KOVRR

Cyber Decisions. Financially Quantified.

FORTUNE 1000 CYBER RISK REPORT

Determining Materiality With Marketplace Benchmarks

OCTOBER 2023

www.kovrr.com

Executive Summary

The growing rate of global cyber events, throughout all industries, has elevated cybersecurity governance to the forefront of corporate concern. Indeed, this rising prevalence spurred the US Securities and Exchange Commission (SEC) in July 2023 to mandate the disclosure of "material" cyber threats and incidents, albeit within a framework of somewhat ambiguous materiality definitions.

This report leverages Kovrr's risk quantification models to highlight the likely occurrence and relative costs of "material" cyber incidents companies might experience in the coming year, potentially eliciting consequences significant enough for SEC disclosures. Ultimately, Kovrr aims to provide insights for those companies seeking a deeper understanding of the types of cyber events and their respective financial impacts that are most likely to be disclosed in the coming years.

Methodology

The results of this report were determined via a comprehensive benchmarking exercise, using the US Fortune 1000 companies as the sample set due to the companies' diverse range of industries. Kovrr's models capture a detailed representation of each company's technological profile and simulate yearly cyber event scenarios tailored to each company's exposure to risk.

The models reveal "material" incidents in the form of data breaches, extortions, interruptions, and service provider events[1]. This report defines materiality as an interruption incident lasting over one hour or an incident where confidential data is breached. Smaller, non-material incidents are grouped and modeled in aggregate.

Kovrr's models produce an assessment of the likely frequency and severity of cyber breaches experienced by Fortune 1000 companies, harnessing our industry insights from previously disclosed breaches, insurance claims data, and incidents that have not been publicly disclosed.

Key Findings

Cyber Risk Across All Industries

The Oil, Gas Extraction, and Mining sector exhibits the highest probability of experiencing a material cyber event, with a frequency of 0.82 events per year (or approximately one material event every 1.2 years). However, the anticipated financial impact remains relatively modest, with a median cost of $28m. In contrast, the Utilities and Infrastructure industry faces a cyber event frequency of 0.62 events per year and a substantial financial impact of $57.9m.

[1] Event incidents (data breaches, extortions, interruptions, and sevice provder events) are defined at the end of the report.

Annual Cost Scenarios

Average Annual Loss (AAL), which combines event frequency and cost across the full range of possibilities, allows us to compare the overall risk between industries. The Finance and Real Estate industry has the highest AAL at $34.3m, owing to the substantial financial ramifications of infrequent but high-impact events. Conversely, the Construction industry has the lowest AAL at $7.3m , indicative of its relatively lower exposure to cyber risk.

Event Drivers

The cyber event types reviewed in this report were interruptions, third-party service provider incidents, extortion events, and data breaches. The report reveals that interruption events are prevalent across industries. Also notably, the Retail Trade industry faces an annual frequency of 0.47 for data breaches (or approximately one material incident every 2 years), while the Finance and Real Estate sector follows closely with 0.42, underscoring their heightened exposure to data-centric cyber incidents.

Cost Drivers

Highly regulated industries, notably Finance and Retail Trade, record the highest median costs per cyber event, totaling $70.5m, due to their extensive accumulation of PII. Third-party liability, regulatory compliance, and productivity loss augment the financial impact. The report also breaks down these costs further according to event type.

Secondary Loss Considerations

While the primary financial impact is evident almost immediately, secondary losses often extend widely over time. The Colonial Pipeline Company ransomware attack in May 2021 is a poignant example, wherein the initial extortion demand of $4.4m indirectly led to nationwide fuel shortages.

Conclusion

The Fortune 1000 dataset is an invaluable benchmark for gauging relative cyber risk frequencies and severities. However, the report underscores the imperative of incorporating secondary losses into risk analyses, as these often augment the financial repercussions of cyber incidents. This holistic approach to quantifying cyber risk equips organizations with a more comprehensive understanding and better preparedness to address the evolving cybersecurity landscape, create cyber risk mitigation programs, and identify "material" threats and incidents.

