2023

Cybersecurity Risk Report

RiskLens

Table of Contents

Executive Summary

Looking out across the sweep of cyber incidents in 2022, attackers spared no industry, sector or organization, no matter how sophisticated. A technology leader like Uber was compromised (reportedly by a 16-year-old from the Lapsus$ gang) along with technology-poor institutions like the Jackson County, MI, Intermediate School District, closed for days by ransomware.

Risk themes continued to evolve in insidiously creative ways, from Insider Misuse (Meta employees were revealed to be ransoming Facebook and Instagram accounts) to ransomware (not just double but triple extortion) to business email compromise (adding voicemail compromise with deep fakes).

Facing this whirl of bad news, cybersecurity defenders, risk managers and business leaders need, more than ever, clarity about their risk landscape and risk posture to guide their actions. At RiskLens, we believe that clarity comes through cyber risk quantification (CRQ). In other words, understanding cyber risk in business terms — dollars and cents — and prioritizing what matters most. To hit that goal requires a transparent, proven risk model and carefully curated cyber risk data. We based this 2023 Cybersecurity Risk Report on Factor Analysis of Information Risk (FAIR™), the international standard for cyber risk quantification (CRQ), and extensive research by the RiskLens Data Science team. We invite you to dig down into this report to discover the most relevant cyber risk data for your organization and benchmark your performance against peers in your industry and others.

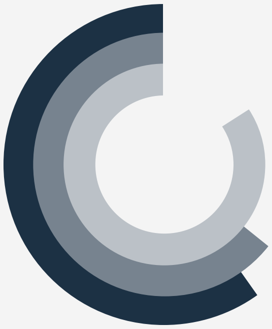
> *"At RiskLens, we believe that clarity comes through cyber risk quantification (CRQ)."*

We conducted this study with a series of simulations built to represent key industries and their exposure to cybersecurity risk in 2022, as presented by a range of cyber threats, both external and internal to the average organization.

The results of this study included the following key findings:

- **The top two threat themes by overall exposure are Web Application Attacks, which had the highest overall loss exposure (risk); and Insider Errors, which were more likely but less costly.**
- **The top two industries by loss exposure are Public Administration and Healthcare, driven by high event probabilities and moderate losses.**
- **Among the levers at the cybersecurity practitioner's disposal to reduce cyber risk are security posture and the data management of records.** Specifically, our study found that making substantial improvements to security posture and reducing the number of records at risk can reduce losses by 60 percent and event probability by 67 percent. Jointly, these levers can reduce overall event exposure by 88 percent.

As a complement to the insights from our study, this report concludes with an article written by Julian Meyrick, Managing Partner & Vice President, Security Strategy Risk & Compliance, Security Services at IBM, a RiskLens partner. In this article, titled, "Using Risk Quantification to Empower Decision Makers and Reduce Cyber Risk across Highly Targeted Industries," Julian describes how organizations can, and have, achieved the promise of CRQ through the disciplined, programmatic application of Factor Analysis of Information Risk (FAIR), the international standard for CRQ.



Security Posture and Data Management of Records

■ Reduce losses by **60%**

■ Event Probability down by **67%**

■ Overall Event Exposure down by **88%**

Introduction

The RiskLens Cybersecurity Risk Report is designed to provide reference estimates for the probability, loss, and loss exposure of common cyber events. 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

This study uses the same underlying methodology as the **RiskLens My Cyber Risk Benchmark tool**. In this approach, real security scans, real events, and real losses drawn from industry sources provide the inputs for hundreds of thousands of FAIR risk scenarios.

RiskLens 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 risks.
- Average Loss (per event) – Useful to know the likely impact of an event in a year if one hits.
- Average Loss Exposure (per scenario) – Useful to make informed decisions on insurance or other investment decisions to handle risk over time.

Averages are calculated across 10,000 simulated years per scenario. Scenarios include secondary outcomes, 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.

Data Sources

Inputs for this simulation study incorporate security scans, events, and loss data from several industry sources in 2022, including:

- **2022 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.

Top Industries by Total Loss Exposure

RiskLens has 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

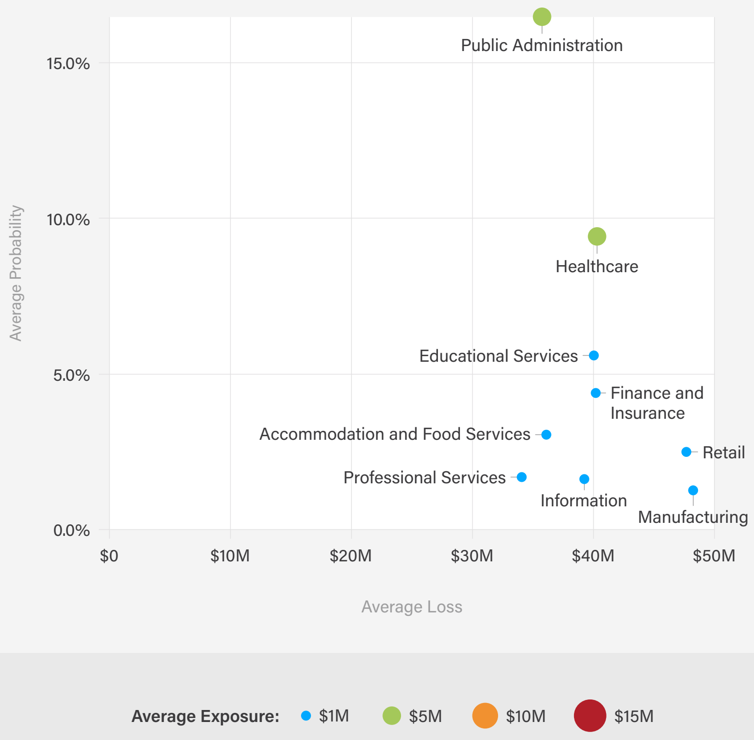
The top two industries by total loss exposure are Public Administration and Healthcare, whose overall exposure was driven by high event probabilities and moderate losses. Public Administration, particularly local governments in the U.S., are the least well-protected among industry categories, often due to budget constraints. They are also among the most likely to be targeted by cyber attackers and, in recent years, have been heavily hit with ransom and encryption attacks causing lengthy disruptions of vital services and revenue sources such as payments for parking tickets or construction permits.

For their part, healthcare providers and payers play a high-stakes game in the cyber risk landscape, with sensitive data (sometimes in the hands of third-party vendors) and patient care at risk, all under the oversight of the U.S. federal government's HHS Office of Civil Rights (OCR) watching – and fining – for violations of HIPAA.

Industry	Loss*	Probability	Exposure
Public Administration	$36.5M	17.0%	$7.6M
Healthcare	$40.6M	9.0%	$5.5M
Educational Services	$40.2M	5.9%	$2.6M
Finance and Insurance	$40.5M	4.1%	$2.1M
Retail	$47.1M	2.5%	$1.5M
Accommodation and Food Services	$36.1M	3.1%	$1.2M
Manufacturing	$48.9M	1.7%	$1.1M
Information	$39.4M	2.2%	$1.1M
Professional Services	$34.7M	2.3%	$974.4K

Industry Topline

Average event probability, loss, and exposure across simulations



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

RiskLens Industry Benchmark simulation study averages. Representative US firm with 1,000 employees and $1B Revenue.

Top Risk Themes by Total Loss Exposure

RiskLens has 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

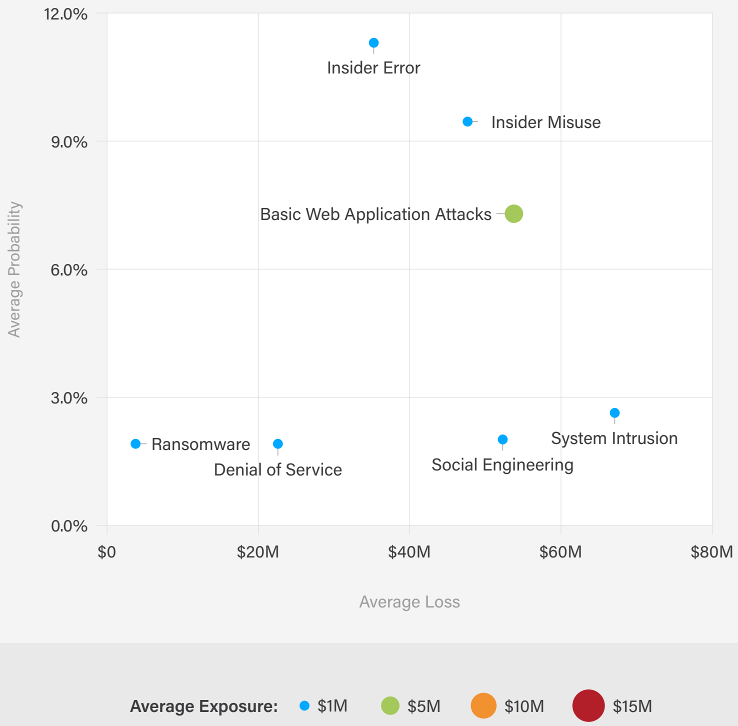
Often when considering risks from existing industry data sources, there is unfortunately only a one-dimensional perspective: only the most expensive events or only the most frequent events. A key value of this simulation study is ranking risks by exposure, a summary of how losses played out probabilistically over 10,000 simulated years, which incorporates both the loss magnitude and probability of events (as well as further secondary loss event simulations).

