assessment and cross-case pattern discovery.

Replicability and Future Extensions. This OSINT-based framework is intentionally designed to be scalable and extensible as additional case studies and sectors are analyzed. The reliance on publicly accessible sources makes the method replicable by both academic researchers and industry practitioners, while allowing for continuous improvement as sentiment analysis tools and public breach disclosures evolve.

3.2.1. Justification of RIS Variables and Equal Weighting

The Reputation Impact Score (RIS) model incorporates four primary variables: Stock Change Rate (S), Investor Trust (T), Employee Sentiment (E), and Customer Sentiment (C). These variables were selected to balance conceptual coverage, data accessibility, and cross-sector applicability in capturing the multidimensional effects of cyber incidents on organizational reputation.

Stock Change Rate (S). Financial markets often serve as the most immediate and visible external evaluation of a company following a cyber incident. Stock prices reflect real-time investor sentiment, market confidence, and perceived financial harm. As prior research shows, breaches frequently trigger stock price volatility and valuation declines as investors react to potential legal, operational, or reputational risks [35, 25]. This variable reflects how quickly and severely markets penalize organizations for security failures, capturing short-term external trust erosion.

Investor Trust (T). Investor Trust captures the resilience or stability of investor confidence following an incident, factoring in both stock volatility and recovery magnitude. As Dennis et al. suggest, volatility is a proxy for market uncertainty, while recovery dynamics reflect whether investors believe the organization can sustain long-term performance despite reputational shocks [7]. This component distinguishes temporary market panic from more persistent trust erosion. Trust modeling in risk management also supports using volatility-adjusted metrics as proxies for organizational resilience in uncertain environments [15].

Employee Sentiment (E) and Customer Sentiment (C). Both internal (employee) and external (customer) sentiment represent longer-term, relational aspects of organizational reputation. Feldman et al. emphasize that reputation is a collective judgment formed over time through stakeholder evaluations, encompassing product quality, leadership integrity, ethical behavior, and social responsibility [8]. Similarly, Coombs' Situational Crisis Communication Theory highlights the importance of emotional responses and perceived responsibility

in shaping reputational consequences after crises [5]. Rindova et al. further argue that employee confidence directly influences organizational culture, internal stability, and productivity, while customer trust has a measurable influence on consumer loyalty, sales, and public credibility [28]. Fombrun and Shanley identify these stakeholder evaluations as central to a firm's reputation capital, which shapes both valuation and resilience [10].

Why These Four Variables Were Prioritized. Alternative reputational indicators such as attack severity, executive turnover, regulatory penalties, or media coverage were considered but excluded from this initial model due to challenges in measurement consistency, limited cross-sector applicability, and the absence of standardized scoring systems that generalize across incident types. Technical scoring systems such as CVSS largely assess exploit complexity rather than stakeholder trust impacts [30, 11]. Furthermore, reputation is fundamentally a cognitive, trust-based phenomenon, and the chosen S, T, E, and C variables reflect that dual emphasis on financial exposure and human trust dynamics. The initial model prioritizes factors with broad applicability and public data accessibility, while remaining adaptable for future refinement [26].

Equal Weighting in the Initial Model. In this initial RIS model, each variable contributes equally to the composite score. This design reflects both simplicity and the current absence of empirically validated weighting schemes across diverse industries and incident types. The equal weighting serves as a transparent starting point, allowing the model to be broadly applied across sectors where the relative importance of financial and sentiment factors may vary. As larger datasets are collected in future work, statistical techniques such as regression modeling or expert elicitation may be used to develop calibrated weighting schemes that reflect sector-specific dynamics, organizational size, and stakeholder diversity.

Exclusion of Attack Severity and Application Criticality in this Version. While the severity of an attack and the criticality of the targeted application are undoubtedly important factors in real-world reputational outcomes, they were not included in this initial RIS formulation for several reasons. First, there is no universally standardized or consistently applied severity scoring system that could be generalized across the diverse types of cyber incidents examined in this study. Existing technical scoring frameworks, such as CVSS, primarily focus on technical exploitability rather than public or market-facing reputational effects [11]. Second, adding industry-specific criticality scores would limit cross-sector comparability and introduce sector bias at this exploratory stage. Finally, the present study's small sample size does not yet allow for sufficient statistical testing of how such modifiers would affect model sensitivity. Future research should explore the integration of severity, regulatory context, and sector criticality as supplemental weighting dimensions once larger and more diverse case datasets become available.

4. Comparative Case Studies: OT Businesses

For this comparative case study, we selected three publicly traded (with stock exchange symbol) US companies involved in OT that have experienced cybersecurity incidents. CISA advisories list incidents and vulnerabilities in OT sectors [6]. The three case studies include Equifax, SolarWinds, and American Water Works.

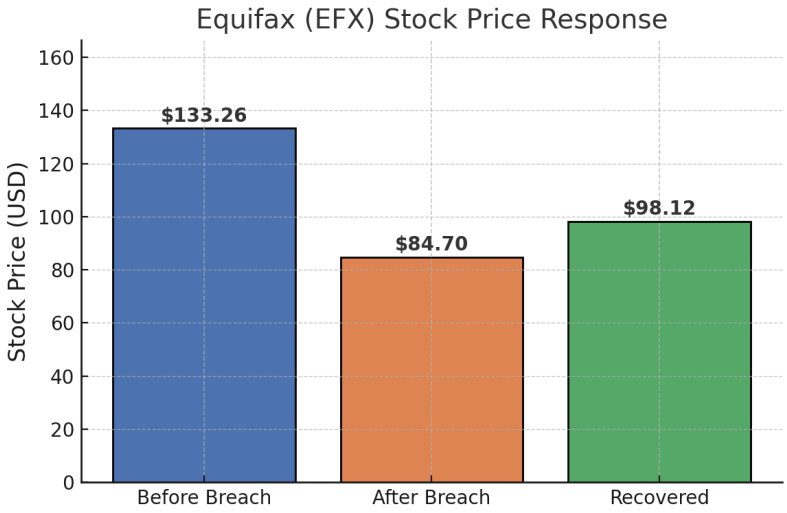

Figure 2: Equifax (EFX) Stock Price Response to 2017 Cybersecurity Breach. Stock price declined from $133.26 prior to breach disclosure to $84.70 immediately after, with partial recovery to $98.12 following initial market stabilization. `https://investor.equifax.com/stock-info/historical-data`

