

# Cyber threat environment

---

# Cyber facts

\$4.54

AVERAGE COST OF A RANSOMWARE  
ATTACK, NOT INCLUDING THE  
EXTORTION PAYMENT

707

NUMBER OF BREACHES REPORTED TO  
THE OCR IN 2022

\$10.1M

AVERAGE COST OF  
A HEALTHCARE DATA BREACH

47%

PERCENTAGE OF SURVEYED  
HEALTHCARE ORGANIZATIONS WHO  
EXPERIENCED A BREACH IN THE  
PAST 2 YEARS

12

YEARS IN A ROW HEALTHCARE HAS  
BEEN THE TOP TARGETED INDUSTRY

277

AVERAGE NUMBER OF DAYS TO  
IDENTIFY AND CONTAIN AN INCIDENT

# *Incident Costs*

1

## **COMMONSPIRIT HEALTH**

Month-long outage and the disclosure of 623,700 patient records due to a ransomware attack resulted in a **>\$150M loss** to date with costs ongoing

2

## **OKLAHOMA STATE UNIVERSITY**

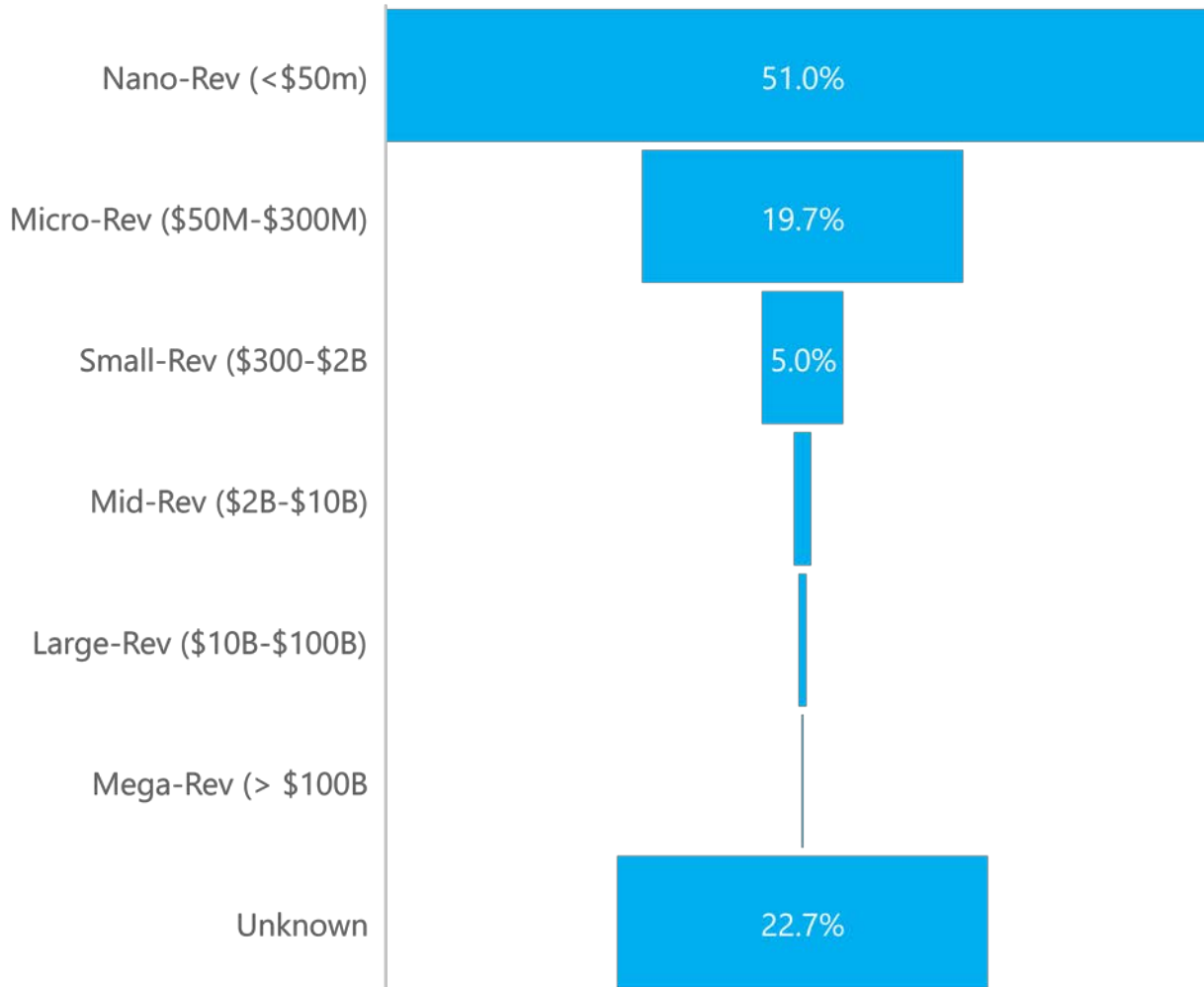
**Paid \$875,000** to the federal government in 2022 to settle alleged violations of HIPAA privacy rules for a 2018 data breach that affected 279,865 patients

