

# Cybersecurity Risk Report

## 2024

Sponsored by



# Table of Contents

<b>01</b>	Key Insights	1
<b>02</b>	Executive Summary	2
<b>03</b>	Top Risk Scenarios by Industry	5
	Banking	5
	Healthcare Providers	5
	Retail	6
	Accommodation	6
	Manufacturing	6
<b>04</b>	Introduction	7
	Methodology	7
	Data Sources	8
	Reference Organization Characteristics	8
	The Price of Bigness	9
<b>05</b>	Top Industries by Total Loss Exposure	12
<b>06</b>	Top Risk Themes by Total Loss Exposure	13
<b>07</b>	The Implementation Challenge	15
<b>08</b>	Top Risk Themes by Industry	17
	Public Administration	18
	Healthcare	19
	Educational Services	20
	Finance and Insurance	21
	Retail	22
	Accommodation and Food Services	23
	Professional Services	24
	Information	25
	Manufacturing	26
<b>09</b>	Defining the Materiality of Cyber Incidents	27



## Key Insights

The two top industries by average loss exposure are Public Administration and Healthcare, driven by a relatively high probability of loss event.

Systems Intrusion and Insider Error are the top 2 risk themes for small businesses, while Basic Web Application Attacks and Social Engineering top the list for large enterprises.

Bigness raises risk. A large organization – measured in revenue and employee count – has a higher likelihood and severity of cyber loss events compared to a mid-market firm. For example, a large healthcare company has a better than 50% chance of a serious Insider Error event in a year versus 26% for a mid-size company.

We saw broad reductions in loss exposure compared to last year. The top four industries for average loss exposure are all down by one-third to one-half year-over-year.



## Executive Summary

- ▄ General improvements in loss exposure
- ▄ New cyber risk reporting rule by the SEC
- ▄ New materiality assessment standard

The 2024 Cybersecurity Risk Report from the FAIR Institute shows broadly positive trends compared to last year's survey.


Take our top four industries for Average Loss Exposure – our basic metric that combines probability and impact for cyber loss events (we explain our methodology below) – expressed in financial terms. Educational Services, Finance, and Public Administration, are all down by about one-third from the 2023 Report on improvements in frequency of incidents or cost. In Healthcare, the numbers are down by about half.

Now, we're talking about relative improvements, here. No one should be celebrating that Healthcare still runs a 26% probability of a serious Insider Error (including misconfigurations), but our findings are undeniably rosier this year compared to last.

There are a few reasons for our lower 2023 estimates:

- ▄ Trends in the risk landscape
- ▄ Inflation adjusted costs cooling off
- ▄ Event probabilities coming down
- ▄ Model improvements producing more accurate and narrower distributions
- ▄ Better data, with thousands more real event losses included in our report this year

Yes, we know the headlines have been awful. The exploitation of the MOVEit file transfer software by the notorious ransomware and extortion gang, Clop, affected the personal data of millions and will surely go down as the attack of the year.



Beneath the headlines about sophisticated external threat actors, the numbers we've analyzed flash a different warning:

Watch out for those simple, old-school threats.

**Of the seven top risk themes among the nine industries we studied, Basic Web Application Attack, typically password theft and stuffing, led for three industries, Insider Misuse (in other words malicious insiders) led for four industries, Insider Error led for one, and the more high-skilled System Intrusion for just one.**

In other words, while the frequency of sophisticated cyber-attacks have dropped, old-school password intrusions still pose a major threat. Revisiting your password protection and data loss prevention controls might be in order.

Also topping the news in 2023, the Securities and Exchange Commission (SEC) issued new rules, effective in December, mandating disclosure of material cyber Incidents (we call them events in this study) within four days from the moment that materiality was determined and disclosure of ongoing processes to manage cybersecurity risk. It was a powerful signal to public companies to improve their cyber risk reporting practices.

The FAIR Institute stepped up to help public companies define event materiality with the release of the FAIR Materiality Assessment Model (FAIR-MAM™), that comprehensively defines what forms of losses contribute to the measure of materiality in financial terms, so CISOs or risk managers can confidently determine when a cyber event cross the line of material impact (more details on this at the end of this report).

- ▄ When used with cyber risk quantification tools, FAIR-MAM can help public companies assess the materiality of cyber events and stay compliant with the requirement of the SEC rule



with a defensible, repeatable, and data-driven approach.

- ▮ To demonstrate FAIR-MAM's concrete applicability to quickly and efficiently determine and measure cyber loss materiality, the FAIR Institute launched an informational web resource called *How Material Is that Hack?*<sup>1</sup> that provides estimated materiality assessments of recent breaches in the news.
- ▮ This year, we are pleased to include original research from EY on the challenges of implementing a cybersecurity program, results from a survey that revealed the structural problems that hold back many programs, and the attributes of the most effective CISOs – as EY calls them, “Secure Creators.”

At the FAIR Institute, we believe that effective cyber risk management can only be achieved through transparent and defensible risk analysis using a standard such as FAIR™ and quality cyber risk data. We based our 2024 Cybersecurity Risk Report on FAIR analyses and extensive research by our data scientists advisors at Safe Security, the Institute's Technical Advisor.

We invite you to discover the most relevant cyber risk data for your industry and benchmark your performance against peers in your industry and others.

Please contact us at [info@fairinstitute.org](mailto:info@fairinstitute.org) if you are interested in learning how you can leverage these data and standard risk modeling resources for your organization.

*“Sometimes it takes the forcing function of a regulation to help mature key business practices and help turn what was an ‘art’ into a ‘business science.’ This feels like one of those moments for cyber risk management. And one when the greater transparency and accountability will greatly help improve our cybersecurity posture as a nation.”*

Nicola (Nick) Sanna  
FAIR Institute Founder  
on the effects if the new SEC rule<sup>2</sup>

---

1 <http://howmaterialisthathack.org/>

2 <https://www.fairinstitute.org/blog/what-the-new-sec-regulation-on-cyber-reporting-means-for-the-risk-management-profession>

# Top Risk Scenarios by Industry

The simulations in the other sections of this report have been conducted according to risk themes per the Verizon DBIR classification based on empirical data, to enable benchmarking. Each theme incorporated a multitude of risk scenarios that match one of those themes.

However, when conducting actual cyber risk assessments for a specific organization, the approach is typically a bottom-up one, where discrete risk scenarios are identified, measured, and prioritized to come up with a ranking of top risks. Those scenarios can then be aggregated in various ways (by threat, by asset, by form of loss, etc.) depending on the reporting need.

FAIR describes risk as a probable loss event, where the asset at risk, the threat and the probable consequence are clearly identified.

Our research has uncovered the following risk scenarios to be the most prevalent in these five industries.

## Banking

- Insider Threat leading to PII/PCI data loss
- Cyber criminals exfiltrating data via Third Party APIs
- Cyber criminals accessing payment system and sending fraudulent wire transfers
- DDoS causes outage of critical customer-facing banking applications
- Big Game Ransomware on critical transaction processing applications causes outage/data loss

## Healthcare Providers

- Ransomware leading to PII/PHI data loss (Electronic Medical Records)
- Cyber criminals exfiltrating patient data via Third Party APIs
- Insider Error leads to data exposure
- Insider Error leads to outage of critical system(s)
- Ransomware causes systems outage

## Retail

- ▮ Cyber criminals exfiltrating PII/PCI data via phishing/web app attack/ransomware
- ▮ Cyber criminals or insider error causing outage of customer-facing eCommerce platform during key time of year
- ▮ Cyber criminals exfiltrating PII/PCI data via Third Party APIs
- ▮ Malicious Insiders exfiltrating PII/PCI data
- ▮ Supply Chain Outage

## Accommodation

- ▮ Cyber criminals exfiltrating PII/PCI data from guest database(s) via network foothold/system intrusion
- ▮ Cyber criminals exfiltrating PII/PCI data from customer-facing web portal (i.e. rewards program, booking website, etc.)
- ▮ Cyber criminals exfiltrating customer data via Third Party APIs
- ▮ Ransomware leading to PII/PCI data loss/outage
- ▮ Insider Threats leading to exfiltrating PII/PCI data or exposing data in error

## Manufacturing

- ▮ Ransomware leading to outage in critical production process
- ▮ Insider Error leading to product liability-related losses resulting from corrupted or deleted data impacting manufacturing quality (OT/ISC Systems)
- ▮ Insider exfiltrating critical Intellectual Property
- ▮ DDoS on network causes widespread network outage
- ▮ Insider error causes outage in critical production process

For next year's edition of this report, we started researching benchmark data for such types of discrete risk scenarios, that are closer to how many organizations conduct quantitative cyber risk assessments.