Consider the top two themes by Probability: Insider Error and Insider Misuse. While these are often the most likely events across industries, they aren't in the top three most expensive losses per event. Similarly, the most expensive theme by Loss is System Intrusion, however it is substantively less probable than the top three most likely themes. The cyber event theme risk practitioners would want to surface to the top is Basic Web Application Attacks, which are relatively probable AND relatively expensive on a per-event basis.

Theme	Loss*	Probability	Exposure
Basic Web Application Attacks	$55.1M	7.0%	$5.1M
Insider Error	$35.5M	11.6%	$4.6M
Insider Misuse	$47M	9.6%	$4.1M
System Intrusion	$66.7M	2.9%	$2.7M
Social Engineering	$54.2M	2.1%	$1.5M
Denial of Service	$22.3M	2.0%	$521.6K
Ransomware	$2.2M	2.0%	$41.9K

Theme Topline

Average event probability, loss, and exposure across simulations



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

RiskLens Industry Benchmark simulation study averages. Representative US firm with 1,000 employees and $1B Revenue.

Average Effect of Security and Records

How can risk strategists and practitioners assess the potential effect of risk posture changes on their exposure? We summarized the average Loss, Probability, and Exposure across a grid of SecurityScorecard scores (A, C, and F) and ranges of records at risk (100k, 1M, 10M). This provides quick reference for the average effect of these variables across themes and industries in our study.

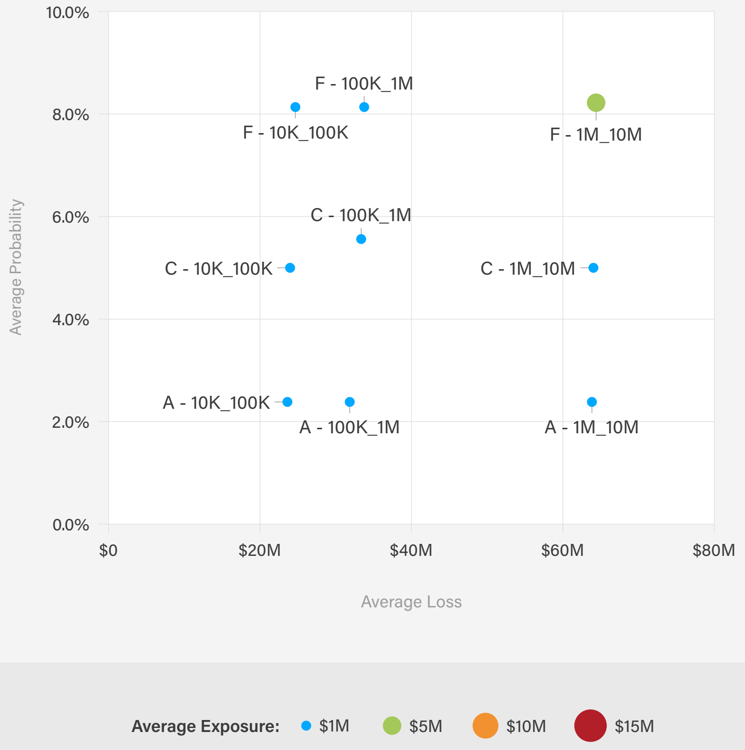
Analysis

Among the levers at the cybersecurity practitioner's disposal to reduce risk are security posture and the data management of records; our study found that substantial improvements to security posture and reductions of records at risk can reduce losses by 60 percent and event probability by 67 percent, and these levers can jointly reduce overall event exposure by 88 percent.

Security and Records	Loss*	Probability	Exposure
F - 1M_10M	$63.6M	8.2%	$6.4M
C - 1M_10M	$63M	5.1%	$3.9M
F - 100K_1M	$33.8M	8.2%	$3.5M
F - 10K_100K	$25.2M	8.2%	$2.4M
C - 100K_1M	$33.4M	5.1%	$2.1M
A - 1M_10M	$62.3M	2.7%	$2.1M
C - 10K_100K	$24.9M	5.1%	$1.5M
A - 100K_1M	$33.1M	2.7%	$1.1M
A - 10K_100K	$24.7M	2.7%	$760.2K

Theme Topline

Average event probability, loss, and exposure across simulations



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

RiskLens Industry Benchmark simulation study averages. Representative US firm with 1,000 employees and $1B Revenue.

Top Risk Themes by Industry

Each industry has a specific risk profile, determined by various factors related to the likelihood and potential financial impact of a given risk theme, including internal and external threats from employees, external actors and even nation states.

The following graphs illustrate the top risk themes that are most relevant to a given industry.

Accommodation and Food Services

This industry includes providers of lodging and/or prepared foods and beverages.

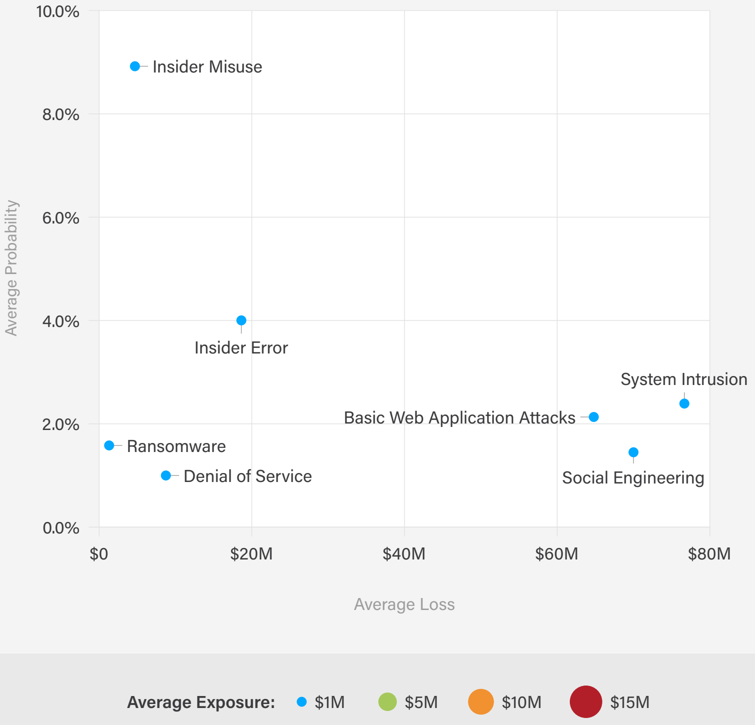
Analysis

Their vast databases of PCI and sensitive personal information (passport numbers, travel itineraries, etc.) make these businesses a juicy target for cyber criminals. Their geographic spread put them in the crosshairs of a large group of regulators with power to levy fines, from state attorneys general to privacy officials in the European Union. And their large customer bases set them up for damaging class action lawsuits. In May 2022, a U.S. federal judge gave the **go-ahead to a class action suit** on behalf of 133 million Americans affected by a breach at Marriott discovered in 2018.

Theme	Loss*	Probability	Exposure
System Intrusion	$81.5M	2.8%	$3.1M
Basic Web Application Attacks	$65.8M	2.2%	$2M
Social Engineering	$70.3M	1.6%	$1.7M
Insider Error	$19.3M	4.0%	$834.4K
Insider Misuse	$6.5M	8.5%	$563K
Denial of Service	$8.6M	1.0%	$89.7K
Ransomware	$745.9K	1.7%	$14K

Accommodation and Food Services Industry

Theme Averages



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

RiskLens Industry Benchmark simulation study averages. Representative US firm with 1,000 employees and $1B Revenue.