Introduction

Cyber risk quantification has become a major topic for discussion amongst boards and senior management. Cybersecurity governance and implementation is one of the biggest business risks companies face today. In July 2023, recognizing the looming threat, the US Securities and Exchange Commission (SEC) passed a series of regulations stipulating organizations must disclose "material" cyber threats and incidents to promote greater transparency.

However, the SEC's definition of "materiality" is vague, claiming that a material incident is one that poses "a substantial likelihood that a reasonable investor…would consider [it] important in making an investment decision." The underlying ambiguity has catalyzed a significant amount of debate among industry experts on how to define the term for reporting purposes more sharply.

While awaiting more acute language from the governing body, cybersecurity leaders generally agree the optimal starting point for determining materiality is to quantify risk financially and benchmark results against industry peers. By quantifying risk in monetary terms, organizations can better understand what might constitute "material" events and subsequently prioritize risk mitigation and budget allocation.

In this report, Kovrr aims to present an understanding of what that threshold of cyber risk might be by conducting a high-level benchmarking exercise based on the US Fortune 1000 companies. The results also offer insights for organizations to forecast the likelihood of specific cyber events and develop material risk management strategies accordingly.

The Fortune 1000 list has been used in this exercise as it offers a comprehensive index of well-known public companies and private enterprises that make corporate and revenue information available to the general public. The organizations in this data set span a broad range of industries, providing a representative overview of the broader, global marketplace.

Kovrr performed a detailed analysis of the Fortune 1000 companies to assess and quantify the levels of cyber risk across industry sectors, offering organizations objective data to internally define materiality and create appropriate risk governance and mitigation programs.

Methodology and Modeling Summary

Kovrr's models allow for a complete internal modeling of a company's digital infrastructure and cyber control framework. For this exercise, we based the internal network and digital infrastructure on benchmarked information about each company and their tech profiles collected via an outside-in scan.

The profile of security controls applied at these companies is considered sensitive information, so we have made assumptions for the level of controls across industries and revenue bands, which are conservative.

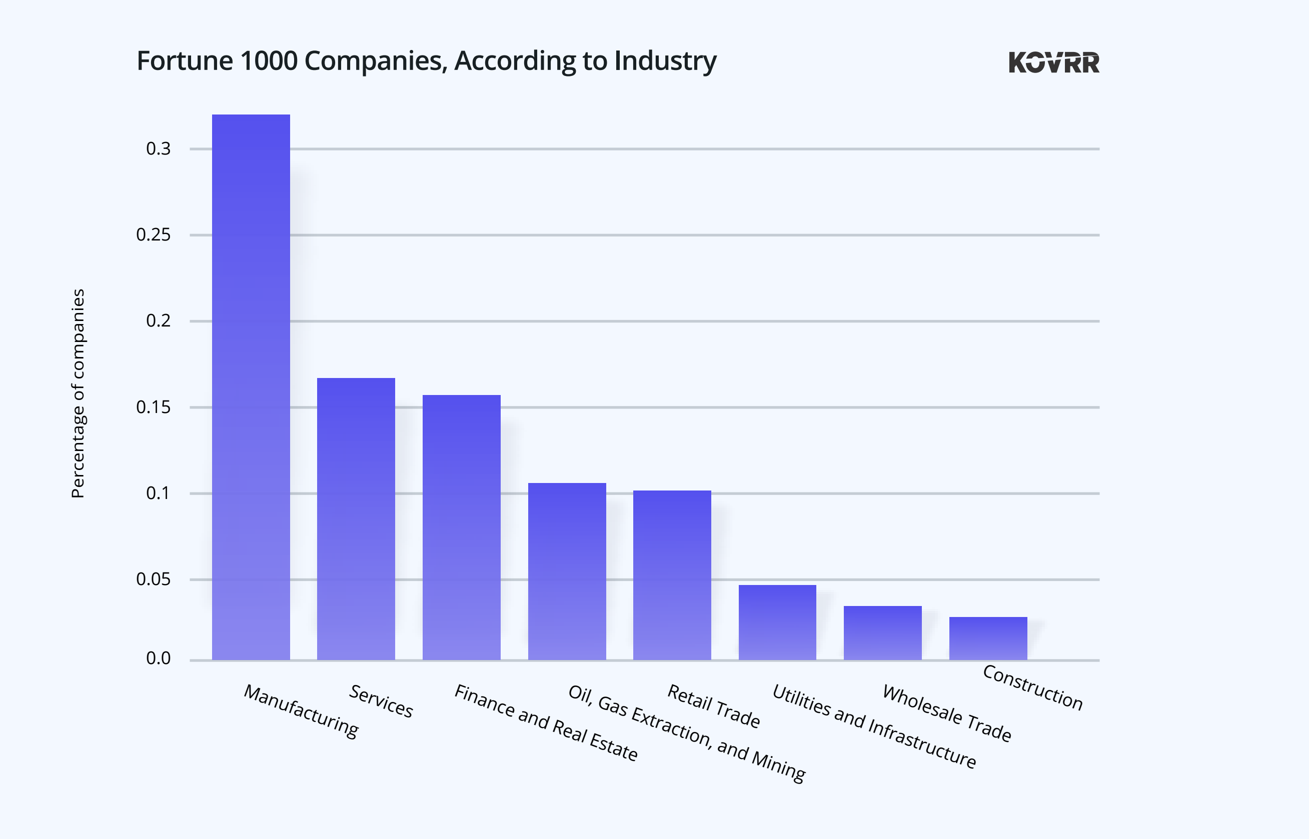
Each Fortune 1000 company's cyber posture and network architecture were integrated into Kovrr's cyber risk quantification models and assessed according to the full range of events and scenarios tailored to each company's exposure.