## Introduction

The FAIR Institute Cybersecurity Risk Report is designed to provide reference estimates for the probability, loss, and loss exposure of common cyber breaches, based on the categorization by the Verizon DBIR. It summarizes the findings by industry and event themes and details how actionable variables, such as security stance and data retention management, can reduce risk exposure.

## Methodology

In our approach, real security scans, real events, and real losses drawn from industry sources provide the inputs for hundreds of thousands of FAIR risk simulations.

We summarized millions of outcomes from those scenarios to provide the average outcomes for a generally representative firm. Using this methodology, we present three key outcome variables:

- ▮ Average Probability (annual) – Useful to compare among types of cyber events.
- ▮ Average Loss (per event) – Useful to know the likely impact of an event in a year if one hits.
- ▮ Average Loss Exposure (per event) – Useful to make informed decisions on insurance amortization or other investment decisions to handle risk over time.

Please note that averages are used in this report because of the emphasis on comparisons.

Averages are calculated across 10,000 simulated years per scenario. Scenarios include secondary outcomes<sup>1</sup>, which are also probabilistically modeled. This means that Average Exposure will not equal Average Probability multiplied by Average Loss, but those are each relevant summaries of those independent distributions.

If you are interested in assessing the risk associated with the specific scenarios outlined in this study for your own company, Safe Security's CRQ software leverages the industry benchmark data and the FAIR standard used in this report to help organizations calculate their own loss exposure to cyber events, compare it to industry averages and assess materiality.

## Data Sources

Inputs for this simulation study incorporate security scans, events, and loss data from several industry sources in 2023, including:

- 2023 Verizon Data Breach Investigations Report (DBIR)
- VERIS Community Database (VCDB)
- SecurityScorecard
- Zywave
- St. Louis Federal Reserve Economic Data (FRED)

## Reference Organization Characteristics

The representative/reference organization used for this simulation study is a mid-sized organization in North America of 500-1,000 employees and USD \$100M-\$1B in revenue with personally identifiable information (PII) records at risk.

<sup>1</sup> According to FAIR, risk analysis must also consider the possible fallout of primary impacts. In many scenarios, the potential impact from things like reputation damage, fines and judgments, legal costs, etc. can be much different and even greater than the immediate primary losses.



Top Risk Scenarios  
by Industry

Introduction

Top Industries by  
Total Loss Exposure

Top Risk Themes by  
Total Loss Exposure

The Implementation  
Challenge

Top Risk Themes  
by Industry

Defining the Materiality  
of Cyber Incidents

## The Price of Bigness

One pattern jumps out of this year's data: Large organizations (measured in revenue and employee count) have a much higher likelihood and severity of cyber loss events compared to our baseline – a mid-market reference firm of up to 1,000 employees and \$1B in revenue.

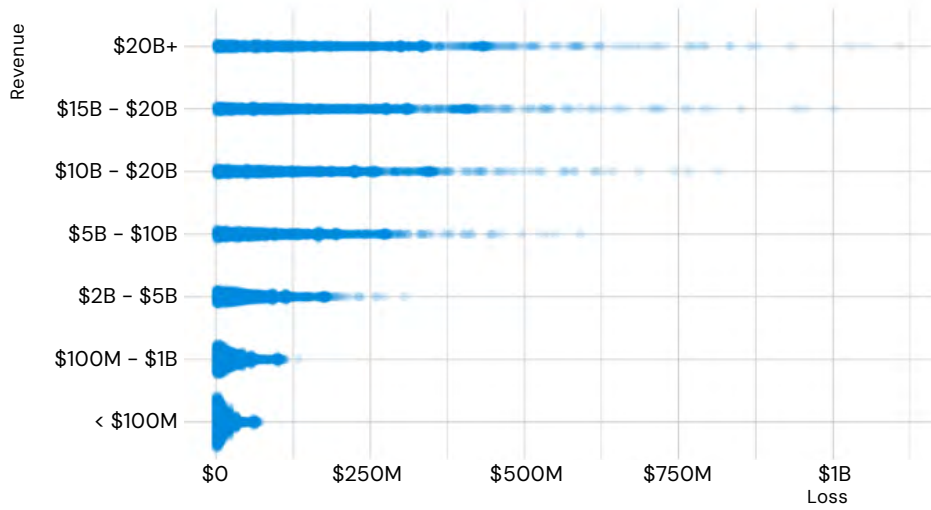
A large healthcare company has a better than 50% chance of a serious Insider Error event! That figure goes down to 26% for our reference mid-market organization.

What's going on here? We can speculate that a compounding effect kicks in. The more people, systems, data, third parties, etc., the more errors will occur, and a series of small events can snowball over time.