Headlines

Sonic Corp. Data Breach Financial Institutions $5.73M Class Action Settlement

IHG Hack: 'Vindictive' Couple Deleted Hotel Chain Data for Fun

Learn More

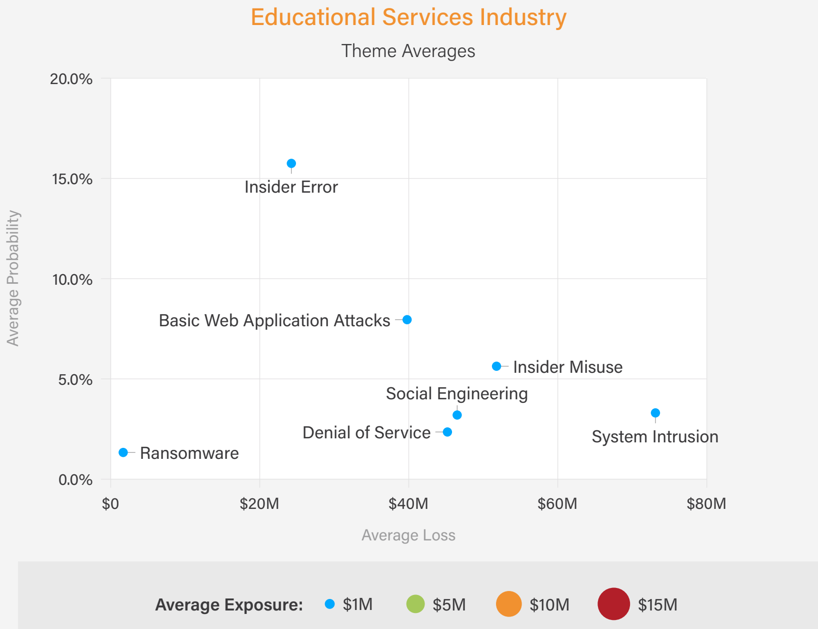
RiskLens Fast Facts on Cyber Risk in the Accommodations Industry

Educational Services

This industry includes schools, colleges, universities, and training centers, privately or publicly owned.

Theme	Loss*	Probability	Exposure
Basic Web Application Attacks	$39.9M	7.8%	$4.2M
Insider Error	$23.5M	15.2%	$3.7M
System Intrusion	$73.2M	3.8%	$3.6M
Insider Misuse	$51.9M	5.7%	$2.9M
Social Engineering	$46.9M	3.7%	$2.4M
Denial of Service	$44.5M	2.9%	$1.4M
Ransomware	$1.3M	1.9%	$28.9K

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



RiskLens Industry Benchmark simulation study averages. Representative US firm with 1,000 employees and $1B Revenue.

Analysis

Isn't ransomware especially an issue for schools? Indeed, CISA and the FBI issued a **joint alert** September 6, 2022, saying, "the education sector, especially kindergarten through twelfth grade (K-12) institutions, have been a frequent target of ransomware attacks. Impacts from these attacks have ranged from restricted access to networks and data, delayed exams, canceled school days, and unauthorized access to and theft of personal information regarding students and staff." Single-event losses tend to be low compared to other industries (K-12 ransomware demands — if paid — are often under USD $100,000 and other costs mostly go to upgrading security); however, school budgets are tight, and the impact of cyber events can be disproportionately large. Hence, the valid concerns around this trend. However, these events often do not register in enterprise industry-level input data and so do not loom large in our sampling. Fortunately, recent experience suggests that K-12 ransomware is on the decline since COVID-19-prompted a peak in 2020.

Headlines

Hackers Release Data after LAUSD Refuses to Pay Ransom

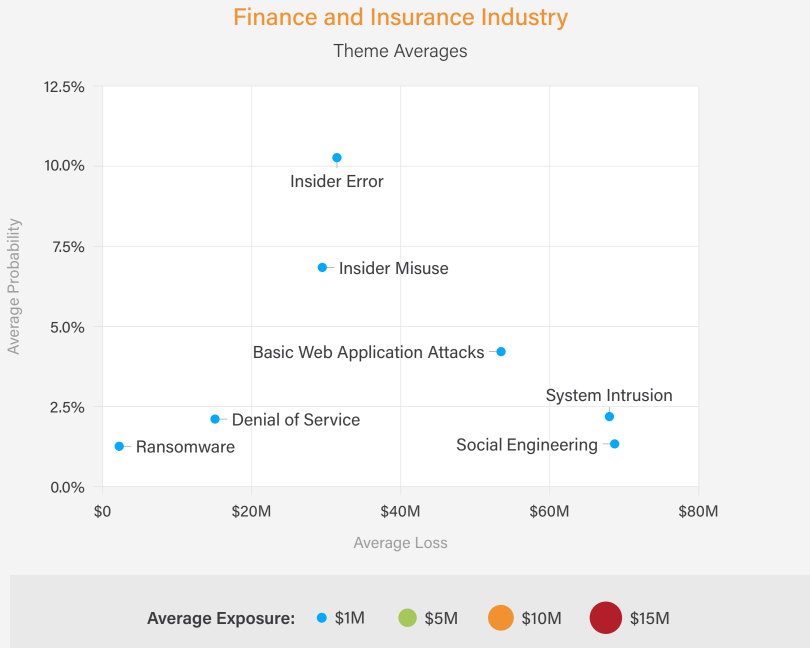
Ransomware Attack and COVID Woes Force this 150-Year-Old College to Shut Down

Finance and Insurance

This industry includes banks, insurers, lenders, investment companies and others involved in financial transactions.

Theme	Loss*	Probability	Exposure
Insider Error	$38.7M	10.4%	$4.5M
Basic Web Application Attacks	$58.7M	4.4%	$3.6M
Insider Misuse	$32.6M	7.0%	$2.4M
System Intrusion	$66.2M	2.1%	$1.9M
Social Engineering	$67.7M	1.6%	$1.7M
Denial of Service	$18.4M	2.1%	$399.9K
Ransomware	$1.1M	1.1%	$13.6K

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



RiskLens Industry Benchmark simulation study averages. Representative US firm with 1,000 employees and $1B Revenue.

Analysis

In a sign of the long tail that a major data breach can generate, it was only this year that lawsuits were settled in the notorious **Equifax data breach** that exposed the personal information of approximately 147 million people. Also in 2022, financial regulators began to lean in more heavily on security practices in finance: the Federal Deposit Insurance Corp., Federal Reserve Board, Securities and Exchange Commission and several other watchdogs either implemented or announced tighter scrutiny of security practices and faster reporting of breaches (Equifax took six weeks to notify the public). According to our research, insider error remains the most likely risk theme in this industry – a failure to patch opened the door to the Equifax hackers.

Headlines

Federal Agencies Announce a New 36-Hour Cybersecurity Incident Rule Reporting Requirement

Block Confirms Cash App Breach after Former Employee Accessed US Customer Data

Learn More

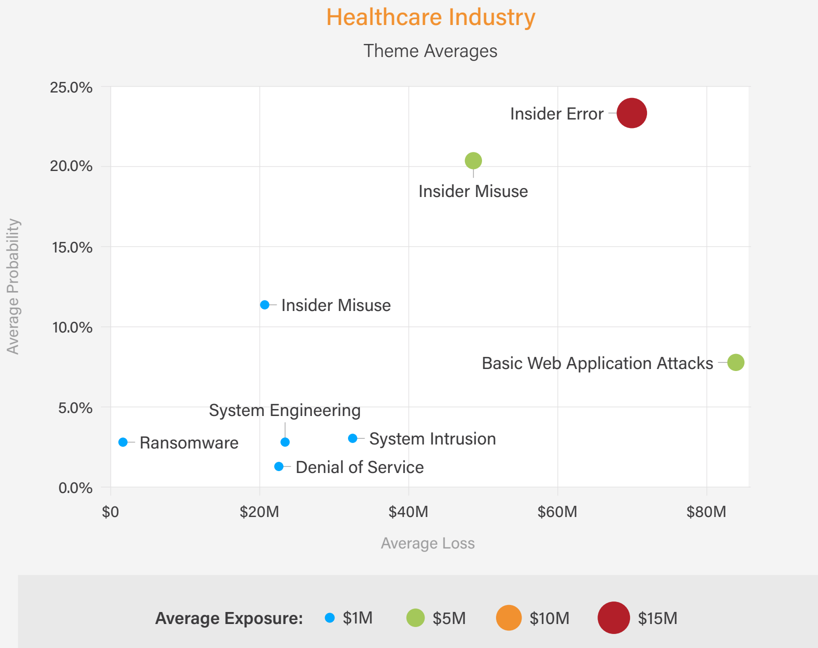
RiskLens Fast Facts on Cyber Risk in the Financial Industry

Healthcare

This industry includes hospitals and outpatient treatment facilities, doctor, and dentist practices.

Theme	Loss*	Probability	Exposure
Insider Error	$69.9M	24.2%	$17.8M
Insider Misuse	$48.5M	20.2%	$9.5M
Basic Web Application Attacks	$82.7M	7.3%	$8M
System Intrusion	$34M	3.8%	$1.7M
Social Engineering	$24.9M	3.0%	$1M
Denial of Service	$23.2M	1.7%	$415.6K
Ransomware	$674.7K	3.1%	$22.5K

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



RiskLens Industry Benchmark simulation study averages. Representative US firm with 1,000 employees and $1B Revenue.