The models cover typical types of cyber events to which a company may be exposed, not just those reported publicly. Included are data breaches, extortions, interruptions, and service provider outages. Excluded events include operational technology and physical damages, which can be modeled but require additional company exposure details.

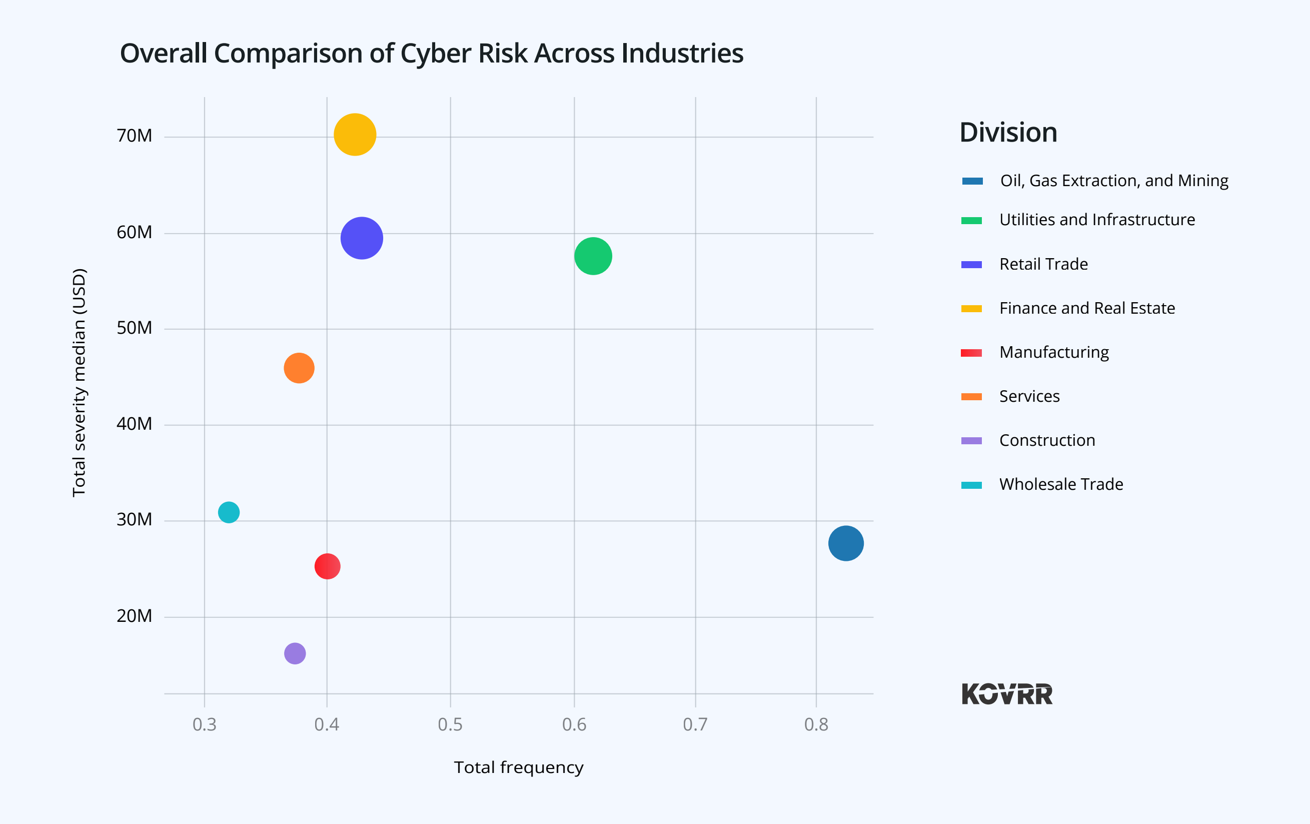
Overall Comparison of Cyber Risk Across Industries