# These charts tell the story

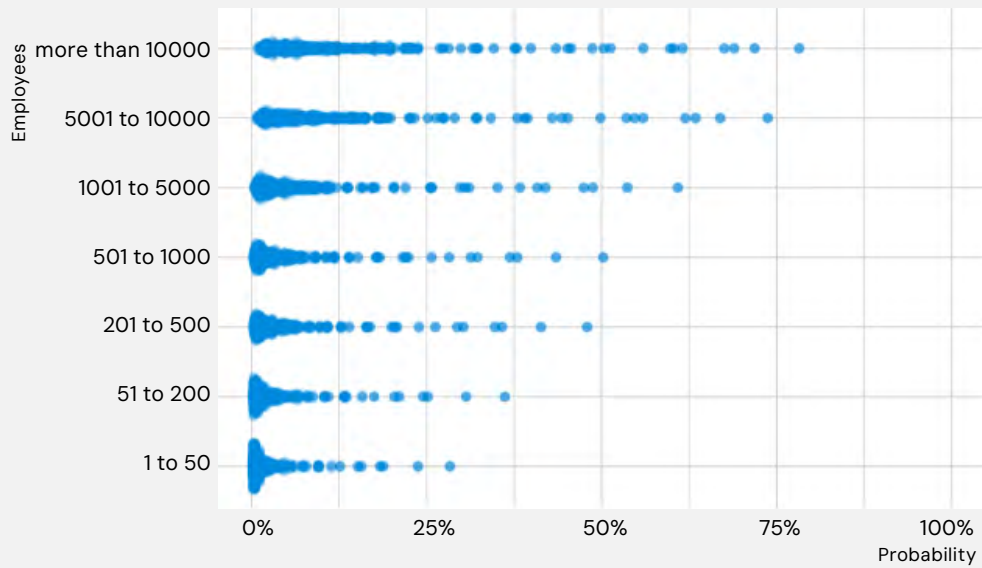
## Larger Revenues, Larger Losses

As firm revenue, increases, expected losses also increase



## More People, More Events

As Firm Employees increases, event probability increases



Top Risk Scenarios  
by Industry

Introduction

Top Industries by  
Total Loss Exposure

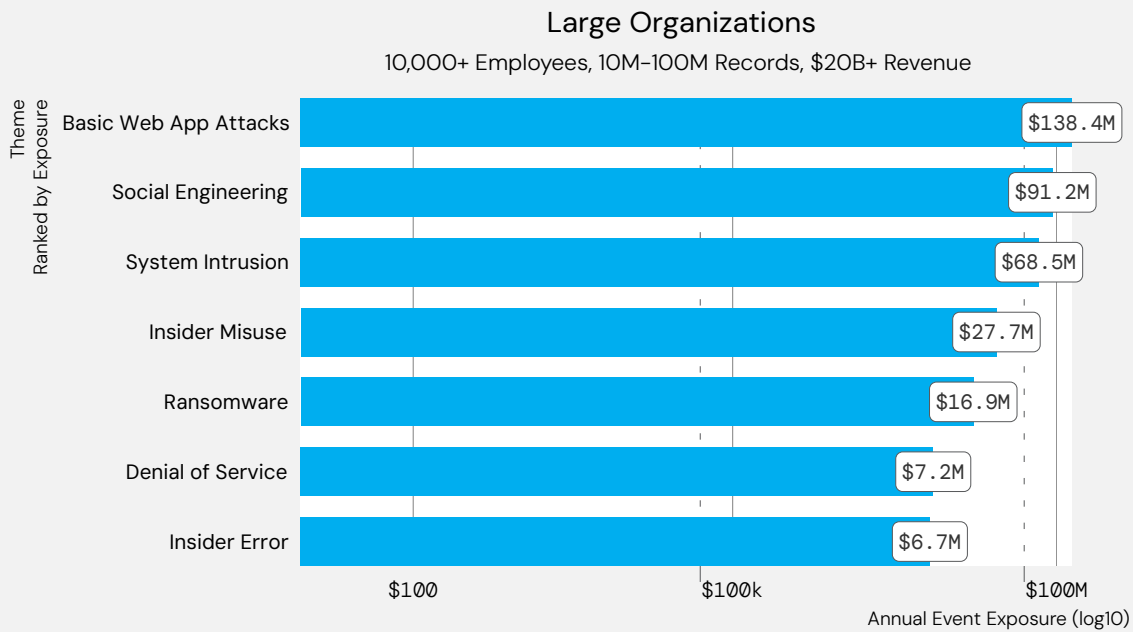
Top Risk Themes by  
Total Loss Exposure

The Implementation  
Challenge

Top Risk Themes  
by Industry

Defining the Materiality  
of Cyber Incidents

The size of an organization also shifts the priorities of cyber defenders based on the probable loss exposure, as this chart shows. For instance, Ransomware is a higher risk in monetary terms for large vs. small businesses.



Top Risk Scenarios by Industry

Introduction

Top Industries by Total Loss Exposure

Top Risk Themes by Total Loss Exposure

The Implementation Challenge

Top Risk Themes by Industry

Defining the Materiality of Cyber Incidents

# Top Industries by Total Loss Exposure

We assessed the average loss exposure (probable likelihood and probable financial impact) related to key risk themes across a range of industries and plotted them to give readers a quantified view of the industries that face the highest overall cyber risk.

## Analysis

As in last year’s report, **the two top industries by average loss exposure (per risk scenario) are Public Administration and Healthcare.**

Key drivers were the relatively high probability of a loss event in a year – on average:

- 16% for Public Administration
- 9% for Healthcare

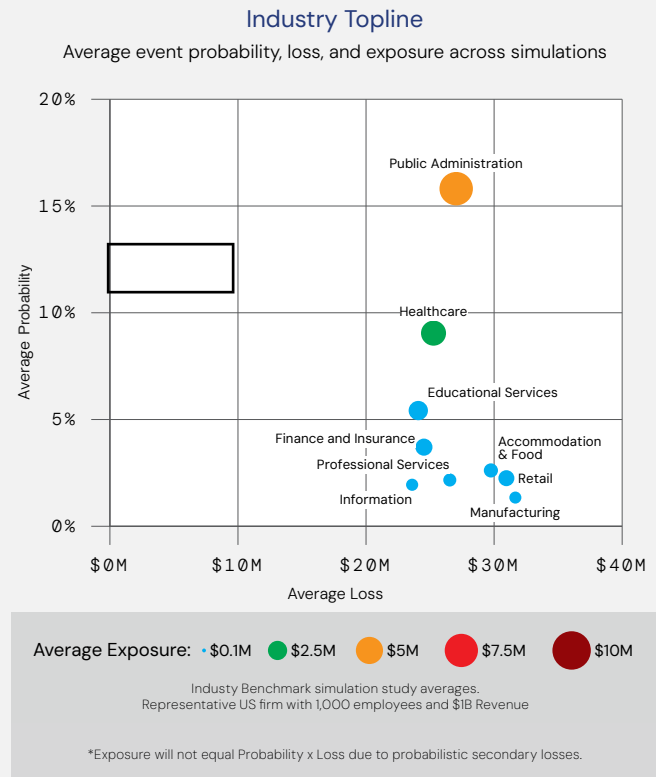
Local governments are particularly vulnerable targets due to underfunded cybersecurity programs and complicated attack surfaces, ranging from DMVs to airports.

- But the loss picture has improved – average loss exposure is down from \$7.6 million in 2022 to \$4.9 million in 2023.
- Insider Misuse Displaced Basic Web Application Attack (by outsiders) is the #1 risk theme

In Healthcare, loss exposure dropped by about half:

- Driven by significant improvement in the average loss per event column, indicating that health institutions may be improving at controlling the impact of those incidents
- In the probability column, hospitals and other providers are still plagued with a high likelihood of attack in a year: 21.8% for insider misuse and 25.9% for insider error, two risk themes particularly targeting sensitive health records

Industry	Loss*	Prob	Exposure
Public Administration	\$27.0M	15.8%	\$4.9M
Healthcare	\$25.3M	9.0%	\$2.7M
Educational Services	\$24.1M	5.4%	\$1.6M
Finance & Insurance	\$24.5M	3.7%	\$1.3M
Retail	\$31.0M	2.3%	\$1.1M
Accommodation & Food	\$29.7M	2.6%	\$872.1K
Professional Services	\$26.5M	2.2%	\$738.1K
Information	\$23.6M	1.9%	\$639.3K
Manufacturing	\$31.7M	1.3%	\$632.6K



Top Risk Scenarios by Industry

Introduction

Top Industries by Total Loss Exposure

Top Risk Themes by Total Loss Exposure

The Implementation Challenge

Top Risk Themes by Industry

Defining the Materiality of Cyber Incidents

# Top Risk Themes by Total Loss Exposure

We assessed the average loss exposure (probable likelihood and probable financial impact) of key risk themes across a range of industries and plotted them to give readers a quantified view of the top risks faced by these industries overall.

## Analysis

In our methodology, we analyze how losses play out probabilistically over 10,000 simulated years, incorporating both the loss magnitude and probability of events (plus secondary loss event simulations).

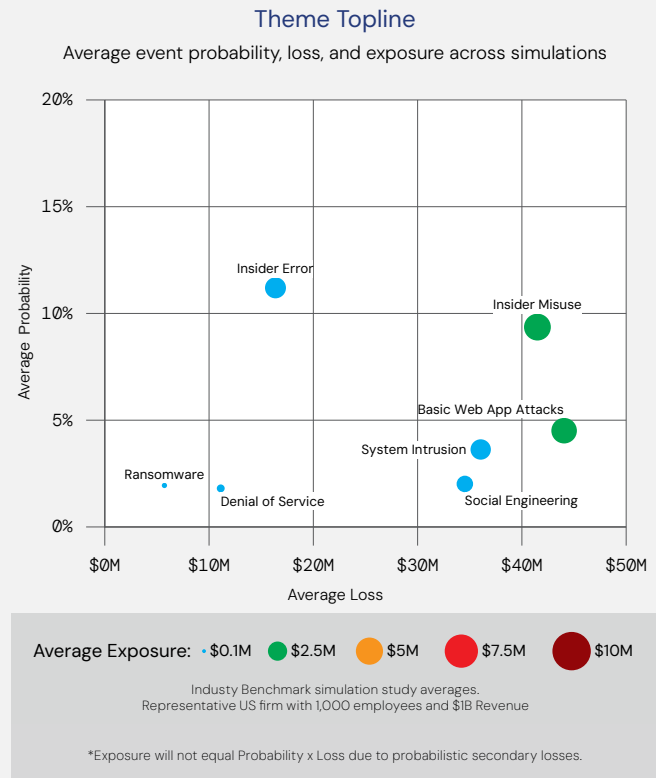
A key value of this simulation study is ranking risks by Average Loss Exposure (per risk scenario). This is a fundamental improvement over much of the cyber risk reporting out there that captures only the most expensive or the most frequent events.