Analysis

It's high stakes in the cyber risk landscape for healthcare providers and payers, with sensitive data (sometimes in the hands of third-party vendors) and patient care at risk, all under the oversight of the U.S. federal government's HHS Office of Civil Rights (OCR) watching – and fining – for violations of HIPAA. Insiders, malicious or not, are the most probable threat actors in this industry – one industry study found that the typical healthcare insider has access to about 20 percent of the organization's records. Consolidation in the healthcare industry, leading to shared IT systems, can magnify the effect of a ransomware attack, as CommonSpirit, the second-largest U.S. hospital chain found this year, with appointments canceled around the country for weeks.

Headlines

CommonSpirit Still Working to Restore EHR Systems after Ransomware Attack Confirmed

Dental Care Alliance Settles Class Action Data Breach Lawsuit for $3 Million

Learn More

RiskLens Fast Facts on Cyber Risk in the Healthcare Industry

Information

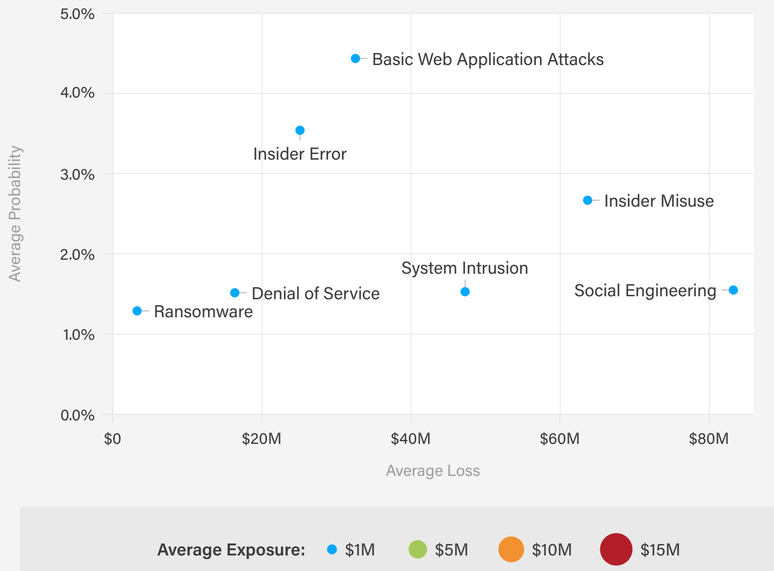
This industry is a broad category covering producers and distributors of information and cultural products, including news, movie/video, website, and music production, but also telecommunications, IT infrastructure, and data processing.

Theme	Loss*	Probability	Exposure
Basic Web Application Attacks	$34.8M	4.4%	$2.1M
Social Engineering	$81.4M	1.5%	$1.8M
Insider Misuse	$63.3M	2.4%	$1.7M
Insider Error	$24.7M	3.5%	$1M
System Intrusion	$47.8M	1.5%	$963.4K
Denial of Service	$19.6M	1.3%	$262.5K
Ransomware	$4.4M	1.2%	$55.9K

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

Information Industry

Theme Averages



RiskLens Industry Benchmark simulation study averages. Representative US firm with 1,000 employees and $1B Revenue.

Analysis

With large customer bases, these organizations are at risk for high costs from lawsuits and other secondary responses. On September 22, Optus, the second-largest wireless carrier in Australia, announced a massive data breach compromising PII for 10 percent of the country's population. According to news reports, the attackers employed several of the attacks that top our risk categories for this industry: Employee error left a web-facing API open, leading to a system intrusion.

Headlines

[Optus Data Breach: Everything We Know So Far about What Happened]

[Lapsus$ Hackers Targeted T-Mobile Source Code in Latest Data Breach]

Learn More

[RiskLens Fast Facts on Cyber Risk in the Telecommunications Industry]

Manufacturing

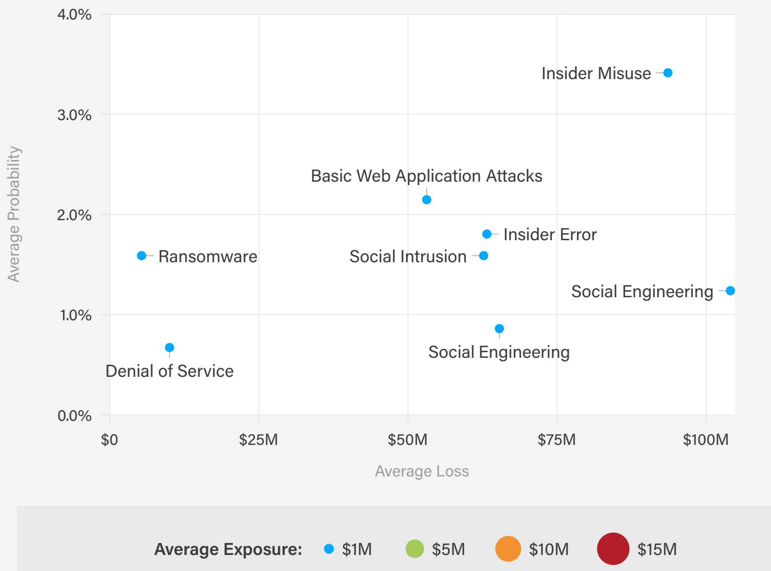
This industry includes plants, factories, or mills that produce or assemble goods for use or consumption.

Theme	Loss*	Probability	Exposure
Insider Misuse	$90.4M	3.4%	$3M
Basic Web Application Attacks	$51.8M	2.1%	$1.5M
System Intrusion	$58.4M	1.6%	$1.3M
Insider Error	$58.6M	1.8%	$1.2M
Social Engineering	$60.5M	0.9%	$832.7K
Ransomware	$7.9M	1.6%	$140.7K
Denial of Service	$14.8M	0.7%	$115.4K

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

Manufacturing Industry

Theme Averages



RiskLens Industry Benchmark simulation study averages. Representative US firm with 1,000 employees and $1B Revenue.

Analysis

Attackers formerly hit manufacturers just for IP theft or other espionage. Now, ransomware is a motive, as attackers have discovered how expensive a production shutdown can be for their victims – an effect that can be magnified if it spreads through supplier networks to multiple companies. Toyota shut down about a third of its production in February after a parts supplier was apparently ransomed; around the same time, its major tire supplier, Bridgestone, also shut plants after a separate attack. Concern grew in 2022 over the probability of attacks directly on OT/ICS systems; CISA and the NSA issued a **joint advisory** outlining TTPs.

Headlines

Bridgestone Hit as Ransomware Torches Toyota Supply Chain

Nvidia Says Its 'Proprietary Information' Is Being Leaked by Hackers

Learn More

RiskLens Fast Facts on Cyber Risk in Manufacturing

Professional Services

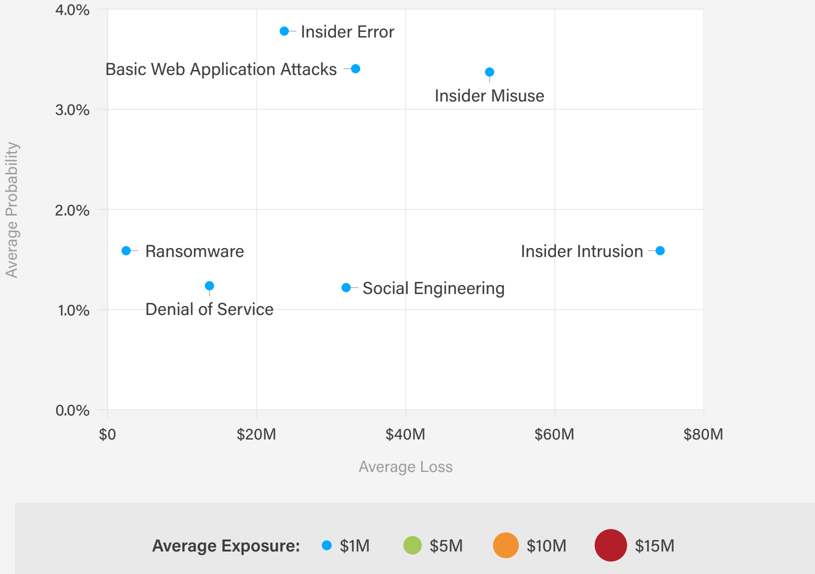
This industry includes lawyers, accountants, architects, engineers, IT consultants, and other technical experts.

Theme	Loss*	Probability	Exposure
Insider Misuse	$59.1M	3.2%	$1.9M
System Intrusion	$75.4M	1.6%	$1.6M
Basic Web Application Attacks	$34.3M	3.4%	$1.6M
Insider Error	$21.3M	3.9%	$870.8K
Social Engineering	$35.4M	1.2%	$641.1K
Denial of Service	$15.4M	1.3%	$212.7K
Ransomware	$2M	1.6%	$32.6K

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

Professional Industry

Theme Averages



RiskLens Industry Benchmark simulation study averages. Representative US firm with 1,000 employees and $1B Revenue.