Company Size and Review Volume. For transparency, we record both the size of each company (in terms of employee headcount) and the number of sentiment reviews analyzed. In this case study:

Equifax: Approximately 11,000 employees; 3,200 Glassdoor reviews; 500 Yelp customer reviews.

SolarWinds: Approximately 2,200 employees; 570 Glassdoor reviews; 130 Gartner customer reviews.

American Water Works: Approximately 6,500 employees; 450 Glassdoor reviews; 90 Trustpilot customer reviews.

Sample Size Sensitivity. It is important to acknowledge that companies with smaller review volumes may exhibit higher variability in sentiment scores, especially for newer or smaller firms. Low sample sizes may lead to distorted or less stable sentiment estimates, particularly on public-facing review platforms. Future work may incorporate weighting adjustments to account for the number of reviews contributing to each sentiment score, or apply confidence intervals to assess score reliability.

4.0.1. Equifax Case Study - RIS Calculation (New York Stock Exchange (NYSE): EFX)

On September 7, 2017, Equifax publicly announced a major cybersecurity breach that exposed over 147 million consumer records due to vulnerability caused by a failure to patch Apache Struts [36]. This unprecedented *financial infrastructure* breach ended with a settlement of approximately $700 million. The stock dropped from $133.26 to a low of $84.70 (a 36.5% decline), before partially recovering to $98.12 by September 25. The stock prices are highlighted in Figure 2.

- Stock Change Rate:

$$\frac{84.70 - 133.26}{133.26} = -0.365 \tag{4}$$

- Stock Volatility (Standard Deviation): 20.47
- Recovery Magnitude:
$$98.12 - 84.70 = 13.42 \tag{5}$$
- Investor Trust:
$$1 - \frac{20.47}{20.47 + 13.42} = 0.396 \tag{6}$$
- Employee Sentiment: 3.5 stars (Glassdoor) = 0.70
- Customer Sentiment: 1.1 stars (Yelp) = 0.22

Reputation Impact Score (RIS):

$$RIS = (-0.365 \times 0.396) + 0.70 + 0.22 = -0.145 + 0.70 + 0.22 = 0.775 \tag{7}$$

RIS: 0.775
Equifax received a Reputation Impact Score (RIS) of 0.775, placing it within the *"reputational risk"* category. While the company experienced a financial recovery following its 2017 cybersecurity breach, the overall RIS reveals deeper long-term reputational damage that was perhaps unrelated to this incident. This lower score is primarily driven by long-standing negative customer sentiment, indicating a loss of public trust that has not been fully repaired by the stock rebound alone. The Equifax case illustrates how significant incidents, particularly those involving sensitive personal data, can cause long-term erosion of stakeholder confidence—ultimately impacting an organization's perceived resilience, even after operational stability is restored.

Recommendation: For Equifax, restoring customer trust remains critical. The company should prioritize transparent communication with consumers regarding data security improvements, implement regular third-party security audits, and proactively offer monitoring services or compensation for affected customers. Public demonstrations of strengthened data protection measures may help repair long-standing consumer skepticism reflected in sentiment scores.

4.0.2. Solarwinds Case Study - RIS Calculation (NYSE: SWI)

Sector: Information Technology (IT used by US gov agencies & OT companies) Breach: 2020 Russian Supply Chain Attack (SUNBURST malware). Status: Publicly traded on NYSE (SWI) Impact: Affected US infrastructure, including energy, transportation, and government.

The Solarwinds software hack was publicly announced on December 8, 2020, although hackers had accessed the system for several months [34]. The stock price started at $23.39, dropped to $14.94 after the announcement, and recovered to $16.82 by January 25, 2021, depicted in Figure 3.

Employee sentiment 3.1 stars (Glassdoor) = 66.2% = 0.662 Customer sentiment 4.5 stars (Gartner[1]) = 0.90

[1]https://www.gartner.com/reviews/market/observability-platforms/vendor/solarwinds

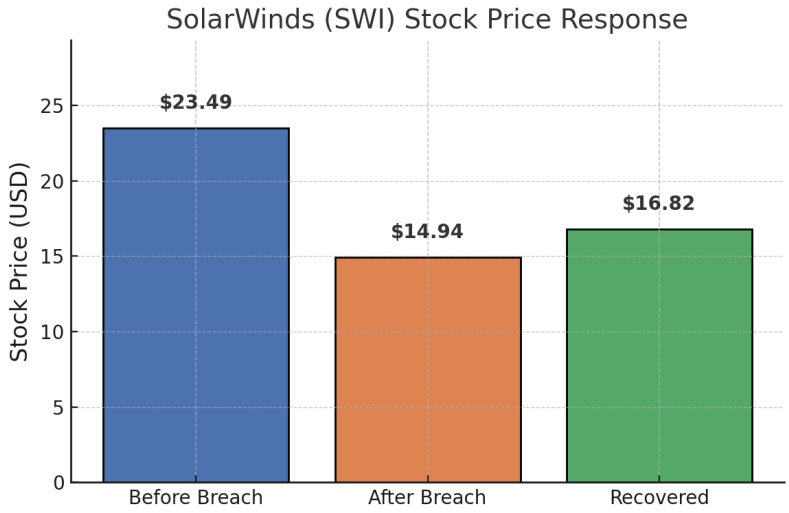

Figure 3: SolarWinds (SWI) Stock Price Response to 2020 Supply Chain Attack. Following breach disclosure, stock price fell from \$23.49 to \$14.94, later recovering to \$16.82 as public communication and customer sentiment stabilized. `https://investors.solarwinds.com/stock-info`

SolarWinds suffered a high-profile cybersecurity breach in December 2020. The stock price dropped significantly and began to recover by January 25, 2021.