Look at the column for Average Loss Per Event: System Intrusion and Social Engineering. The two score relatively high in cost but, balanced out by low probability, yield relatively low exposure. Insider Error is the most probable risk event in a year, but the relatively low Average Loss Per Event holds its Average Loss Exposure (per scenario) down to third place.

This year, every one of our Risk Theme estimates saw a drop in Average Loss Exposure (per event), some quite sizeable:

- Basic Web Application Attacks fell from \$5.1 million to \$2.8 million
- Insider Error (Including Misconfigurations) from \$4.6 million to \$1.9 million
- Insider Misuse fell from \$4.1 million to \$3.1 million

Theme	Loss*	Prob	Exposure
Insider Misuse	\$41.5M	9.4%	\$3.1M
Basic Web App Attacks	\$44.0M	4.5%	\$2.8M
Insider Error	\$16.4M	11.2%	\$1.9M
System Intrusion	\$36.1M	3.6%	\$1.8M
Social Engineering	\$34.5M	2.0%	\$1.2M
Denial of Service	\$11.1M	1.8%	\$274.9K
Ransomware	\$5.7M	1.9%	\$123.4K



Top Risk Scenarios by Industry

Introduction

Top Industries by Total Loss Exposure

Top Risk Themes by Total Loss Exposure

The Implementation Challenge

Top Risk Themes by Industry

Defining the Materiality of Cyber Incidents

## Main Risk Reduction Factors

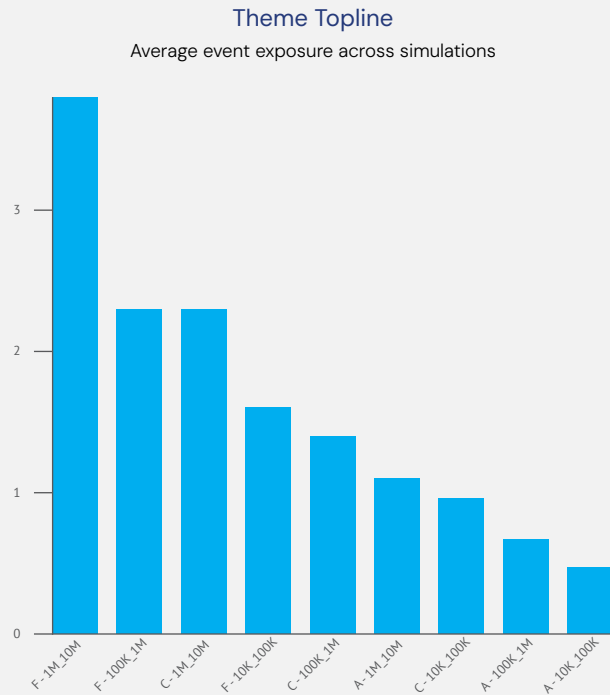
When it comes to cyber risk reduction for the data breach scenarios analyzed in this study, there are two key levers a security organization can pull:

1. reducing the number of records held in databases.
2. raising the security profile, such as securing web applications and endpoints or increasing patching cadence.

We compared variables of SecurityScorecard letter grades for risk posture and database size to get a picture of the average effect on loss exposure.

As the chart shows, the risk reduction can be dramatic – An organization with an F grade and 1M – 10M records that improved to an A grade and 100K – 1 M records would see a reduction in loss exposure of 82%.

Security grade & Records	Exposure
F - 1M_10M	\$3.8M
F - 100K_1M	\$2.3M
C - 1M_10M	\$2.3M
F - 10K_100K	\$1.6M
C - 100K_1M	\$1.4M
A - 1M_10M	\$1.1M
C - 10K_100K	\$956.9K
A - 100K_1M	\$666.8K
A - 10K_100K	\$469.3K



Top Risk Scenarios by Industry

Introduction

Top Industries by Total Loss Exposure

Top Risk Themes by Total Loss Exposure

The Implementation Challenge

Top Risk Themes by Industry

Defining the Materiality of Cyber Incidents



# The Implementation Challenge



Research from EY

How Global Companies Are Responding to Evolving Cyber Risks

In early 2023, EY surveyed 500 global C-suite and cybersecurity leaders across 19 different sectors and 25 countries, to better understand how companies approach their organization's cybersecurity. EY found that there is commonality among the top challenges and preparations for today's risks, and future attacks.

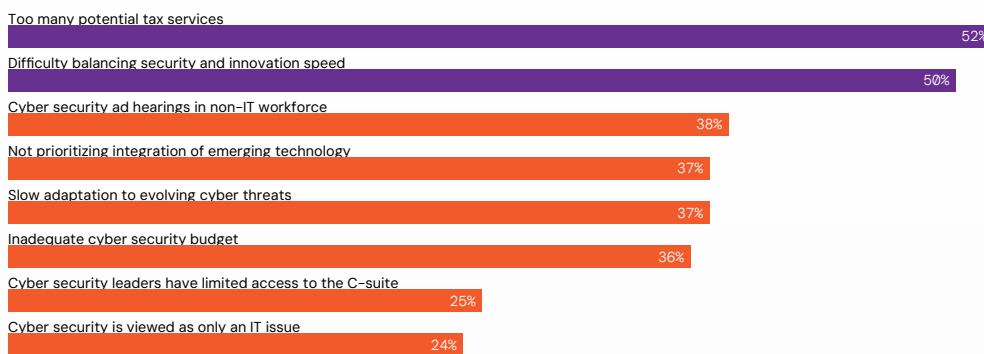
Using statistical modeling, EY identified leading organizations with the most effective cybersecurity — EY calls this group "Secure Creators." Compared to their lower-performing counterparts, "Prone Enterprises," Secure Creators have fewer cyber incidents and are quicker at detecting and responding to incidents. They are also more likely to be satisfied with their cybersecurity approach today (51% vs. 36%) and more likely to feel prepared for the threats of tomorrow (53% vs. 41%).

"Too many attack surfaces" was the most cited internal challenge to organizations' cybersecurity approach. Within the organization, the transition to cloud computing at scale and the Internet of Things (IoT) have increased openings for cyber breaches. Moreover, an ecosystem-led approach to business today, while helping drive value, also presents a significant cybersecurity challenge. All told, 53% of cyber leaders agree there is no such thing as a secure perimeter in today's digital ecosystem. Most dangerous of all are supply chains, responsible for 62% of system intrusion incidents.

CISOs need to transform how cybersecurity technology is introduced across the enterprise,

## Biggest internal challenges to the organization's cybersecurity approach

Percentage selecting a challenge among their top three choices



Data visualization bar chart showing the top internal challenges to the organization cyber security approach.

developing a holistic technology strategy that rationalizes existing systems and addresses the cybersecurity needs of emerging business imperatives such as cloud and ecosystem partnerships and makes full use of automation. Secure Creators follow this approach.