Analysis

"The threats to the security of data in computers, networks, and cloud services used by attorneys and law firms appear to be at an all-time high," said the American Bar Association's ***2021 Legal Technology Survey Report***. Twenty-five percent of reporting firms said they had at some time experienced a data breach, though only 7 percent said sensitive information was exfiltrated. A data breach in legal, accounting, engineering or other technical firms could reveal the most sensitive information about client business affairs or IP, and a malicious or non-malicious insider can easily be the cause with a forwarded email.

Headlines

Law Firm Bricker & Eckler: Data Breach $1.9M Class Action Settlement

Accounting Firm Bansley & Kiener Data Breach $900K Class Action Settlement

Learn More

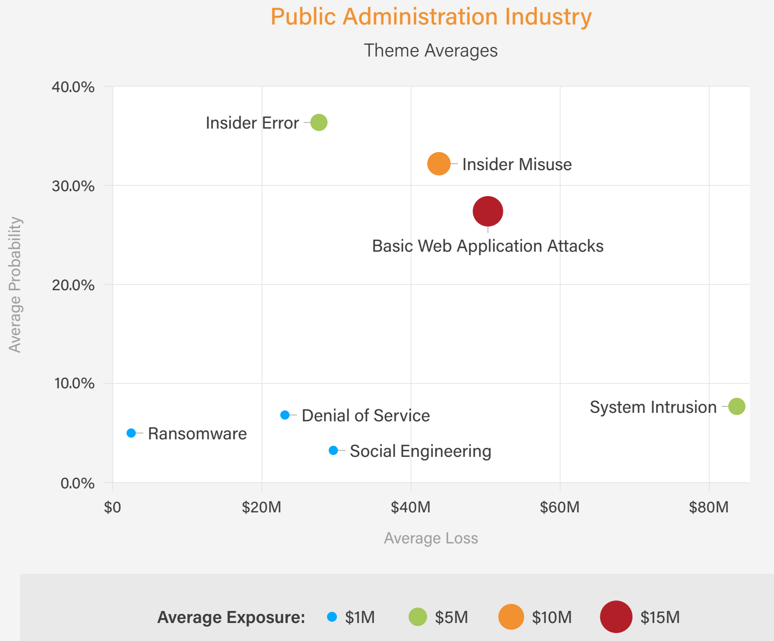
RiskLens Fast Facts on Cyber Risk for Attorneys, Accountants and Other Professionals

Public Administration

This industry includes state and local government agencies.

Theme	Loss*	Probability	Exposure
Basic Web Application Attacks	$50.6M	27.7%	$18.3M
Insider Misuse	$41.6M	31.9%	$13.7M
Insider Error	$24.3M	37.6%	$9.8M
System Intrusion	$82.9M	7.1%	$8.2M
Social Engineering	$30.5M	4.3%	$2.1M
Denial of Service	$24.4M	5.5%	$1.4M
Ransomware	$1.2M	5.0%	$65.4K

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



RiskLens Industry Benchmark simulation study averages. Representative US firm with 1,000 employees and $1B Revenue.

Analysis

Public Administration, particularly local governments in the U.S., are the least well-protected among industry categories, often due to budget constraints. They are also among the most likely to be targeted by cyber attackers and in recent years have been heavily hit with ransom and encryption attacks causing lengthy disruptions of vital services and revenue sources, such as payments for parking tickets or construction permits. Still, in terms of frequency of incidents, governments are far more prone to human errors, such as misconfigurations of cloud databases, leading to service interruption or data breaches. Of course, nothing at the local government level touches the reach of a federal data breach – seven years later, the Office of Personnel Management has finally settled with victims of a massive PII theft attributed to China.

Headlines

A Judge Has Finalized the $63M OPM Hack Settlement. Feds Now Have Two Months to Sign Up for Damages

Cyberattacks Hit Multiple Colorado Communities this Year. The Latest State Government Attack Shows Why Experts Are Worried

Learn More

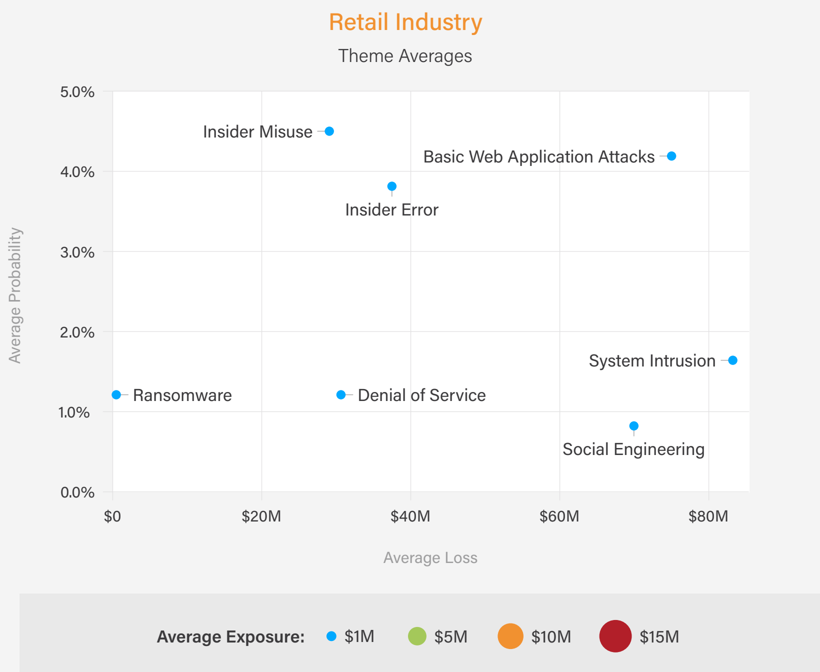
RiskLens Fast Facts on Cyber Risk for Local Governments

Retail

This industry includes sellers of merchandise via brick-and-mortar or online stores.

Theme	Loss*	Probability	Exposure
Basic Web Application Attacks	$77.6M	4.1%	$4.3M
Insider Error	$39.2M	3.9%	$1.7M
System Intrusion	$81.1M	1.5%	$1.7M
Insider Misuse	$29.5M	4.5%	$1.3M
Social Engineering	$70.3M	0.9%	$927.9K
Denial of Service	$31.8M	1.1%	$384.7K
Ransomware	$303.9K	1.1%	$3.7K

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



RiskLens Industry Benchmark simulation study averages. Representative US firm with 1,000 employees and $1B Revenue.

Analysis

With a heavy reliance on online sales, this industry presents a large attack surface and a relatively high probability of web application attack, opening the way for system intrusion to launch ransomware or steal credit card data. In 2022, the Wawa chain had to settle with attorney general's from eight states for $8 million for a credit card breach – the AGs accused Wawa of failing to meet the PCI DSS standard for credit card security. But as this **RiskLens case study** shows, PCI DSS compliance can be prohibitively costly without applying a quantitative risk analysis.

Headlines

Wawa to Pay $8 million in Data Breach Settlement with State AGs

Inside the Turmoil at Sobeys-owned Stores after Ransomware Attack

Learn More

RiskLens Fast Facts on Cyber Risk in the Retail Industry

FAIR Risk Analysis Shows CISO How to Save Millions Responding to PCI Audit

Top Industries by Risk Theme

Just as a view of the top risk themes within a given industry is valuable to help those industries understand where their top sources of loss may be concentrated, an assessment of the top industries within a given risk theme is likewise critical to understanding which industries are most likely to experience loss due to a given threat.

The following graphs illustrate the industries with the greatest potential loss exposure to seven of the top risk themes.

Basic Web Application Attack

This threat involves compromise of a web application via brute force or code exploitation to create business interruption or data breach, or possibly gain a foothold to target critical assets.