- Stock Price Before Breach: \$23.39
- Stock Low After Breach: \$14.94
- Stock Price on Jan 25, 2021: \$16.82
- Stock Change Rate:
$$\frac{14.94 - 23.39}{23.39} = -0.361 \tag{8}$$
- Stock Recovery Magnitude:
$$16.82 - 14.94 = 1.88 \tag{9}$$
- Volatility (Standard Deviation):
$$\text{SD} = \sqrt{\frac{(23.39 - 18.38)^2 + (14.94 - 18.38)^2 + (16.82 - 18.38)^2}{3}} = 3.62 \tag{10}$$
- Investor Trust:
$$1 - \frac{3.62}{3.62 + 1.88} = 1 - \frac{3.62}{5.50} = 0.342 \tag{11}$$
- Employee Sentiment: 3.1 stars = 0.662
- Customer Sentiment: 4.5 stars = 0.90

Reputation Impact Score (RIS):

$$RIS = (-0.361 \times 0.342) + 0.662 + 0.90 = -0.123 + 0.662 + 0.90 = 1.439 \tag{12}$$

RIS: 1.439
SolarWinds received a Reputation Impact Score (RIS) of 1.439, placing it in the upper range of the *"moderate recovery"* category and approaching "strong resilience." Despite the high-profile nature of the 2020 breach and its connection to nation-state actors, the company demonstrated substantial reputational recovery. This outcome is largely attributed to strong customer sentiment, which suggests that end-users and clients retained trust in the brand's long-term reliability. While the incident caused a significant short-term decline in stock value, SolarWinds' ability to manage public perception and stabilize investor confidence played a key role in its subsequent rebound. The case highlights how proactive communication and positive stakeholder relationships can mitigate reputational harm even amid complex cybersecurity crises.

Recommendation: For SolarWinds, customer sentiment remains strong, but the company could further strengthen internal resilience by investing in employee engagement, cybersecurity training, and organizational culture improvements. Continued transparency in reporting software supply chain security practices will help maintain client confidence and reinforce long-term reputation stability.

4.0.3. American Water Works Case Study - RIS Calculation (NYSE: AWK)

On October 3, 2024, reports emerged that cyberattacks had targeted U.S. water infrastructure systems, including operations managed by American Water Works. The attacks, which exploited vulnerabilities in Supervisory Control and Data Acquisition (SCADA) systems, triggered concerns from both the EPA and CISA. No ransomware group claimed responsibility, but the breach raised national security alarms due to the company's service footprint across 14 states and at least 18 military installations. The incident occurred amid a broader surge in cyberattacks against water facilities, a sector widely regarded as vulnerable by experts. Since March 2024, White House officials have issued warnings to governors about the more than 170,000 U.S. water systems susceptible to cyber threats [33, 32].

Before the breach announcement, American Water Works stock traded at $146.10. Following the news, it dropped to $136.18 by October 9, before recovering to $142.58 by October 16. Employee sentiment averaged 3.4 stars on Glassdoor (68%), while customer sentiment on Trustpilot stood at 3.2 stars (64%).

- Stock Price Before Breach: $146.10
- Stock Low After Breach: $136.18 (Oct 9)
- Stock Price Post-Recovery: $142.58 (Oct 16)
- Stock Change Rate:

$$\frac{136.18 - 146.10}{146.10} = -0.068 \tag{13}$$

- Stock Recovery Magnitude:

$$142.58 - 136.18 = 6.40 \tag{14}$$

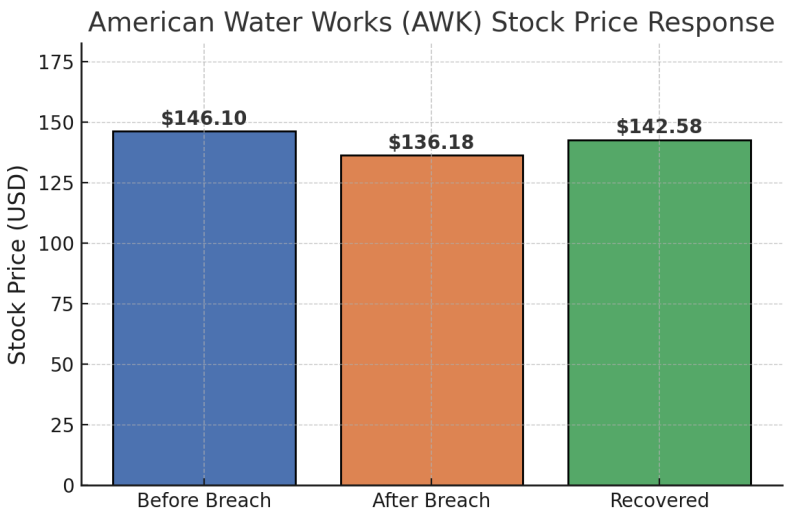

Figure 4: American Water Works (AWK) Stock Price Response to 2024 Water Infrastructure Breach. Stock price decreased from $146.10 to $136.18 after the incident, recovering to $142.58 in subsequent weeks as investor trust and public confidence remained stable. `https://ir.amwater.com/stock-information/`