The Fortune 1000 companies have been sorted according to the US Standard Industry Classification (SIC), which provides the structure for the primary industry groupings. Where a company operates across multiple sectors, we have used the primary operation of the company as the classifier.

The bulk of the companies in this study service the Manufacturing industry, covering over 30% of the total sample population. Because specific industry sectors (like Manufacturing) have a higher representation while others have lower representations, there can be a respectively increased volatility in the results.



The following charts in this report segment the results by frequency (the average number of events expected to occur in a given year) and severity (the median cost of an event once it occurs).



The data reveals that the Oil, Gas Extraction, and Mining industry has by far the largest expectation of frequency. These companies have a high probability of a cyber incident occurring within a year, with an event frequency of 0.82 events per year. Still, the predicted cost of events is expected to be relatively low, with a median of $28m.

The Utilities and Infrastructure industry draws more attention, as it experiences a relatively high annual frequency of cyber events at 0.62 and is combined with a high financial impact of $57.9m, suggesting this to be one of the most vulnerable industries to risk.

At this point, it is worth noting that the costs are the costs to the company being considered and not any secondary impacts to businesses that may rely on them (unless there is direct liability through data record exposure). Disruption to the 2021 Colonial Pipeline attack, for example, caused a temporary but significant impact on energy supplies across the US, which will be discussed in detail below.

Annual Cost Scenarios

Each of the bubbles' sizes, according to industry, illustrates the respective Average Annual Loss (AAL), a combination of annual event frequency and their given cost. The AAL allows us to compare the overall statistical distribution between industries of how frequency and severity combine, including the effect of tail risk (or extreme scenarios).

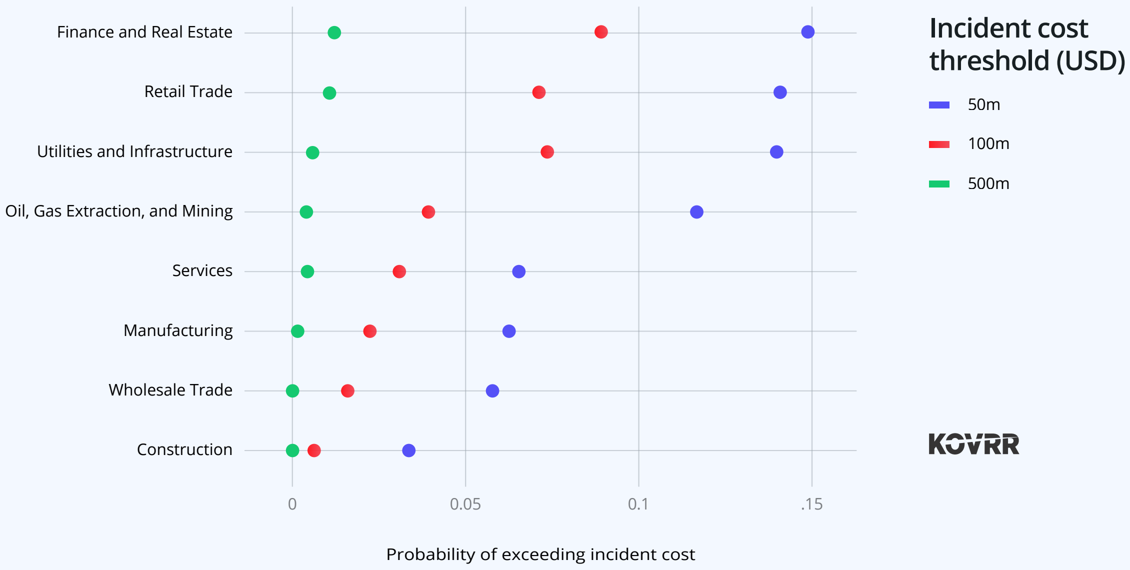
The Finance and Real Estate industry has the highest AAL, at $34.3m, while the Construction industry faces the lowest at $7.3m. The AAL highlights that although the Finance and Real Estate and Retail Trade industries have a relatively low event frequency, this is offset by the overall cost of events, with these businesses facing significant financial ramifications and risk.