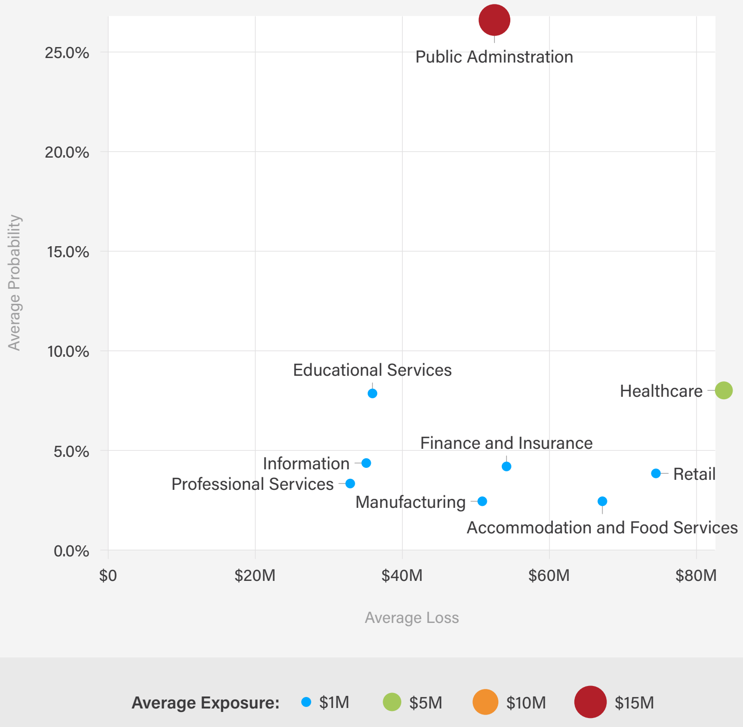
Analysis

A web application attack is one of the simplest and most direct forms of attack, but should not be underestimated. Basic web application attacks (BWAA) have been steadily increasing in recent years, particularly for government and healthcare targets. Stolen credentials are the most common way in for attackers, so multi-factor authentication and password management controls should be relatively effective responses.

Industry	Loss*	Probability	Exposure
Public Administration	$50.6M	27.7%	$18.3M
Healthcare	$82.7M	7.3%	$8M
Retail	$77.6M	4.1%	$4.3M
Educational Services	$39.9M	7.8%	$4.2M
Finance and Insurance	$58.7M	4.4%	$3.6M
Information	$34.8M	4.4%	$2.1M
Accommodation and Food Services	$65.8M	2.2%	$2M
Professional Services	$34.3M	3.4%	$1.6M
Manufacturing	$51.8M	2.1%	$1.5M

Basic Web Application Attack Theme

Industry Averages



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

RiskLens Industry Benchmark simulation study averages. Representative US firm with 1,000 employees and $1B Revenue.

Headlines

[FBI Warns of Hackers Selling Credentials for US College Networks]

[Personal Information of 68,000 DraftKings Users Exposed in Credential Stuffing Attack]

Learn More

[BWAA-ck to Basics: Insights from the 2022 Verizon DBIR on Basic Web Application Attacks]

Denial of Service

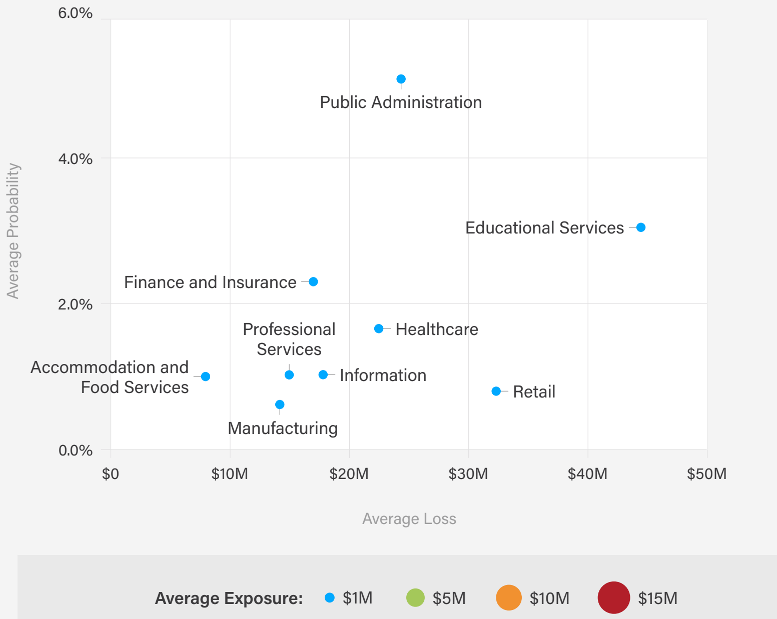
This threat involves attackers flooding the target's system with traffic or information that triggers a crash, making the system unavailable, leading to a business interruption.

Industry	Loss*	Probability	Exposure
Public Administration	$24.4M	5.5%	$1.4M
Educational Services	$44.5M	2.9%	$1.4M
Healthcare	$23.2M	1.7%	$415.6K
Finance and Insurance	$18.4M	2.1%	$399.9K
Retail	$31.8M	1.1%	$384.7K
Information	$19.6M	1.3%	$262.5K
Professional Services	$15.4M	1.3%	$212.7K
Manufacturing	$14.8M	0.7%	$115.4K
Accommodation and Food Services	$8.6M	1.0%	$89.7K

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

Denial of Service Theme

Industry Averages



RiskLens Industry Benchmark simulation study averages. Representative US firm with 1,000 employees and $1B Revenue.

Analysis

These attacks may be relatively infrequent for most industries but don't assume that attackers won't step it up. Cloudflare reported its largest intercepted DDoS attack ever originated not from home-based Internet of Things devices, the standard attack vector, but cloud service providers, indicating that virtual machines had been hijacked.

Headlines

US Airports' Sites Taken Down in DDoS Attacks by Pro-Russian Hackers

CloudFlare Says It Stopped Largest HTTPS DDoS Attack on Record

Insider Error

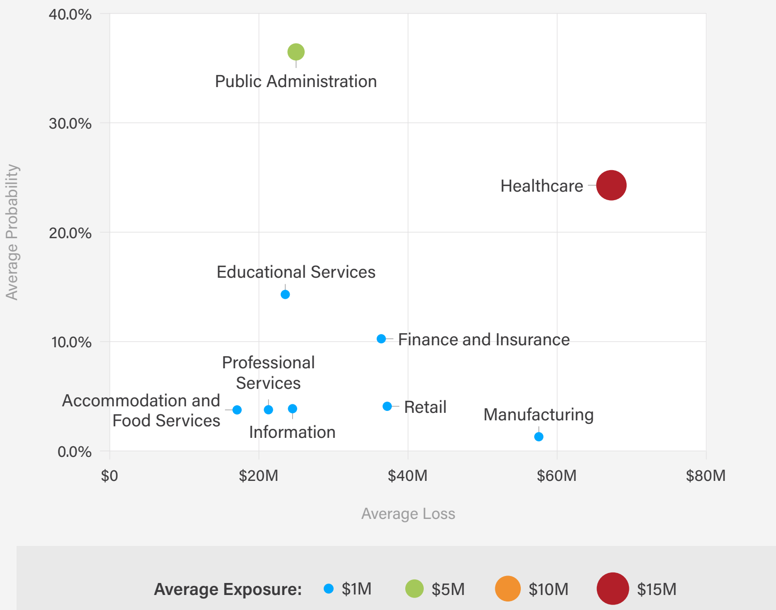
This threat involves misconfigurations, failures to renew expired certificates, improper publishing and other unintentional errors by staff members that can have damaging consequences to the bottom line.

Industry	Loss*	Probability	Exposure
Healthcare	$69.9M	24.2%	$17.8M
Public Administration	$24.3M	37.6%	$9.8M
Finance and Insurance	$38.7M	10.4%	$4.5M
Educational Services	$23.5M	15.2%	$3.7M
Retail	$39.2M	3.9%	$1.7M
Manufacturing	$58.6M	1.8%	$1.2M
Information	$24.7M	3.5%	$1M
Professional Services	$21.3M	3.9%	$870.8K
Accommodation and Food Services	$19.3M	4.0%	$834.4K

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

Insider Error Theme

Industry Averages



RiskLens Industry Benchmark simulation study averages. Representative US firm with 1,000 employees and $1B Revenue.

Analysis

Small slips with major consequences: Look at the case of a misconfigured Meta tracking pixel for advertising that leaked confidential health information from the MyChart patient-data application widely used by U.S. healthcare systems. Misconfigured security settings are among the most common fails leading to data breach from cloud storage.

Headlines

[Misconfigured Meta Pixel Exposed Healthcare Data of 1.3M Patients]

[Wegmans' $400,000 Fine for Exposed Customer Data Should Leave All Retailers on High Alert]

Learn More

[Amazon S3 Bucket Data Breaches – a FAIR™ Risk Analysis]

Insider Misuse

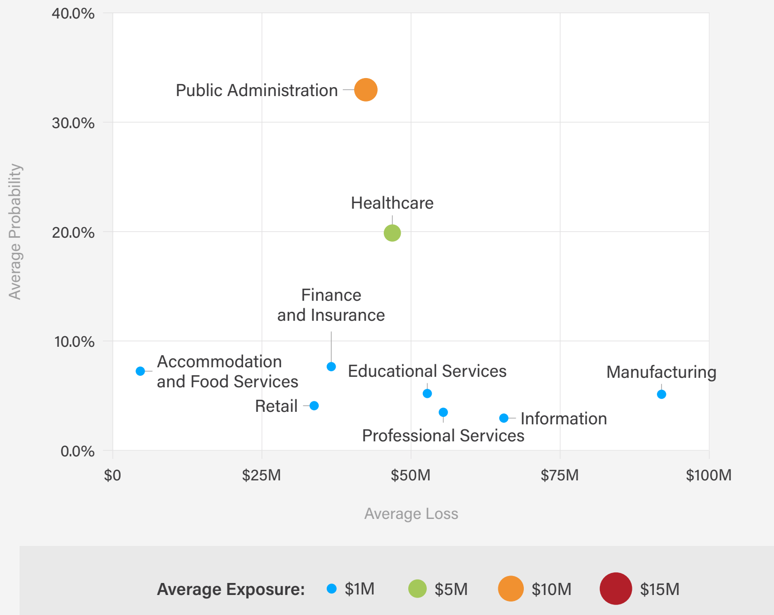
This threat involves intentional and malicious disclosure or modification of sensitive data by trusted employees, leading to significant loss to the company.