- Volatility (Standard Deviation):
  Mean: $\mu =$
  $$\frac{146.10 + 136.18 + 142.58}{3} = 141.62 \tag{15}$$
  SD:
  $$\sqrt{\frac{(146.10 - 141.62)^2 + (136.18 - 141.62)^2 + (142.58 - 141.62)^2}{3}} = \tag{16}$$
  $$\sqrt{\frac{20.07 + 29.60 + 0.92}{3}} = \sqrt{16.86} \approx 4.10 \tag{17}$$
- Investor Trust:
  $$1 - \frac{4.10}{4.10 + 6.40} = 1 - \frac{4.10}{10.50} = 0.61 \tag{18}$$
- Employee Sentiment: 3.4 stars = 0.68
- Customer Sentiment: 3.2 stars = 0.64

Reputation Impact Score (RIS):

$$RIS = (-0.068 \times 0.61) + 0.68 + 0.64 = -0.0415 + 0.68 + 0.64 = 1.2785 \tag{19}$$

RIS: 1.279
American Water Works earned a Reputation Impact Score (RIS) of 1.279, which falls solidly within the *"moderate recovery"* range. Although the 2024 cyberattack targeted critical water infrastructure—a sector typically associated with heightened public concern—the company

maintained relatively strong stakeholder sentiment. Both employee and customer trust metrics contributed positively to the final RIS, helping to offset the reputational impact of the breach. Investor confidence and recovery magnitude also indicated resilience, though not at the level of stronger-performing peers like SolarWinds. This case highlights how companies providing essential services can maintain reputational stability by fostering a trusted internal culture and delivering consistent public service, even amid the scrutiny of national cybersecurity threats.

Recommendation: For American Water Works, maintaining public trust will require ongoing investment in both technical and communication capabilities. Strengthening OT cybersecurity defenses, expanding partnerships with government threat intelligence centers, and clearly communicating resilience measures to the public will help protect reputation as infrastructure threats evolve.

4.0.4. Case Study Summary

With all three RIS calculations complete, we now compare them side-by-side to evaluate differences in reputational resilience and stakeholder sentiment. These comparisons are summarized in Table 2 and visualized in Figures 5.

5. Analysis

In this section, we analyze the OT case studies to discover trends within the infrastructure industries.

OT Case Study Findings: RIS Comparison. Table 2 presents the Reputation Impact Score (RIS) results alongside key input metrics for the three OT company case studies. According to the findings, two of the three companies—SolarWinds and American Water—achieved RIS values that fall within the "moderate recovery" range. Equifax, however, received the lowest RIS, placing it in the "reputational risk" category. This lower score is primarily attributed to low consumer sentiment. A visual comparison of these results is shown in Figure 5.

Table 2: Reputation Impact Score (RIS) Components and Results for Equifax, SolarWinds, and American Water Case Studies. The table shows stock performance, sentiment scores, and resulting RIS values for each company following their cybersecurity incidents.

	Stock Change Rate	**Volatility**	**Recovery Magnitude**	**Investor Trust**	**Employee Sentiment**	**Customer Sentiment**	**Reputation Impact Score (RIS)**
Equifax	−0.365	20.47	13.42	0.396	0.70	0.22	0.775
SolarWinds	−0.361	3.62	1.88	0.342	0.662	0.90	1.439
American Water	−0.068	4.10	6.40	0.610	0.68	0.64	1.279

The RIS framework thus offers a multidimensional view of cyber incident impact, supporting more strategic decision-making in both private industry and national infrastructure planning.

The comparative bar depicted in Figure 5 highlights key differences in how each company responded to and recovered from cybersecurity incidents. SolarWinds achieved the highest