3

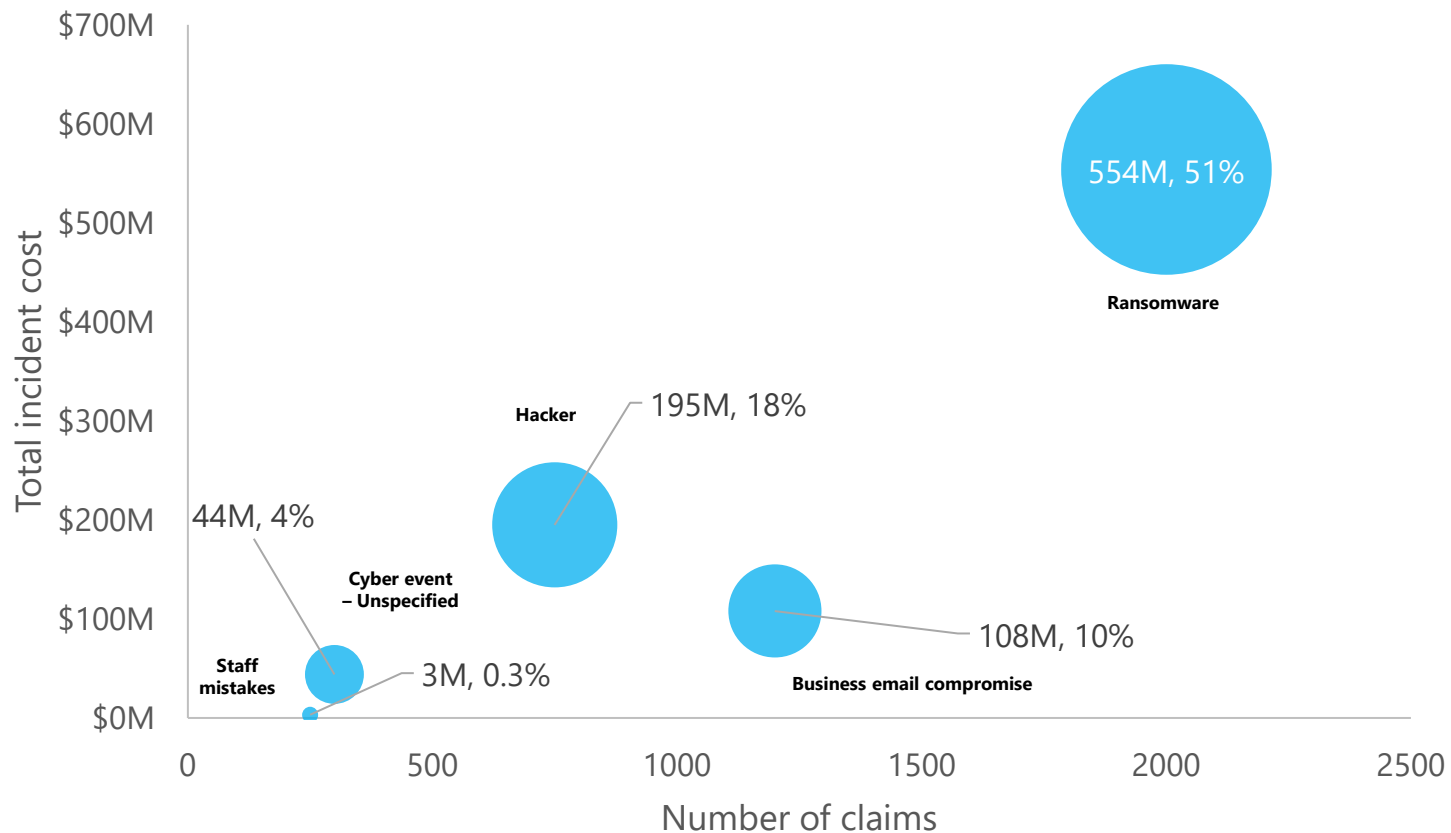
## **ST. JOSEPH HEALTH SYSTEM**

A class action **settlement of \$7.5M** was reached for the 2011 and 2012 data breach of 31,000 patient records, of which the defendant agreed to spend approximately \$17 million to improve their cyber-security