Industry	Loss*	Probability	Exposure
Public Administration	$41.6M	31.9%	$13.7M
Healthcare	$48.5M	20.2%	$9.5M
Manufacturing	$90.4M	3.4%	$3M
Educational Services	$51.9M	5.7%	$2.9M
Finance and Insurance	$32.6M	7.0%	$2.4M
Professional Services	$59.1M	3.2%	$1.9M
Information	$63.3M	2.4%	$1.7M
Retail	$29.5M	4.5%	$1.3M
Accommodation and Food Services	$6.5M	8.5%	$563K

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

Insider Misuse Theme

Industry Averages



RiskLens Industry Benchmark simulation study averages. Representative US firm with 1,000 employees and $1B Revenue.

Analysis

Government pops up to the top of the list for this risk category, a sector where many insiders have their hands on valuable data. Case in point: the California Department of Motor Vehicles (DMV) employees who took bribes from truck driving schools to **alter database records** to falsely show their students had passed the commercial driver license exam.

Headlines

IT Specialist Charged in Healthcare Cyberattack Highlights Insider Threat Risks

Yahoo Lawsuit Alleges Employee Stole Trade Secrets upon Receiving Trade Desk Job Offer

Learn More

Video: Analyze the Risk Associated with a Privileged Insider

Ransomware

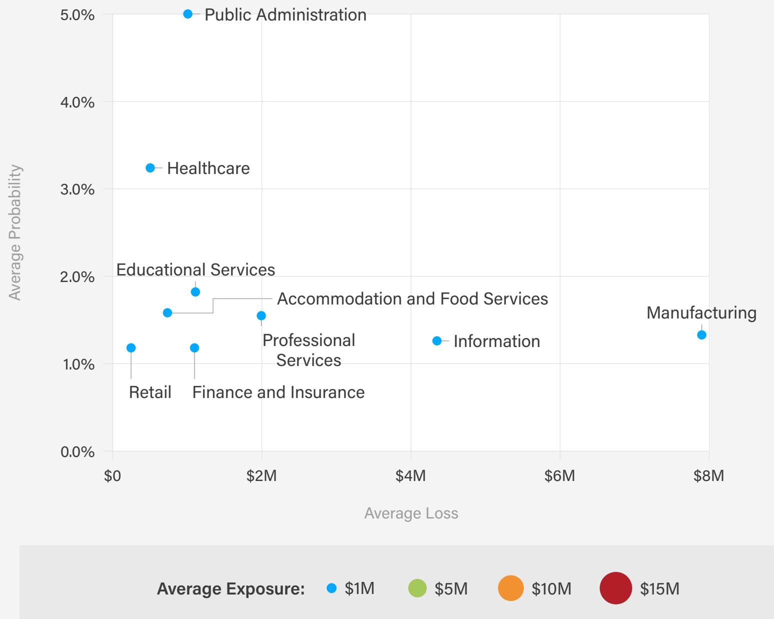
This threat involves malware-based attacks designed to pressure a company to pay a ransom by encrypting and withholding access to systems or files, and further extorting the victim by threatening to make sensitive information public.

Industry	Loss*	Probability	Exposure
Manufacturing	$7.9M	1.6%	$140.7K
Public Administration	$1.2M	5.0%	$65.4K
Information	$4.4M	1.2%	$55.9K
Professional Services	$2M	1.6%	$32.6K
Educational Services	$1.3M	1.9%	$28.9K
Healthcare	$674.7K	3.1%	$22.5K
Accommodation and Food Services	$745.9K	1.7%	$14K
Finance and Insurance	$1.1M	1.1%	$13.6K
Retail	$303.9K	1.1%	$3.7K

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

Ransomware Theme

Industry Averages



RiskLens Industry Benchmark simulation study averages. Representative US firm with 1,000 employees and $1B Revenue.

Analysis

Ransomware payments reported by banks to the U.S. Treasury under the Bank Secrecy Act **topped $1 billion in 2021**, up 188 percent in a year — and surely only a slice of actual ransomware payments made. Manufacturing companies stand to lose the most in a single incident, our data show, with the high cost of a production outage. Several of the leading semiconductor makers were hit in 2022 – raising the suspicion that the ransomware attacks were covers for espionage by nation state actors. Still, ransomware gets a disproportionate amount of news coverage and mindshare versus the number of actual events and notably the impact of those events, a good reminder of the value of collected and vetted data.

Headlines

10 Hospital Ransomware Attacks in 2022

Semiconductor Industry Faced 8 Attacks from Ransomware Groups, Extortion Gangs in 2022

Learn More

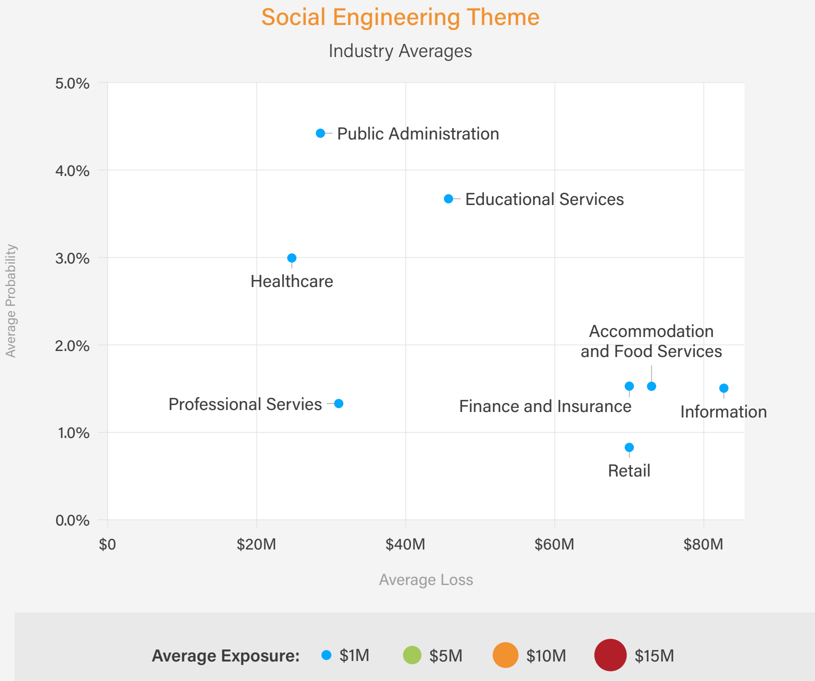
Webinar: Colonial Pipeline Ransomware – A FAIR Perspective

Social Engineering

This threat involves tricking insiders into sharing confidential or personal information or making a payment, often through an email that appears to come from a friend, a well-known brand or business partner, possibly resulting in data breach or business interruption if an attacker gains entry to the network.

Industry	Loss*	Probability	Exposure
Educational Services	$46.9M	3.7%	$2.4M
Public Administration	$30.5M	4.3%	$2.1M
Information	$81.4M	1.5%	$1.8M
Finance and Insurance	$67.7M	1.6%	$1.7M
Accommodation and Food Services	$70.3M	1.6%	$1.7M
Healthcare	$24.9M	3.0%	$1M
Retail	$70.3M	0.9%	$927.9K
Manufacturing	$60.5M	0.9%	$832.7K
Professional Services	$35.4M	1.2%	$641.1K

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



RiskLens Industry Benchmark simulation study averages. Representative US firm with 1,000 employees and $1B Revenue.

Analysis

Educational Services rank high for risk in this category, with phishing targeting students who may not be as adept at spotting email lures as corporate users. In an indication of the size of the problem, the Duke University cybersecurity team reported blocking 65 million fraudulent emails in a month – and still in September, it suffered a major phishing attack.

A new development in social engineering this year: "MFA fatigue," messages via email or text that persistently ask users to enter their credentials on a fake corporate page until the users give in. This year, Cisco, Microsoft, and Uber were hit with breaches by the Lapsus$ gang initiated by MFA requests.