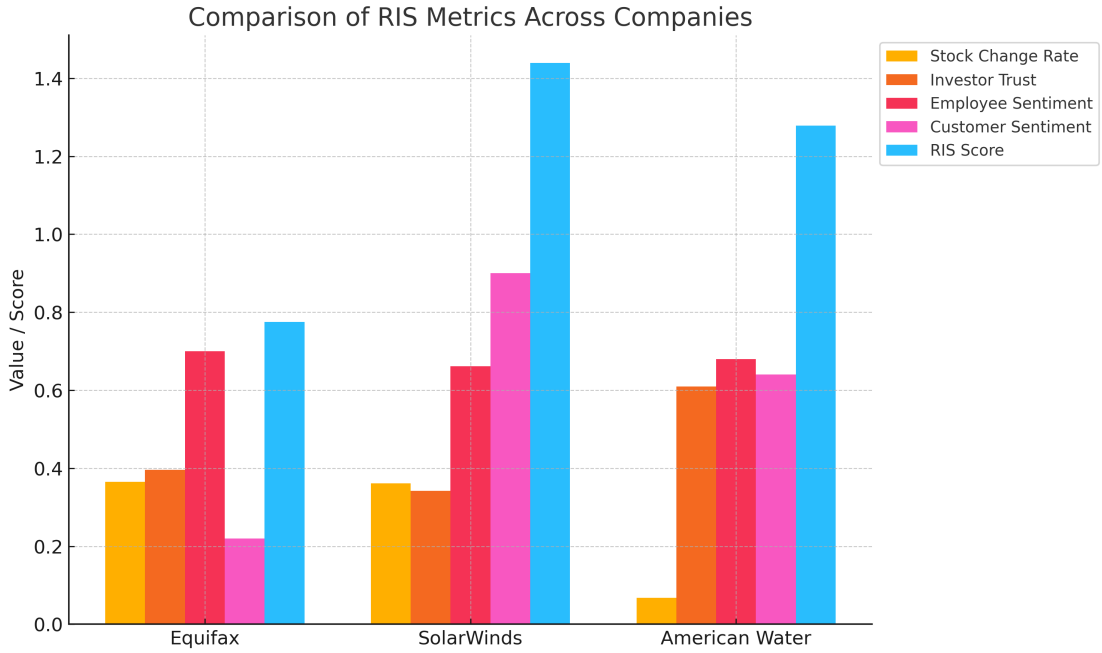

Figure 5: RIS Comparison Across Three OT Companies After Cyber Incidents. This bar chart displays the Reputation Impact Score (RIS) for Equifax (0.775), SolarWinds (1.439), and American Water Works (1.279). The scores reflect each company's reputational resilience based on financial recovery and stakeholder sentiment. While Equifax showed the lowest RIS due to weak customer trust, SolarWinds achieved the highest score, driven by strong external sentiment despite financial losses.

overall RIS score, largely due to exceptional customer sentiment (0.90) and balanced performance across other metrics. In contrast, Equifax exhibited strong internal sentiment but suffered from significantly low customer trust (0.22), resulting in the lowest RIS despite a similar financial recovery pattern to SolarWinds. American Water Works displayed moderate RIS performance, with the highest investor trust (0.61) and a relatively minor stock drop, reflecting its stability as a company. These findings emphasize that, in this case study, while financial indicators such as stock recovery are important, stakeholder sentiment—especially from customers—plays a crucial role in post-breach reputation resilience, leading to the following insight.

Insight 1. *Operational technology companies with high investor trust still experience reputational risk if public-facing sentiment is low.*

Post-Incident Rebound: Key Reputation Factors. Financial performance and stakeholder sentiment—spanning both internal employees and external consumers—play a critical long-term role in a company's resilience and return on investment (ROI) following cybersecurity incidents. Reputation, however, is not an asset that can be constructed overnight. It requires consistent trust-building, clear communication, and strong leadership over time. Business leaders must prioritize transparency and stakeholder engagement before, during, and after an incident to maintain reputational integrity. Research shows that trust recovery is significantly influenced by how organizations manage both emotional and perceptual responses

to crises [35, 8, 25]. Companies that proactively cultivate credibility through sentiment-aware communication strategies are more likely to rebound and retain investor and public confidence.

Insight 2. *Companies in regulated industries, like water infrastructure, may appear more stable due to investor trust—but remain vulnerable to cascading reputational effects.*

Insight 3. *RIS reveals that moderate financial impact can be offset by strong stakeholder sentiment—making communication strategy a vital layer of cyber defense.*

6. Discussion

OT cybersecurity does not appear to receive the attention it deserves. Despite the critical role that OT systems play in sustaining water, energy, transportation, and public safety infrastructure, these systems often remain under-prioritized in broader strategies. This neglect stems, in part, from a false sense of security, limited public awareness, and possibly the invisibility of OT systems in daily life. Moreover, without immediate financial consequences or public outcry, many organizations delay necessary investments in OT defenses. As a result, these vulnerabilities persist, leaving essential services vulnerable to both criminal and nation-state cyber threats that could lead to cascading failures across multiple sectors.

Given this landscape of underinvestment and persistent risk, there is a growing need for tools that help organizations understand and anticipate the broader consequences of cyber incidents—particularly their impact on public trust, stakeholder sentiment, and long-term stability. The RIS model introduced in this paper addresses this gap by providing a quantifiable method for assessing reputational damage and resilience. While developed in the context of OT cybersecurity, the model's flexibility enables its application to a broader range of reputational events and industries.

In addition to measuring reputational damage, the RIS model offers organizations a framework to guide recovery and risk management decisions based on their assessed score. Table 3 summarizes general recommendations that companies may consider depending on their RIS category. Higher RIS scores suggest that current resilience measures are effective, while lower scores indicate a need for more aggressive reputation repair, stakeholder outreach, and transparency efforts.

6.1. Application

Our formula analyzes cybersecurity incidents for the OT case study. Still, this metric can measure the reputation impacts of any company and any historical event, such as a change in leadership or negative publicity. Additionally, formula variables can be rearranged or isolated to predict outcomes, such as poor consumer ratings, stock changes, incident scenario modeling, or risk simulation.

6.1.1. Risk Simulation

The RIS formula can be rearranged once a company's RIS is calculated to predict other variables. For example, companies may include this calculation into risk simulation or scenario modeling to predict how much of the stock is expected to drop after an incident [14].

Adjusted Formula: To isolate and solve for Stock Change Rate (S):

Table 3: Reputation Impact Score (RIS), Ranges, and Recommended Actions: The RIS provides guidance on an organizational response after a cyber incident. Higher scores suggest strong resilience; lower scores indicate greater reputational risk requiring stronger corrective actions.

Reputation Impact Score (RIS)	**Recommended Actions**
High (1.5 or higher)	Maintain current practices and monitor emerging risks.
Moderate (between 1.0 & 1.5)	Strengthen communication, review defenses, and address trust concerns.
Low (below 1.0)	Increase transparency, engage stakeholders, and implement corrective measures.