While 70% defined themselves as early adopters of emerging technology, they are focused on advanced solutions to simplify their environment, in particular by harnessing automation. They are

Top Risk Scenarios by Industry

Introduction

Top Industries by Total Loss Exposure

Top Risk Themes by Total Loss Exposure

The Implementation Challenge

Top Risk Themes by Industry

Defining the Materiality of Cyber Incidents

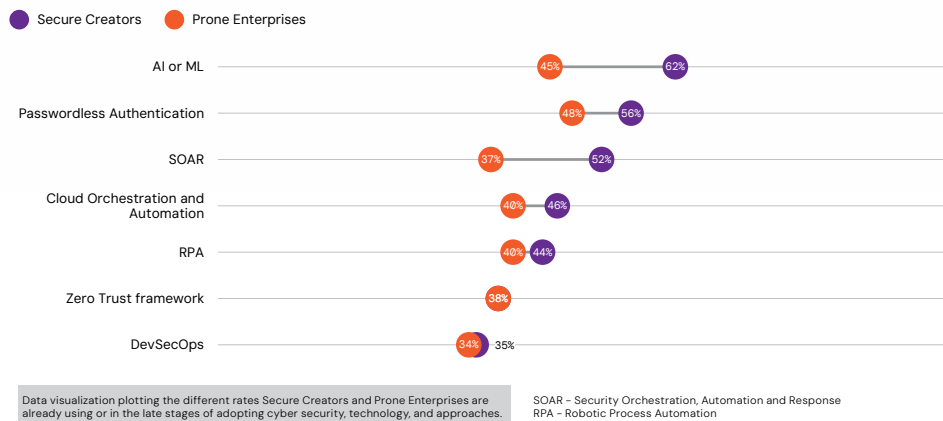


more likely to use or are in the late stages of adopting artificial intelligence or machine learning (AI or ML) (62% vs. 45%) and Security, Orchestration, Automation and Response (SOAR) (52% vs. 37%). This gives them a seamless, organization-wide defense, and a clear line of sight to cybersecurity incidents.

Cyber risk quantification is an emerging area where automation and data analytics can add insight and aid risk prioritization. Executive committees and boards are asking more questions about cyber

### Secure Creators are focused on automation

Percent already using or in the late stages of adopting in their cyber security approach



and digital risk. Cyber leadership should aspire to have a business dialog with stakeholders. Explaining cyber risk in dollar value terms is far more powerful and enables better decision-making, than the technical updates CISOs have traditionally provided.

You can access the full "EY 2023 Global Cybersecurity Leadership Insights Study" at [https://www.ey.com/en\\_gl/consulting/is-your-greatest-risk-the-complexity-of-your-cyber-strategy?linkId=238232488](https://www.ey.com/en_gl/consulting/is-your-greatest-risk-the-complexity-of-your-cyber-strategy?linkId=238232488)

- Top Risk Scenarios by Industry
- Introduction
- Top Industries by Total Loss Exposure
- Top Risk Themes by Total Loss Exposure
- The Implementation Challenge
- Top Risk Themes by Industry
- Defining the Materiality of Cyber Incidents



Top Risk Scenarios  
by Industry

Introduction

Top Industries by  
Total Loss Exposure

Top Risk Themes by  
Total Loss Exposure

The Implementation  
Challenge

Top Risk Themes  
by Industry

Defining the Materiality  
of Cyber Incidents

## Top Risk Themes by Industry

Public Administration.....	18
Healthcare.....	19
Educational Services.....	20
Finance and Insurance.....	21
Retail.....	22
Accommodation and Food Services.....	23
Professional Services.....	24
Information.....	25
Manufacturing.....	26

# Public Administration

## #1 for Loss Exposure

State and local government agencies.

Theme	Loss*	Prob	Exposure
Insider Misuse	\$27.6M	31.0%	\$9.1M
System Intrusion	\$34.0M	18.4%	\$8.7M
Basic Web App Attacks	\$33.9M	11.2%	\$5.7M
Insider Error	\$12.1M	36.4%	\$4.8M
Social Engineering	\$67.9M	4.1%	\$4.8M
Denial of Service	\$10.4M	5.0%	\$647.6K
Ransomware	\$3.4M	4.5%	\$200.6K

\*Exposure will not equal Probability x Loss due to probabilistic secondary losses.

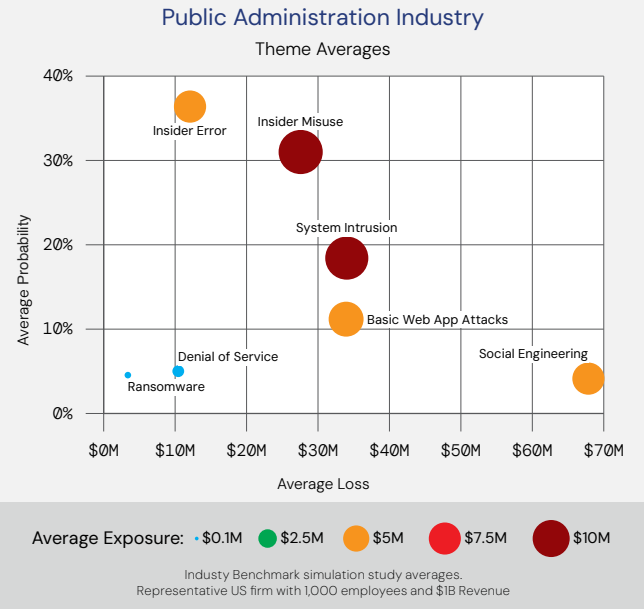
## Analysis

Oakland, CA...Dallas, TX...Lowell, MA...Augusta, GA... and many more hacked, disrupted, ransomed, and later sued municipalities have kept Public Administration at #1 again this year.

Local governments by now are well known in cyber criminal circles for their under-funded cybersecurity programs and their enormously complicated attack surfaces, ranging from DMVs to schools to hospitals to airports.

## Top Risk Theme

Insider Misuse, leading to exploitation of sensitive data



Now for the good news. Average loss exposure is down significantly from \$7.6M in 2022 to \$4.9M in 2023, thanks to reductions in probability. One interesting development among the risk themes is that insider misuse displaced basic web application attacks as the #1 risk theme.

Top Risk Scenarios by Industry

Introduction

Top Industries by Total Loss Exposure

Top Risk Themes by Total Loss Exposure

The Implementation Challenge

Top Risk Themes by Industry

Defining the Materiality of Cyber Incidents

# Healthcare

## #2 for Loss Exposure

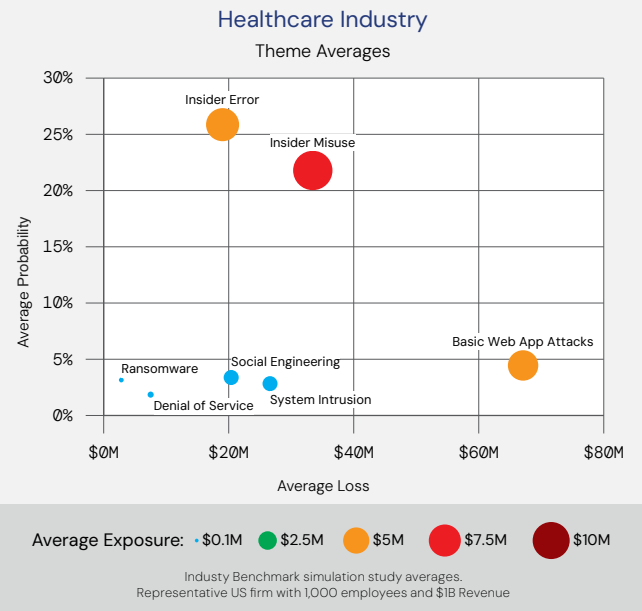
Hospitals and outpatient treatment facilities, health and dental practices.

Theme	Loss*	Prob	Exposure
Insider Misuse	\$33.5M	21.8%	\$7.2M
Insider Error	\$19.0M	25.9%	\$5.1M
Basic Web App Attacks	\$67.1M	4.4%	\$4.3M
Social Engineering	\$20.4M	3.4%	\$1.1M
System Intrusion	\$26.6M	2.8%	\$1.0M
Denial of Service	\$7.5M	1.9%	\$174.7K
Ransomware	\$2.8M	3.2%	\$108.3K

\*Exposure will not equal Probability x Loss due to probabilistic secondary losses.