Headlines

MFA Fatigue: Hackers' New Favorite Tactic in High-Profile Breaches

Hackers Breached Mailchimp to Phish Cryptocurrency Wallets

Learn More

After the Mailchimp Hack, Assess Your Risk of Social Engineering and Web Application Attack

System Intrusion

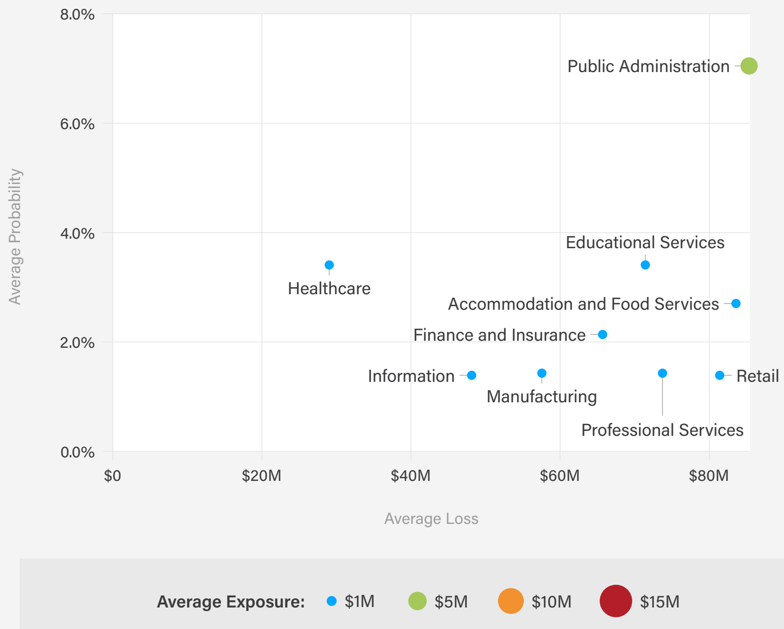
This threat involves code exploitation or brute-force password guessing, allowing a bad actor (often of the advanced persistent threat – APT – variety) a foothold in the network. This allows access to sensitive assets, resulting in a data breach, business interruption, espionage, or other perils. For the purposes of this analysis, this category does not include ransomware or social engineering-based attacks.

Industry	Loss*	Probability	Exposure
Public Administration	$82.9M	7.1%	$8.2M
Educational Services	$73.2M	3.8%	$3.6M
Accommodation and Food Services	$81.5M	2.8%	$3.1M
Finance and Insurance	$66.2M	2.1%	$1.9M
Healthcare	$34M	3.8%	$1.7M
Retail	$81.1M	1.5%	$1.7M
Professional Services	$75.4M	1.6%	$1.6M
Manufacturing	$58.4M	1.6%	$1.3M
Information	$47.8M	1.5%	$963.4K

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

System Intrusion Theme

Industry Averages



RiskLens Industry Benchmark simulation study averages. Representative US firm with 1,000 employees and $1B Revenue.

Analysis

The software supply chain has emerged as the most common and most threatening vector for these complex attacks since the SolarWinds episode and more recently the Apache Log4j vulnerability that CISA called “endemic.” Government and government contractors are particular targets for APT actors; in October, CISA issued an alert documenting a three-month infiltration at a major defense contractor starting with an intrusion in the Microsoft Exchange Server and later using Impacket, a collection of open-source tools for manipulating network protocols.

Headlines

[Fake Google Software Updates Spread New Ransomware]

[Feds Sound Alarm on Rising OT/ICS Threats From APT Groups]

Learn More

[CISA Warning on Russia-sponsored Cyber Threats – How to Prioritize Your Response]

FEATURE ARTICLE

Using Risk Quantification to Empower Decision Makers and Reduce Cyber Risk across Highly Targeted Industries

By Julian Meyrick, Managing Partner & Vice President, Security Strategy Risk & Compliance, Security Services at IBM, a RiskLens partner.

When handling security issues for an enterprise, the following questions arise from key stakeholders:

- How can we avoid becoming the next headline?
- Are we addressing key vulnerabilities and threats?
- What's the potential impact to the business if these risks are not addressed?
- How do I build a business case about the potential risks?

With the average cost of a data breach increasing 13% in the last two years to more than $4.35M, according to the 2022 IBM Cost of a Data Breach Report, quantifying security risk financially is the best way to prioritize initiatives and gain executive buy-in. Cyber risk quantification makes security strategy consumable to upper management, including board executives, to give them an understanding of security programs and initiatives that can protect their organization as well as what could happen if they fail to implement recommended controls.

Although communicating the value of risk quantification isn't always easy, here are just a few examples of how it enables better decision making to reduce cyber risk.

Securing IT and OT Environments in Manufacturing

According to the 2022 IBM X-Force Threat Intelligence Index, manufacturing became the world's most attacked industry in 2021, outpacing finance and insurance in the number of cyberattacks in that year. Increased digitization, the increasing reliance on supply chains, rapid adoption of new technology and difficulty acquiring budget for security investments leaves organizations vulnerable.

One global manufacturer needed to reduce financial exposure to threat actors and prioritize security initiatives from multiple security assessments across IT and OT environments to transform their security program and protect value.

An enterprise-level approach to risk quantification was needed to help the client understand the big picture and form a strategic view of the environment. Risk quantification helped inform the client on the value of the various security initiatives by showing how they each move the needle on reducing risk and identifying solutions that address more than one risk. This allowed the organization to manage the expense of improving security and technology across the enterprise.

Outside of prioritizing risks and identifying cost-effective solutions to reduce risk, the organization was able to focus on what was most important – keeping the manufacturing facilities operational and protected from threats.

Meeting Regulatory Requirements and Managing Risk in Government Contracting

With heightened awareness around cybersecurity threats and regulatory requirements, defense contractors must prioritize projects that will meet regulatory and government security requirements, provide internal executives with risk insights, and maintain an effective ongoing risk posture by optimizing their security spending.

This was the challenge for one of our defense contractor clients. After defining an integrated approach, the client was able to develop a sustainable risk management program, including development of a target operating model for risk management leveraging FAIR, design and documentation of a risk management governance model, operationalization of risk quantification, stakeholder management around change and adoption of the new program, and development of reporting and monitoring materials.

This enabled them to manage the regulatory requirements and internal risk to continue to effectively grow the business. Building a risk management target operating model that leverages FAIR provided the type of financial risk insights business leaders require to make effective decisions.

Reporting and Prioritizing Cyber Initiatives in Travel

With over 200 travel sites, 29 million virtual conversations, and more than 70 PB of data, one of the largest global travel providers approached us with some big challenges to solve.

They lacked a centralized ability to identify and manage risks and were unable to prioritize top risks across business units. Further, they had concerns that many risks and mitigation efforts were being treated as "one-off" situations. They were also seeking a systemic approach to manage risks that could be scaled across their brands over time.

We helped them build a sustainable risk intake, analysis, and management process that can scale with changes in the business landscape. We then leveraged risk quantification for the analysis portion of the risk management process. By quantifying the identified risks, the client could now prioritize initiatives, report risks to leadership and have meaningful conversations around risk appetite and risk acceptance. As a result of the program build, they were able to show where security was adding value by reducing risk across the organization via an ROI analysis around data encryption efforts.

Using FAIR, they raised awareness about technology, digital & security risks, influenced behaviors of employees and fostered a culture of security and compliance within their organization.

How You Can Do It Too

These are just a few examples of how risk quantification can reduce cyber risk and empower better decision making. Adopting a quantitative risk-based approach better equips organizations to focus their investments, address critical skill gaps, determine whether their control frameworks are effective, and provide for business justification of their security spend. This move results in actual risk reduction as the goal and focuses investments on the organization's top priorities.

About Us

- RiskLens helps organizations make better cybersecurity and technology investment decisions with software solutions that quantify cyber risk in financial terms.
- We are the creators of Factor Analysis of Information Risk (FAIR™), the international standard for cyber risk quantification, and the Technical Advisor to the FAIR Institute.
- The RiskLens platform is the only enterprise-scale software-as-a-service (SaaS) application for FAIR analysis.
- The RiskLens FAIR Enterprise Model (RFEM) creates flexibility to adopt FAIR and build programs, supporting companies at various maturity levels and with different business needs.
- RiskLens Pro is an easy and affordable managed service that helps organizations quickly define, assess, and communicate cyber risks in financial terms, with no in-house expertise or significant time commitment necessary.
- The RiskLens My Cyber Risk Benchmark tool provides a boardroom-ready assessment of your company's top seven risk themes in financial terms.
- With capabilities across the risk management process, and a large client base of Fortune 500 businesses, RiskLens is the only company with the expertise to help organizations navigate their most complex and challenging cybersecurity decisions. Visit us at **www.risklens.com**.

RiskLens®