- S = Stock Change Rate (what to solve for in this case)
- R = Expected RIS (e.g., 0.75 for moderate recovery)
- T = Investor Trust (between 0–1, based on historical data or simulated from volatility/recovery)

If the RIS, investor trust, employee sentiment, and customer sentiment are known, the formula can be rearranged to solve for the expected Stock Change Rate:

$$\text{Stock Change Rate} = \frac{\text{RIS} - \text{Employee Sentiment} - \text{Customer Sentiment}}{\text{Investor Trust}} \tag{20}$$

This inverse calculation allows analysts to estimate the percentage drop (or gain) in stock price associated with an incident based on the expected RIS and sentiment dynamics. For example, if:

- RIS = 0.75
- Employee Sentiment = 0.70
- Customer Sentiment = 0.20
- Investor Trust = 0.50

Then:

$$\text{Stock Change Rate} = \frac{0.75 - 0.70 - 0.20}{0.50} = \frac{-0.15}{0.50} = -0.30 \tag{21}$$

This suggests a predicted 30% drop in stock value following an incident.

Insight 4. *The RIS formula provides an early warning mechanism—companies can simulate outcomes and prepare risk communication plans before a breach occurs.*

This simulation capability allows organizations to proactively model reputational risk under different incident scenarios, stakeholder sentiment conditions, and market stability assumptions. By incorporating RIS into tabletop exercises or crisis planning, companies can better estimate potential financial exposure and develop pre-incident communication strategies to mitigate reputational harm.

6.2. Cognitive Warfare and Reputational Vulnerability

OT companies face not only technical threats but also psychological ones. A false sense of security—fueled by cognitive biases such as underestimation, denial, optimism, evasion, and simplification [16]—can delay critical cybersecurity investments and increase vulnerability. These mental traps, as highlighted by Cano and others, often lead OT leaders to underestimate adversaries or overestimate their own resilience [4]. Figure 6 presents a visual model of these cognitive pitfalls, adapted for this research.

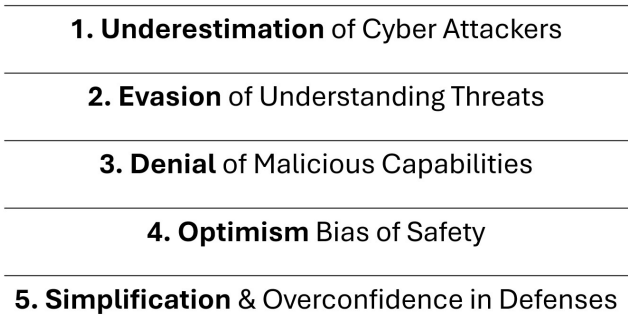

Figure 6: Cognitive Biases Contributing to a False Sense of Cybersecurity. The figure illustrates five common psychological biases that may delay investment in cybersecurity defenses.

This complacency is not accidental—it is often the objective of adversaries engaged in cognitive warfare. State actors such as the People's Republic of China (PRC) use cognitive warfare and influence campaigns to manipulate perception, degrade public trust, and reduce American preparedness. Gershaneck's work on political warfare details how these strategies target decision-makers' perceptions rather than relying on physical confrontation [13]. These operations aim to confuse and distract rather than persuade, weakening social cohesion and institutional credibility over time.

Recent examples, such as the Volt Typhoon hacking campaign, demonstrate the real-world implications of these tactics. According to federal investigators, the campaign aimed to disable critical infrastructure and interfere with US military deployment in East Asia [32, 33]. These goals align with the PRC's long-term political warfare strategy, where cyber incidents serve as instruments of distraction, sabotage, and psychological disruption [13].

The reputational consequences of such attacks can be severe. A breach in a water utility, for instance, risks not only service disruption but also cascading public health effects and the erosion of public trust [6]. The RIS model presented in this paper addresses this challenge by quantifying not only the technical impact but also stakeholder sentiment—a vital defense against perception manipulation. The true measure of such operations is the erosion of belief in truth, legitimacy, and stability [13]. By integrating sentiment metrics and trust modeling, RIS helps detect reputational degradation that may otherwise remain hidden beneath surface-level recovery metrics.

Insight 5. *A false sense of security, driven by cognitive biases such as denial or simplification, can delay critical action in OT cybersecurity defense.*

Insight 6. *Volt Typhoon's hacking campaign aligns with PRC political warfare strategies, where distraction and manipulation—not destruction—are the primary objectives.*

6.3. Limitations and Future Work

While the Reputation Impact Score (RIS) offers a novel, integrative approach to measuring reputational risk, several limitations warrant discussion, and multiple opportunities for future work exist to refine and extend the model.

First, this initial formulation assumes equal weighting across financial and sentiment metrics (Stock Change Rate, Investor Trust, Employee Sentiment, and Customer Sentiment). This equal weighting simplifies the model and allows for cross-sector comparability at small sample sizes, but it does not account for potential differences in how each factor contributes to reputation recovery. As additional case studies are collected, future research can apply advanced statistical methods, such as regression modeling, structural equation modeling, or machine learning optimization, to empirically derive appropriate weighting schemes that reflect sector-specific or incident-specific dynamics. Future modeling efforts may incorporate review volume weighting to reduce sensitivity to small sample sizes, particularly for organizations with limited public review footprints.

Second, the RIS model currently excludes explicit measures of attack severity or application criticality. Future work may explore the integration of standardized severity scoring frameworks, such as the Common Vulnerability Scoring System (CVSS) or MITRE ATT&CK impact categories, to capture the technical complexity and systemic risk associated with specific incidents. Similarly, sector criticality rankings, such as those published by CISA or the National Risk Management Center, may offer a way to differentiate reputational vulnerability across different critical infrastructure sectors.