## Top Risk Theme

Insider Misuse, often sending sensitive patient data to the wrong recipient by email or snail-mail.



## Analysis

Some possible welcome relief for this cyber-troubled sector indicated by our latest numbers. Loss exposure dropped by about half over 2022, driven by significant improvements in the average loss per event column (while average probability of attack remained high).

Probabilities of 21.8% and 25.9% for the top risk themes of insider misuse and insider error, are nothing to celebrate, but the declining per-event loss figures indicate that Healthcare could be better at controlling the impact.

In a new category of human error for this sector, online therapy provider Cerebral announced that it leaked patient data through tracking pixels used by websites.

## The Price of Bigness

A Healthcare organization with over 10,000 employees and over \$20 billion in revenue has a 54.3% probability of an Insider Error costing \$30.4 million, with an annualized exposure of \$13.9 million.

Top Risk Scenarios by Industry  
Introduction  
Top Industries by Total Loss Exposure  
Top Risk Themes by Total Loss Exposure  
The Implementation Challenge  
Top Risk Themes by Industry  
Defining the Materiality of Cyber Incidents

# Educational Services

## #3 for Loss Exposure

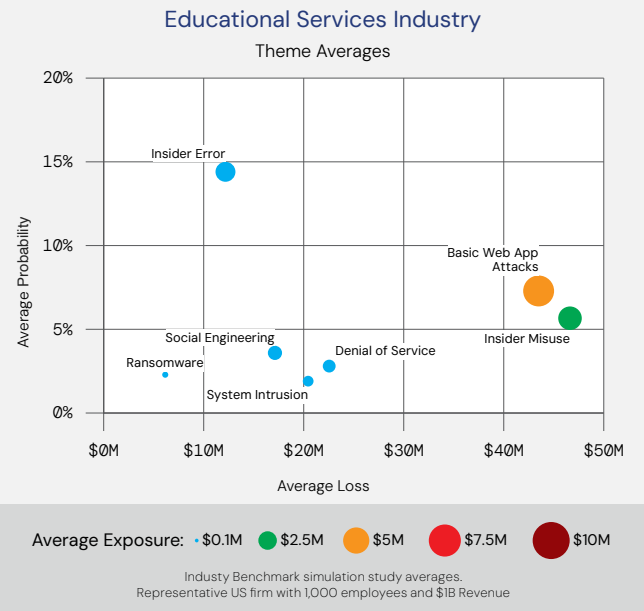
Privately or publicly owned schools, colleges, universities, and training centers.

Theme	Loss*	Prob	Exposure
Basic Web App Attacks	\$43.5M	7.3%	\$4.5M
Insider Misuse	\$46.6M	5.7%	\$2.6M
Insider Error	\$12.2M	14.4%	\$1.9M
Social Engineering	\$17.1M	3.6%	\$938.6K
Denial of Service	\$22.5M	2.8%	\$767.1K
System Intrusion	\$20.4M	1.9%	\$536.9K
Ransomware	\$6.2M	2.3%	\$171.7K

\*Exposure will not equal Probability x Loss due to probabilistic secondary losses.

## Top Risk Theme

Basic Web Application attack, leveraging stolen credentials.



## Analysis

Surely one of the most despicable subsets of the cybercriminal class are attackers who target K-12 schools to steal student information and disrupt teaching.

School districts are typically underfunded for cybersecurity and increasingly dependent on EdTech. After a cyber attack, students can take two to nine months to make up for the learning loss, a government study found.

A troubling finding of our study was that schools are twice as likely to suffer a loss event from insider error than outsider attack, indicating some serious training deficiencies.

The good news is that loss exposure in dollars from insider error is down from 2022 by about half, part of the overall downward slope in exposure for this sector.

Top Risk Scenarios by Industry

Introduction

Top Industries by Total Loss Exposure

Top Risk Themes by Total Loss Exposure

The Implementation Challenge

Top Risk Themes by Industry

Defining the Materiality of Cyber Incidents

# Finance and Insurance

## #4 for loss exposure

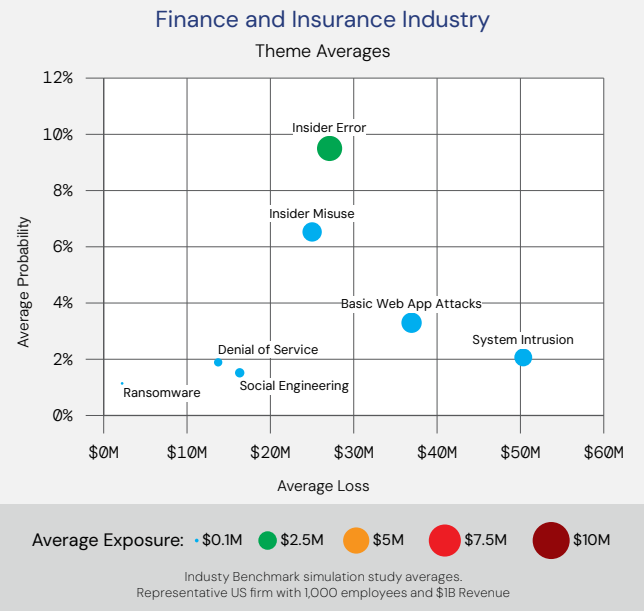
Banks, insurers, lenders, investment companies and others involved in financial transactions.

Theme	Loss*	Prob	Exposure
Insider Error	\$27.1M	9.5%	\$3.0M
Basic Web App Attacks	\$36.9M	3.3%	\$1.9M
Insider Misuse	\$25.0M	6.5%	\$1.7M
System Intrusion	\$50.3M	2.1%	\$1.5M
Social Engineering	\$16.3M	1.5%	\$409.9K
Denial of Service	\$13.7M	1.9%	\$324.1K
Ransomware	\$2.2M	1.1%	\$34.4K

\*Exposure will not equal Probability x Loss due to probabilistic secondary losses.

## Top Risk Theme

Insider Error, often for leaking customer financial data.



## Analysis

In a massive illustration of the hazards of third-party risk, a long list of insurance companies fell victim to the MOVEit hack through Pension Benefit Information (PBI), a widely used service that monitors death notices for insurers. Millions of records were compromised.

Among them was JP Morgan, which became the face for insider error – the leading risk category in the banking industry – when the SEC fined it \$4 million for accidentally deleting financial records of its retail banking customers in a botched attempt to clean out email inboxes.

## The Price of Bigness

A large Finance and Insurance organization with over 10,000 employees and over \$20 billion in revenue has a 7.7% risk of a System Intrusion costing \$300.2 million, with an annualized exposure of \$27.9 million.

# Retail

## #5 for Loss Exposure

Sellers of merchandise via brick-and-mortar or online stores.