## Percentage of claims by revenue size



## Top causes of loss – SMEs



# *Common cyberattacks*

 <b>MALWARE</b>	 <b>SOCIAL ENGINEERING</b>	 <b>MAN-IN-THE MIDDLE</b>	 <b>DENIAL OF SERVICE</b>	 <b>SQL INJECTION</b>
Spyware Ransomware Worms Trojan horses	Phishing Spear phishing Whaling Vishing Baiting Pretexting Tailgating/ piggybacking Quid pro quo	Email hijacking Wi-Fi and browser eavesdropping IP and DNS spoofing	Denial-of-service attack Distributed denial of service	Database attack In-band Blind Out-of-band

# *Regulatory landscape*

**International, federal, state and local regulators continue to expand privacy protections around the globe. Significant regulatory activity includes:**

- European Union's General Data Protection Regulation
- China's Personal Information Protection Law and Data Security Law
- U.S. Treasury's Office of Foreign Assets control's updated advisory on ransomware payments
- State legislation, including:
  - California Consumer Privacy Act and California Privacy Rights Act
  - Virginia Consumer Data Protection Act
  - Colorado Privacy Act
  - Utah Consumer Privacy Act

**Some laws have been around for some time but have recently seen an increase in litigation and/or enforcement activity.**

**Examples include:**

- Health Information Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Illinois Biometric Information Privacy Act (BIPA)
- Children's Online Privacy Protection Act (COPPA)
- Fair and Accurate Credit Transactions Act
- Regulation S-P
- Video Privacy Protection Act (VPPA)
- Federal and state wiretap laws

ENFORCEMENT agencies are entrusted to administer, investigate and impose consequences on organizations failing to comply with various privacy protections. Examples of enforcement agencies include:

- Data protection authorities
- U.S. Department of Health and Human Services, Office of Civil Rights
- Securities and Exchange Commission
- Federal Trade Commission
- State attorneys general

Liability for failure to comply with privacy protections can subject an organization to costly and lengthy litigation by third parties and/or proceedings initiated by the regulatory body claiming violations of various laws.

# Cyber insurance market conditions

---



# *Cyber Liability Market Update*

## **Market Overview**

- While the cyber market continues to be challenging, there are signs of moderation. Premiums are still rising given the ongoing claims environment, but there is a substantial increase in capacity, which is driving competition and more favorable outcomes.
- Concerns over systemic risk and website tracking are the forefront of insurers' minds.
- The scrutiny around controls continues to tighten and focus is becoming increasingly granular, bringing the implementation of controls into the limelight. Where previously the implementation of Multi Factor Authentication (MFA) for remote access may have sated underwriters' requirements, further controls are being required for insurability, much less broad and robust coverage.

## **Challenges**

- Renewals are taking much longer to complete as insurers continue to re-evaluate their books of business due to the ongoing and changing threat landscape.
- Insurer remediation efforts include invasive underwriting and minimum security control requirements, which continue to change based on new threats.
- Insureds with robust, best-in-class infosec controls are seeing flat to slight rate decreases, while those with good controls are experiencing 0%-20% rate increases.
- Ransomware coverage limitations are applied in the absence of adequate security controls – sublimits, coinsurance, exclusions etc.
- Strong cyber security controls continue to be a minimum for insurability.