Third, while the present study relies on publicly available sentiment platforms (e.g., Glassdoor, Trustpilot), these sources often reflect incomplete or biased samples, depending on the firm's size and online engagement levels. As natural language processing (NLP) techniques advance, future research may utilize text-based sentiment extraction from broader datasets such as social media, earnings calls, investor briefings, or legal proceedings to develop richer sentiment models that account for emotional tone, trust language, and stakeholder narratives over time.

Fourth, while this study aligns financial data to relatively short incident windows, longer longitudinal studies may capture delayed or extended reputation effects that are not immediately observable in the initial post-incident market response. Incorporating longer-term timelines, quarterly financial data, and cross-incident comparisons may help further distinguish transient market corrections from durable reputational shifts.

Finally, while this study focused on cybersecurity incidents, the RIS framework may be adapted to assess reputational impacts from other organizational crises, such as leadership scandals, product failures, regulatory violations, or geopolitical conflicts. Expanding the model's generalizability may enhance its utility for enterprise risk management across diverse organizational settings.

7. Conclusion

This paper introduces the RIS, a quantifiable framework for measuring reputational risk and organizational resilience in the aftermath of cybersecurity incidents. By integrating financial indicators with sentiment-based trust metrics, RIS captures how public perception,

stakeholder confidence, and cognitive bias influence post-breach outcomes. The model highlights that reputation is not only a consequence of security failures—it is shaped by how incidents are perceived, communicated, and remembered. Notably, the same psychological biases that weaken reputation, such as denial or optimism bias, are often responsible for delayed investments in cyber defense, increasing the likelihood of incidents in the first place. RIS provides a structured means of evaluating this full reputational lifecycle—from vulnerability to recovery.

Insight 7. *Reputation is no longer a passive asset—it must be actively defended like any other system of critical infrastructure.*

Insight 8. *ROI follows trust. Reputation is not a result- it is a driver.*

Insight 9. *Cognitive bias and public sentiment are not side effects—they drive financial and strategic outcomes.*

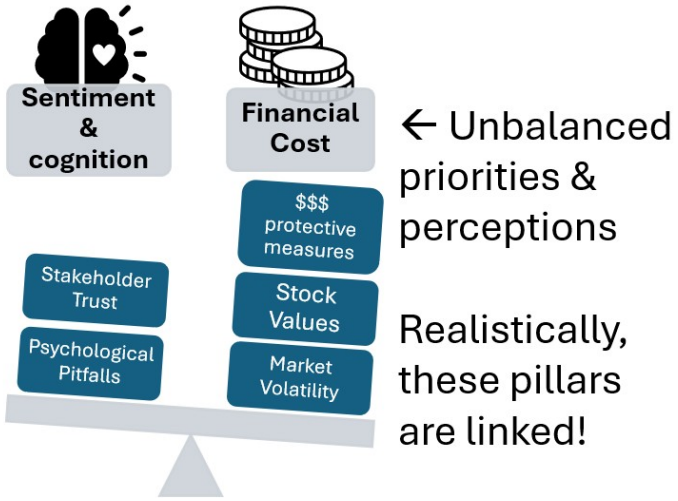

Figure 7: Unbalanced Business Priorities: How Cognitive Bias and Sentiment Shape Financial Outcomes. The figure illustrates how business leaders may overweight financial performance while underestimating the role of public sentiment and psychological biases. These cognitive factors directly influence investor confidence, customer trust, and post-incident recovery, making reputation management a primary driver of financial resilience after incidents.

Financial indicators and sentiment and cognitive biases are inextricably linked. While Americans and business leaders often prioritize the bottom-line ROI, the RIS reveals that public sentiment and cognitive biases are not secondary factors—they are primary drivers of stock performance, stakeholder trust, and organizational decision-making. This includes the false sense of security that leads to lacking cybersecurity prioritization. In reality, psychological perception significantly influences financial outcomes, including investor confidence, customer loyalty, and even internal policy changes. These unbalanced priorities and perceptions of business leaders are depicted in Figure 7. RIS exposes this dynamic by quantifying the intersection of perception and cost, demonstrating that sentiment ultimately helps shape the financial and strategic trajectory of post-breach recovery.

Through comparative case studies of Equifax, SolarWinds, and American Water Works, our findings show that while financial recovery plays a role, public-facing sentiment—especially customer trust—can be equally, if not more, influential in shaping post-breach outcomes. The RIS model not only provides organizations with a framework to assess their current standing but also enables risk simulation to anticipate potential fallout from future incidents.

This interdisciplinary approach underscores the increasing significance of psychological biases and cognitive warfare in shaping public perception and informed decision-making. By incorporating these soft-power threats into quantitative assessments, RIS serves as a strategic tool for business leaders, policymakers, and cybersecurity professionals working to protect both reputation and national resilience.

Insight 10. *By translating trust into a measurable outcome, RIS turns perception into a cybersecurity metric.*

Future work may refine this model by applying advanced sentiment analysis techniques and expanding to other sectors. As cyber threats evolve, so too must our methods for understanding their full impact—not just on systems, but on trust.

Data availability statement. The authors confirm that the data supporting the findings of this study are available within the article and/or its supplementary materials.

References

[1] Alain Barrat, Marc Barthélemy, and Alessandro Vespignani. *Dynamical processes on complex networks*. Cambridge University Press, 2008.

[2] Stefano Battiston, Guido Caldarelli, Diego Garlaschelli, and Roberta Sinatra. Network approaches to reputation dynamics. *Europhysics Letters*, 141(2):21001, 2023.

[3] Hugh Boyes. *Industrial Control Systems (ICS) Cyber Security: Defence in Depth Strategies*. Institution of Engineering and Technology, 2013.

[4] Jeimy J. Cano. Overcoming a false sense of security. *ISACA Journal, Volume 1*, 2022. Accessed: February 12, 2025.