Theme	Loss*	Prob	Exposure
Basic Web App Attacks	\$65.0M	4.3%	\$4.0M
Insider Misuse	\$37.0M	3.8%	\$1.4M
System Intrusion	\$55.8M	1.3%	\$1.0M
Insider Error	\$26.0M	3.4%	\$946.4K
Social Engineering	\$17.3M	0.9%	\$219.5K
Denial of Service	\$14.9M	1.1%	\$205.2K
Ransomware	\$0.7M	1.0%	\$8.3K

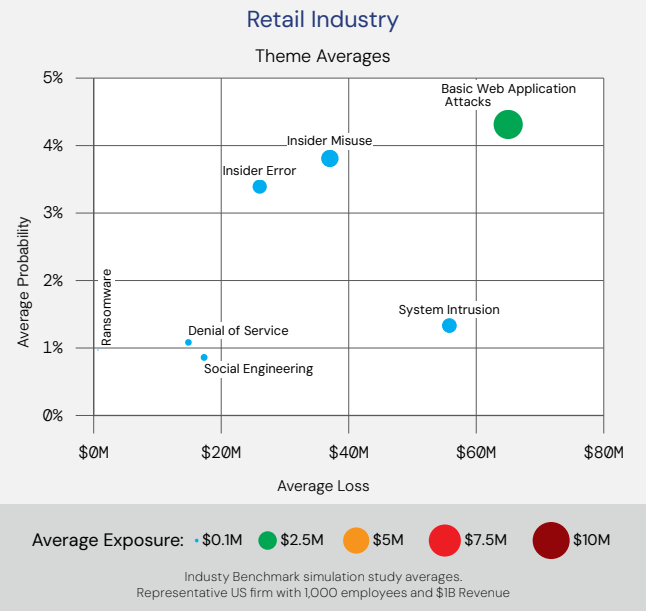
\*Exposure will not equal Probability x Loss due to probabilistic secondary losses.

## Analysis

A particularly insistent basic web application attack campaign pummeled the retail chain Hot Topic in 2023, with 12 days of breaches, spread across five waves of attacks during the first half of the year, powered by automated credential stuffing. Unable to tell which accounts, if any, were compromised, Hot Topic asked all its clients to re-register.

## Top Risk Theme

Basic Web Application Attacks, often by credential/password theft.



The Retail sector showed an improvement in overall average loss exposure at \$1.1M, down from \$1.5M in 2022, with Basic Web Application Attack again the worse threat.



# Accommodation and Food Services

## #6 for Loss Exposure

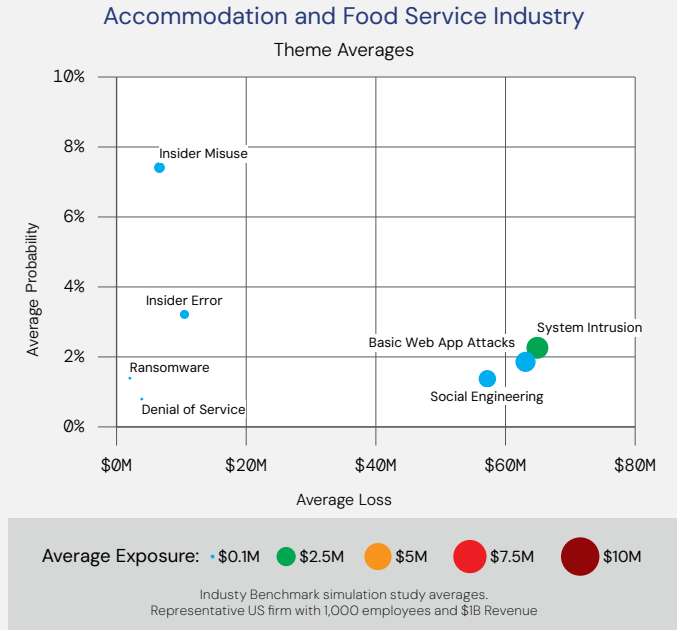
Providers of lodging and/or prepared foods and beverages.

Theme	Loss*	Prob	Exposure
System Intrusion	\$64.9M	2.3%	\$2.1M
Basic Web App Attacks	\$63.1M	1.9%	\$1.8M
Social Engineering	\$57.2M	1.4%	\$1.3M
Insider Misuse	\$6.6M	7.4%	\$500.7K
Insider Error	\$10.5M	3.2%	\$360.4K
Denial of Service	\$3.9M	0.8%	\$37.3K
Ransomware	\$2.1M	1.4%	\$35.7K

\*Exposure will not equal Probability x Loss due to probabilistic secondary losses.

## Top Risk Theme

System Intrusion, typically via malware to gather credit card data.



## Analysis

Organizations in this category maintain large databases of personal customer information or rely heavily on just-in-time supply chains – both vulnerable targets for attack.

In 2023, that led to what must have been the first cyber salad shortage– Dole, the major supplier of packaged fresh fruits and vegetables, had to temporarily shut down North American production this year (losing \$10 million) after it was hit with ransomware.

But overall, loss exposure in this sector dropped by about one quarter year to year, led by reduction in costs from System Intrusion incidents.

Top Risk Scenarios by Industry

Introduction

Top Industries by Total Loss Exposure

Top Risk Themes by Total Loss Exposure

The Implementation Challenge

Top Risk Themes by Industry

Defining the Materiality of Cyber Incidents

# Professional Services

## #7 for Loss Exposure

Lawyers, accountants, architects, engineers, IT consultants, and other technical experts.

Theme	Loss*	Prob	Exposure
Insider Misuse	\$57.3M	3.3%	\$1.9M
Basic Web App Attacks	\$32.1M	2.8%	\$1.3M
Social Engineering	\$42.1M	1.3%	\$799.0K
System Intrusion	\$27.4M	1.4%	\$543.8K
Insider Error	\$10.6M	3.6%	\$411.7K
Denial of Service	\$9.6M	1.2%	\$137.2K
Ransomware	\$6.8M	1.6%	\$131.3K

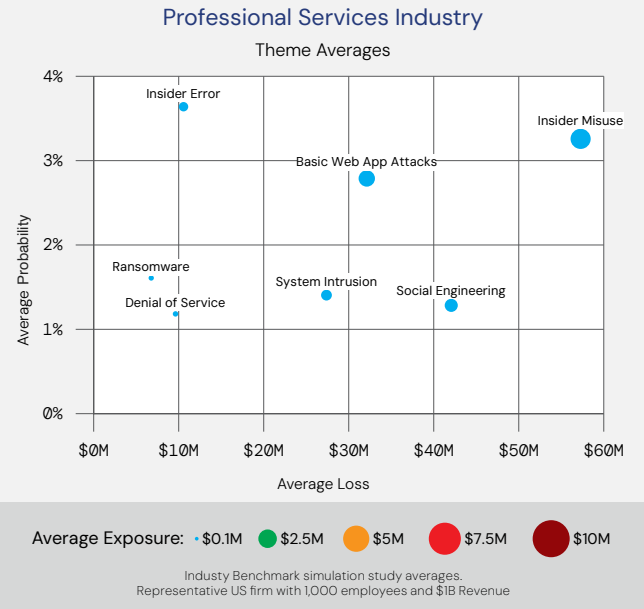
\*Exposure will not equal Probability x Loss due to probabilistic secondary losses.

## Analysis

Law firms and other professional services are the keepers of sensitive client data – and heavy users of digital tools. Two ways that can go wrong were illustrated by the unfortunate international law firm Proskauer Rose in 2023. Proskauer exposed client M&A data on an unsecured Microsoft Azure cloud server, it was revealed in April. Then in July, came news that Proskauer and other big firms were caught up in the MOVEit compromise.

## Top Risk Theme

Insider Misuse, most likely to leak sensitive information.



Overall, Professional Services moved up from 9th place on our list, the lowest spot, to 7th – though average loss exposure per scenario went down from \$974K to \$738K.

# Information

## #8 for Loss Exposure

Broad category covering producers and distributors of information and cultural products, including news, movie/video, website, and music production, but also telecommunications, IT infrastructure, and data processing.