The Construction, Wholesale Trade, and Manufacturing industries experience the lowest risk regarding frequency, impact, and Average Annual Loss.

Although the AAL summarizes the overall comparable loss, it does not inherently provide a clear framework for a business's cybersecurity decision-making. A more interesting perspective is to present these distributions in terms of probabilities. The chart below shows the probability of a company experiencing an adverse year of cyber events (one or more), which will have implications for business and capital.

(Note: This is an average probability across each cohort of companies.)

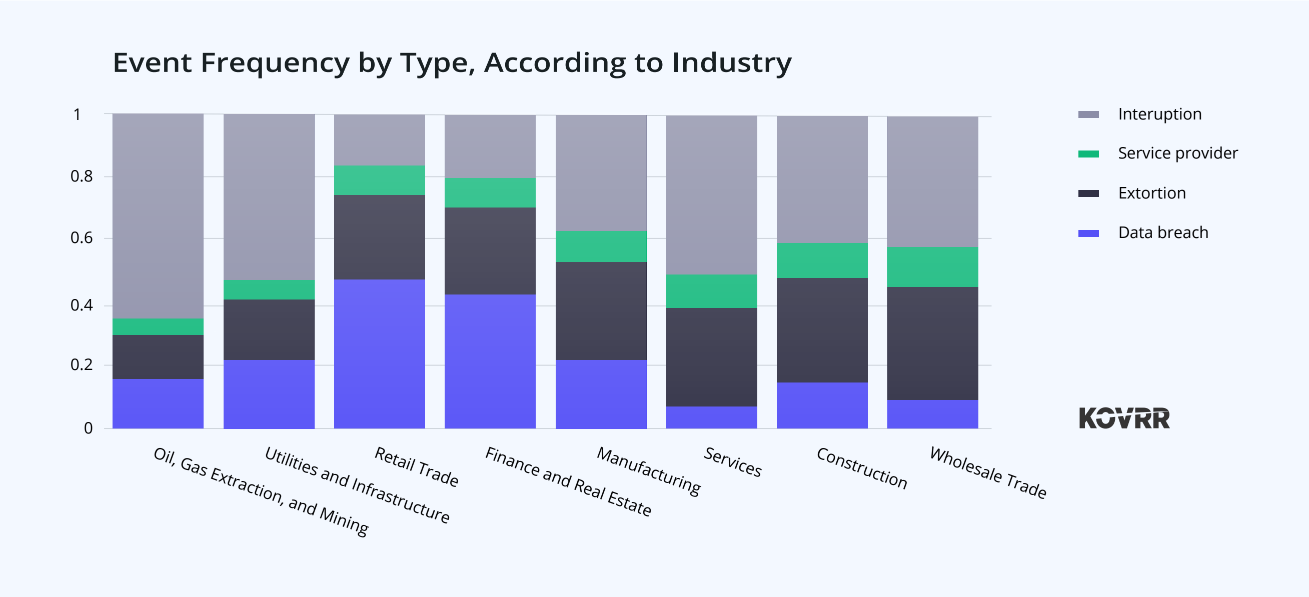
Average Expected Probability of Event Severity, According to Industry