[5] W. Timothy Coombs. *Protecting Organization Reputations During a Crisis: The Development and Application of Situational Crisis Communication Theory*, volume 10. 2007.

[6] Cybersecurity and Infrastructure Security Agency (CISA). China - nation-state cyber actors, 2025. Accessed: February 12, 2025.

[7] Patrick Dennis, Stewart Mayhew, and Chris Stivers. Stock returns, implied volatility innovations, and the asymmetric volatility phenomenon. *Journal of Financial and Quantitative Analysis*, 41(2):381–406, 2006.

[8] Percy Marquina Feldman, Rolando Arellano Bahamonde, and Isabelle Velasquez Bellido. A new approach for measuring corporate reputation. *RAE - Revista de Administração de Empresas*, 54(1):53–66, 2014. Accessed: February 12, 2025.

[9] Charles J. Fombrun. *Reputation: Realizing Value from the Corporate Image*. Harvard Business School Press, Boston, MA, 1996.

[10] Charles J. Fombrun and Mark Shanley. What's in a name? reputation building and corporate strategy. *Academy of Management Journal*, 33(2):233–258, 1990.

[11] Forum of Incident Response and Security Teams (FIRST). Common vulnerability scoring system (cvss) v3.1 specification document, 2019. Accessed: April 2025.

[12] David Garcia and Frank Schweitzer. Reputation and trust in complex systems: A review. *Physics of Life Reviews*, 46:8–45, 2023.

[13] Kerry K. Gershaneck. *Political Warfare: Strategies for Combating China's Plan to 'Win without Fighting'*. Marine Corps University Press, Quantico, Virginia, 2020.

[14] Yacov Y. Haimes. On the definition of vulnerabilities in measuring risks to infrastructures. *Risk Analysis*, 29(3):383–392, 2009.

[15] Yacov Y. Haimes. *Risk Modeling, Assessment, and Management*. John Wiley & Sons, 4th edition, 2015.

[16] Daniel Kahneman. *Thinking, Fast and Slow*. Farrar, Straus and Giroux, New York, 2011.

[17] Yungwook Kim and Jungeun Yang. *Corporate Reputation and Return on Investment (ROI): Measuring the Bottom-Line Impact of Reputation*, pages 574–589. 04 2013.

[18] Christos A Makridis. Do data breaches damage reputation? evidence from 45 companies between 2002 and 2018. *Journal of Cybersecurity*, 7(1):tyab021, 09 2021.

[19] Roger C. Mayer, James H. Davis, and F. David Schoorman. An integrative model of organizational trust. *Academy of Management Review*, 20(3):709–734, 1995.

[20] Billy R. Miller and D. J. Rowe. *Securing SCADA Systems*. McGraw-Hill, 2012.

[21] MITRE Corporation. Mitre att&ck framework, 2024. Accessed: 2024-12-21.

[22] Mike Nkongolo. Navigating the complex nexus: Cybersecurity in political landscapes. *arXiv preprint*, 2308.08005v1, 2023. Accessed on March 8, 2025.

[23] David W. Opderbeck. Cybersecurity, encryption, and corporate social responsibility. *Georgetown Journal of International Affairs*, 18(3):105–111, 2017. Accessed: February 22, 2025.

[24] Bo Pang and Lillian Lee. Opinion mining and sentiment analysis. *Foundations and Trends in Information Retrieval*, 2(1-2):1–135, 2008.

[25] Jin Peng, Haofei Zhang, Juan Mao, and Shouhuai Xu. Repeated data breaches and firm value. *Economics Letters*, 224:111001, 2023.

[26] Michael Pirson and Deepak Malhotra. Foundations of organizational trust: What matters to different stakeholders? *Organization Science*, 22(4):1087–1104, 2011.

[27] Michael Power. *Organized uncertainty: Designing a world of risk management*. Oxford University Press, 2007.

[28] Violina P. Rindova, I.O. Williamson, A.P. Petkova, and J.M. Sever. Being good or being known: An empirical examination of the dimensions, antecedents, and consequences of organizational reputation. *Academy of Management Journal*, 48(6):1033–1049, 2005.

[29] Matthew Shedd and Richard John. Measuring the impact of data breaches on organizational reputation: An experimental investigation. *Journal of Cybersecurity*, 6(1):tyaa017, 2020.

[30] Paul Slovic. The perception of risk. *Risk Analysis*, 20(1):1–11, 2000.

[31] Keith Stouffer, Michael Pease, CheeYee Tang, Timothy Zimmerman, Victoria Pillitteri, Suzanne Lightman, Adam Hahn, Stephanie Saravia, Aslam Sherule, and Michael Thompson. Guide to operational technology (ot) security. Special Publication NIST SP 800-82r3, National Institute of Standards and Technology (NIST), September 2023.

[32] U.S. Environmental Protection Agency. Epa warns of increasing water infrastructure cyber threats, 2024. Accessed: March 15, 2025.

[33] Christian Vasquez. American water says it was hit with cyberattack. *CyberScoop*, 2024. Accessed: March 15, 2025.

[34] Marcus Willett. Lessons of the solarwinds hack. *Survival*, 63(2):7–26, 2021.

[35] Shouhuai Xu and Jin Peng. Repeated data breaches and executive compensation. *Journal of Cybersecurity*, 7(1):tyab018, 2021.

[36] Yixin Zou, Abraham H Mhaidli, Austin McCall, and Florian Schaub. "i've got nothing to lose": Consumers' risk perceptions and protective actions after the equifax data breach. In *Fourteenth Symposium on Usable Privacy and security (soups 2018)*, pages 197–216, 2018.