Theme	Loss*	Prob	Exposure
Basic Web App Attacks	\$23.6M	3.7%	\$1.3M
Insider Misuse	\$53.3M	2.1%	\$1.3M
Social Engineering	\$28.8M	1.3%	\$590.3K
System Intrusion	\$24.6M	1.4%	\$511.7K
Insider Error	\$14.6M	3.0%	\$500.5K
Ransomware	\$10.5M	1.0%	\$142.3K
Denial of Service	\$9.9M	1.1%	\$132.1K

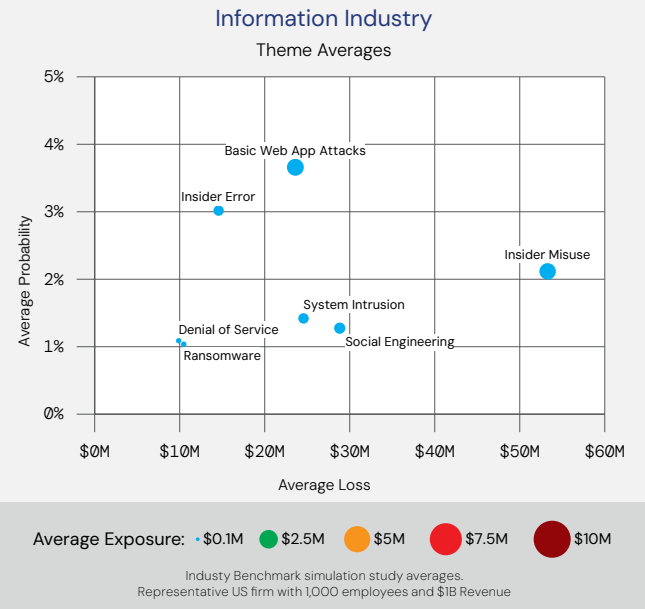
\*Exposure will not equal Probability x Loss due to probabilistic secondary losses.

## Analysis

Information stands relatively low for risk compared to other industries but web application attacks remain the #1 threat for this industry. T-Mobile reported that a threat actor stole personal information on 37 million customers by an attack on an API.

## Top Risk Theme

Basic Web Application Attacks, most likely by financially motivated criminals.



Still, the trend is positive, with overall average loss exposure at \$639K, down from \$1.1M last year.

## The Price of Bigness

A large Information organization with over 10,000 employees and over \$20 billion in revenue faces a 12.8% probability of a Web Application attack costing \$211.6 million, with an annualized exposure of \$30.1M.

# Manufacturing

## #9 for Loss Exposure

Plants, factories, or mills that produce or assemble goods for use or consumption.

Theme	Loss*	Prob	Exposure
Insider Misuse	\$86.5M	2.7%	\$2.4M
Basic Web App Attacks	\$31.2M	1.7%	\$753.2K
Social Engineering	\$43.7M	0.7%	\$480.4K
System Intrusion	\$20.4M	1.0%	\$288.5K
Ransomware	\$16.9M	1.4%	\$277.6K
Insider Error	\$15.3M	1.4%	\$226.7K
Denial of Service	\$7.6M	0.5%	\$48.4K

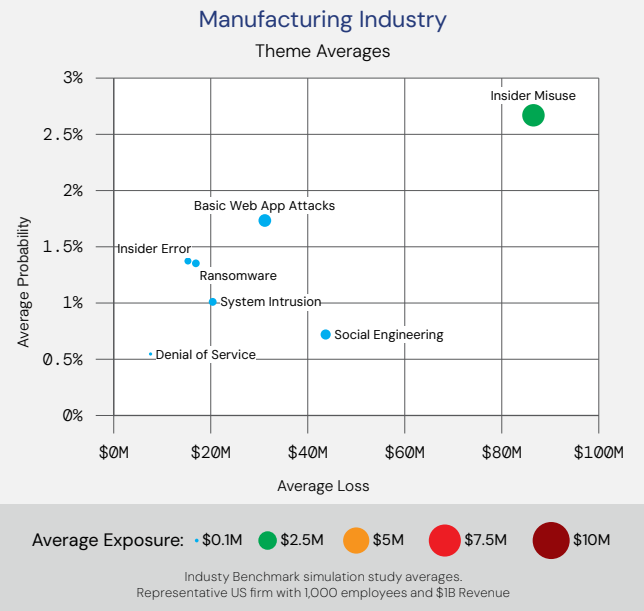
\*Exposure will not equal Probability x Loss due to probabilistic secondary losses.

## Analysis

Some substantial reductions in average loss per event helped drive down loss exposure in our numbers for this sector in 2023 vs. 2022. However, some strong cautions persist:

## Top Risk Theme

Insider Misuse, including theft of intellectual property.



In March, CISA issued advisories for 49 vulnerabilities in industrial control systems, some unpatched. The Lockbit ransomware gang demanded an unusually stiff ransom, \$70 million, from TSMC after hacking one of the chipmaking giant's suppliers. TSMC said its operations were not affected.

Top Risk Scenarios by Industry  
Introduction  
Top Industries by Total Loss Exposure  
Top Risk Themes by Total Loss Exposure  
The Implementation Challenge  
Top Risk Themes by Industry  
Defining the Materiality of Cyber Incidents

# Defining the Materiality of Cyber Incidents

In 2023, the Securities and Exchange Commission (SEC) issued new rules mandating companies file a disclosure of a data breach or other cyber incident within four days of determining that the event would have a “material” financial impact. Confusion and consternation followed.

The impact of a major incident can play out over a period – first to discover the extent of the immediate damage, then to reckon the after-effects (for instance, in legal fines or judgments). How could companies gather the data and work through the calculations to satisfy the regulators... and in a few days?

The FAIR Institute came through with a key resource not available before, with the release of the FAIR Materiality Assessment Model (FAIR-MAM™) – the only standard taxonomy to comprehensively define what forms of losses contribute to the measure of materiality in financial terms.

FAIR-MAM tracks cyber losses in 10 categories (for instance, data loss, privacy compromise, business interruption), which break down further in subcategories of more granular forms of loss, to model probable loss to any organization’s cost structure. CISOs or risk managers can use FAIR-MAM in conjunction with a CRQ tool<sup>1</sup> to game out probable losses from top risk scenarios before any incident or to quickly determine if the materiality line has been crossed just after an incident.

Learn more about FAIR-MAM:

<https://www.fairinstitute.org/blog/new-fair-standard-fair-materiality-assessment-model-fair-mam>

The FAIR Institute also provides a free, online information resource based on FAIR-MAM, “How Material Is that Hack?” to show its practical applicability. It provides estimated materiality assessments of recent breaches working from publicly available information and cyber risk analysis based on the FAIR-MAM model.

You can access “How Material Is that Hack?” here: <http://howmaterialisthathack.org/>

---

1 <https://www.safe.security/resources/blog/safe-launches-industry-first-fair-mam-implementation/>



## About Us

### The FAIR Institute

The FAIR Institute is a research-driven not-for-profit organization dedicated to advancing the discipline of cyber and operational risk management through education, standards and collaboration. The driver behind our mission is the breakthrough achieved by FAIR™, the risk taxonomy and quantification standard, key to effective risk management.

Its members – forward-thinking risk officers, cybersecurity leaders and business executives – now exceed 15,000 in over 100 countries, with representation of 50% of Fortune 1000. The FAIR Institute has been recognized by SC Media as one of the three most influential industry organizations of the last 30 years.

To learn more and get involved, visit: [www.fairinstitute.org](http://www.fairinstitute.org).



## About the Sponsors of this Report

### Safe Security

Safe Security is the leader in AI-driven cyber risk management. It has redefined cyber risk measurement and management with its real-time, data-driven approach that empowers enterprise leaders, regulators, and cyber insurance carriers to understand cyber risk in an aggregated and granular manner. The recent acquisition of RiskLens brings together the power of the world's most advanced cyber risk analytics model (FAIR), supported by practitioners in over 50% of Fortune 500 companies, with the world's most advanced AI-fueled Cyber Risk Cloud of Clouds, processing over three billion signals a day.

Having raised over \$100M, Safe is growing over 200% year over year, consecutively for the last three years, and serves some of the largest global enterprises. Visit [safe.security](https://safe.security) and follow us at [@SafeCRQ](https://twitter.com/SafeCRQ).

### EY

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through Consulting and Assurance to help clients grow, transform and operate.

EY's Cyber Practice within Consulting serves as a trusted advisor to global clients including managed services.

Working across Consulting, Assurance, Law, Strategy, Tax and Transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.