The Finance and Real Estate, Retail Trade, Utilities, and Oil, Gas Extraction, and Mining industries all have a higher than 10% chance of a cyber event or events costing the included businesses more than $50m in a single year and a more than 5% chance of them costing more than $100m. To put these figures into context, the average annual revenue of a company in the Fortune 1000 is approximately $15bn, and the daily revenue is approximately $41m. This is a more practical interpretation of the model results, which can support financial planning.

Event Drivers

Part of a robust cyber defense management program is planning for the type of incident likely to occur. The chart below breaks down the types of events by how likely they are to occur in each industry sector. Overall, interruption events are common across many industries, including DDoS and internal disruptions to access to data and internal services such as email, Slack, and other internal communication tools.



The data shows that the most significant threat within the Retail Trade industry is a data breach, which comprises 47% of all cyber events occurring within the industry. The only other industry that comes close to the data breach risk frequency is Finance and Real Estate, with 42% of the total. Both these industries have large exposures to data records, which are likely to be targeted as part of a cyber incident.

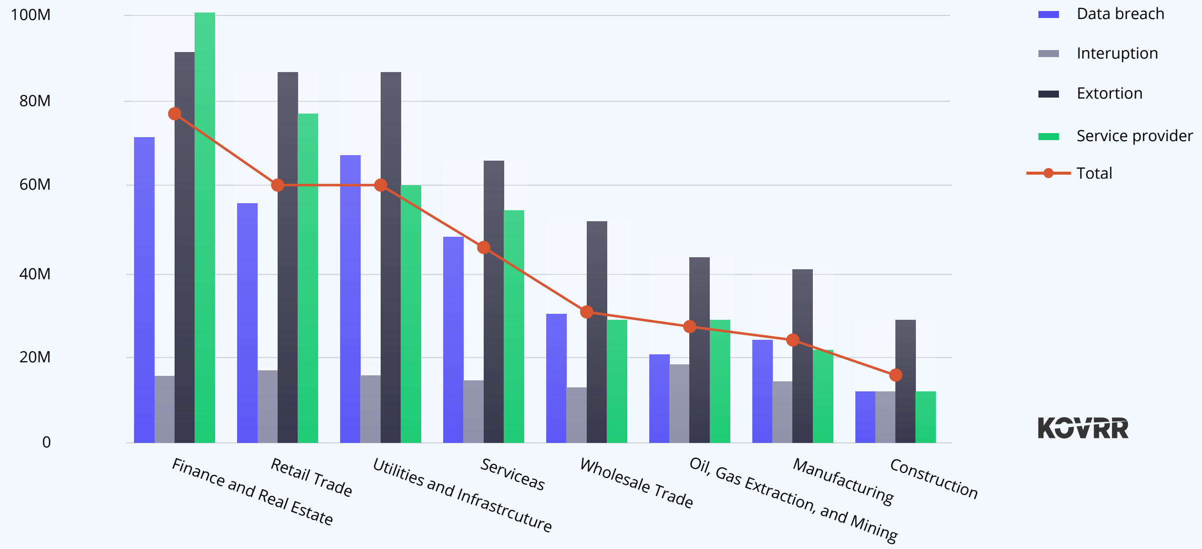
Conversely, these two industries are the least likely to experience an interruption event, an attack type that the other industries confront more frequently. There is a 17% chance of interruption in Retail and Trade and 21% in Finance and Real Estate.

Throughout all industries, there is relatively the same probability of experiencing an extortion event. However, Oil, Gas Extraction, and Mining and Utilities and Infrastructure companies experience slightly less than the others, at 14% and 19%, respectively. The rest of the industries suffer from extortion events between 27% to 36% of the time.

Drivers of Cost

The most frequent events are not always the most costly. For example, although interruption events are the most common across many industries, their cost is relatively low compared to other incidents, such as data breaches and extortion events.

Event Severity by Type, According to Industry



The industries that experience the highest average median cost of events are those highly regulated, such as Finance and Retail Trade, with a total loss of $70.5m per event. Similarly, industries that gather large quantities of Personal Identifiable Information (PII), such as Retail Trade ($59.8m), also have a relatively high financial impact from a cyber incident.

Additional factors augmenting a cyber event's financial consequences include third-party liability, regulation and compliance, and productivity loss.

The other average media costs of a cyber incident, according to industry, are:

Utilities and Infrastructure	**$57.9m**
Services	**$46.2m**
Wholesale Trade	**$31.2m**
Oil, Gas Extraction, and Mining	**$28.0m**
Manufacturing	**$25.6m**
Construction	**$16.5m**

The data again shows that companies that operate within highly regulated industries with high-volume transactions experience the most significant financial consequences. The Finance and Real Estate industry bears the brunt of their monetary losses from third-party service provider events, with an impact of $101.7m, followed closely by extortion incidents, amounting to $91.8m.

The rest of the industries experience their largest financial impact from extortion events.

Across all industries, the monetary loss from interruption events remains relatively low compared to other cyber events, ranging from $12.5m in the Construction industry to $18.23m in the Oil, Gas Extraction, and Mining industry.

Discussion: Secondary Losses

The US Fortune 1000 companies provide solid benchmarks to compare relative frequencies and severities of cyber events and offer crucial information for companies to leverage when determining material risks. However, it's critical to consider the secondary losses that might have occurred within these industries.

Such losses may not be immediately apparent or even directly caused by the initial cyber incident. Instead, they emerge over time as a chain reaction from the primary impact and often are more widespread and damaging.

Secondary losses are especially worth evaluating within the context of the Oil, Gas Extraction, and Mining industry. Although the Fortune 1000 data indicates a relatively low financial severity compared to other industries, there is a high potential for secondary losses, as evidenced in the Colonial Pipeline Company ransomware attack in May 2021.

Although the primary impact of the extortion only required the company to shut down for five days and pay $4.4m to the hackers, it catalyzed a myriad of secondary events, such as fuel shortages across the country affecting individual drivers and airlines.

Similarly, the cyber events within the Utilities and Infrastructure industry, which include public electric and water companies, have a high probability of causing mass disruption and, subsequently, significant secondary financial losses and consequences.

Overall, the Fortune 1000 is a highly representative dataset for benchmarking and determining what constitutes a material cyber risk. Nevertheless, organizations should not discount the potential for secondary losses, which augments financial impact. When conducting risk analyses, organizations should include these consequences in their parameters when calculating final loss estimates.

Event Definitions

The event definitions catalog includes:

Data Breaches

These are incidents in which company data is exfiltrated and confidentiality is breached for the company and potentially associated third parties.

Extortion Events

These include all incidents in which an extortion demand is made. This extortion could ensue following a data breach, interruption of service, or both.

Interruptions

These incidents are defined as any disruption to business-critical systems and data, such as DDoS or data wiping. Interruption incidents do not include extortion events.

Third-Party Service Provider Events

These incidents include a data breach or interruption within an organization's third-party service. They might include the breach of S3 buckets or a third-party outage.

PETER DYSON has worked in risk and capital modeling for over 15 years and joined Kovrr in July 2021 to lead the analytics team. He has gained a wealth of experience through senior modeling roles in the insurance industry, including cyber risk analytics, actuarial consulting, catastrophe modeling, and capital modeling. His qualifications include a Ph.D. in thermofluid modeling and a passion for technology and analytics.

KOVRR's cyber risk quantification platform empowers enterprise decision-makers to manage cyber exposure more effectively by providing an in-depth risk analysis that drives actionable, financially justified decisions.

Regardless of an organization's current framework, model, or risk register, Kovrr leverages the data and elevates the relative level of insight. Our enterprise-ready solution offers security teams a sharper, more granular risk assessment that's scalable on demand.

Learn more about how Kovrr can help your enterprise revamp its cyber risk management program today with CRQ by reaching out to contact@kovrr.com.

KOVRR
Cyber Decisions. Financially Quantified.

www.kovrr.com