# *Trends*

## Claims frequency is **decreasing**

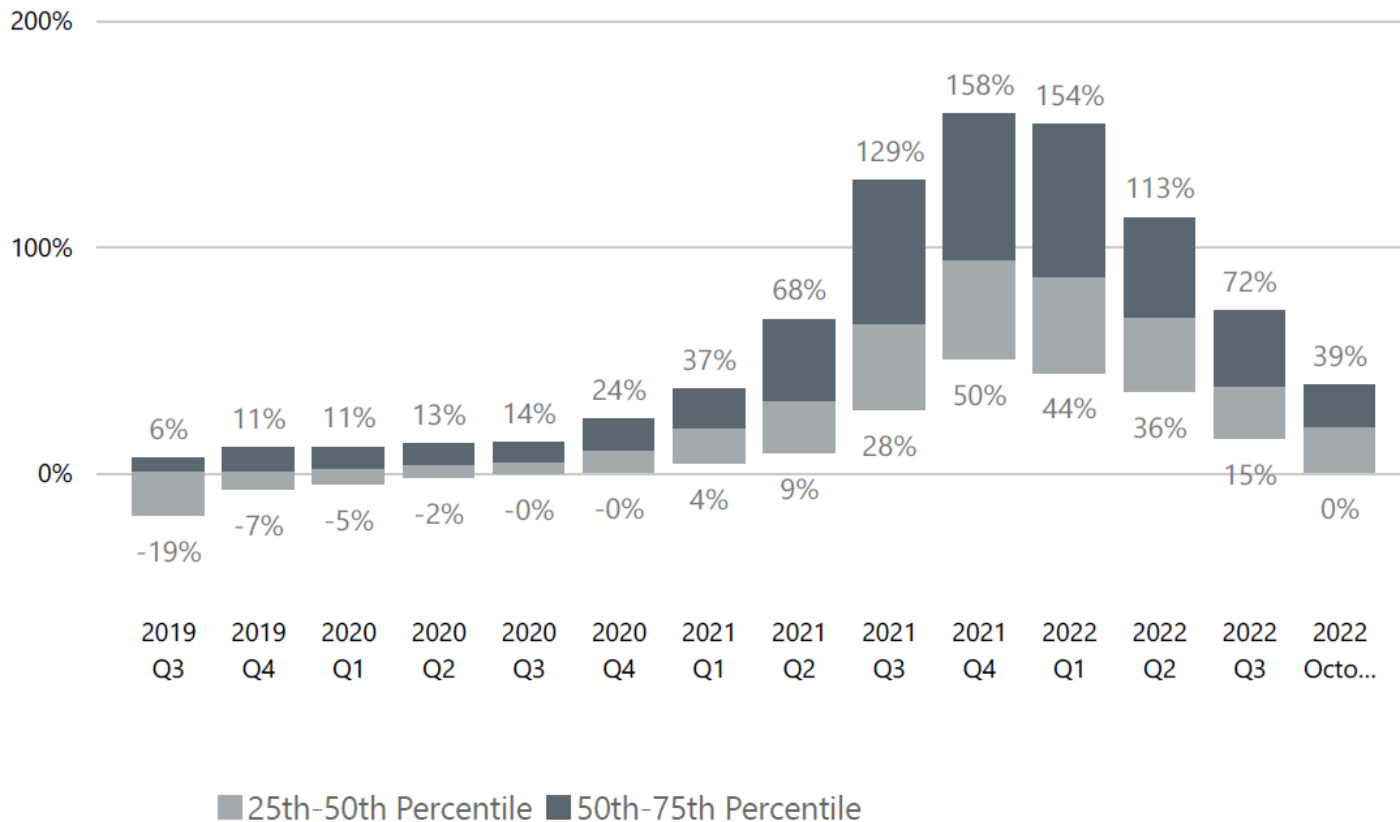
1. Threat actors are preoccupied by the conflict between Russia and Ukraine
2. Minimum security control requirements have had measurable impacts
3. Concerns over the ban of extortion payments and the FBI target of ransomware threat groups have threatened Ransomware as Service models

## Claims severity is **increasing**

1. Threat actors are engaging in targeted attacks
2. Substantial time is taken to scope victims' networks to identify crown jewels to exploit prior to deploying ransomware
3. Phishing and vishing attacks are becoming increasingly more sophisticated
4. Security best practices like MFA are being bypassed

# Lockton Cyber Renewal Insights – Total Price Change

## TOTAL PRICE CHANGE BY QUARTER



Quarter	Median	Average	Count
2019 Q3	0.0%	-2.3%	210
2019 Q4	0.0%	3.4%	168
2020 Q1	1.9%	17.7%	216
2020 Q2	3.8%	17.0%	280
2020 Q3	4.7%	11.0%	323
2020 Q4	10.1%	20.5%	320
2021 Q1	20.0%	24.5%	307
2021 Q2	31.7%	48.4%	364
2021 Q3	66.1%	101.0%	383
2021 Q4	94.0%	125.3%	411
2022 Q1	86.9%	124.2%	357
2022 Q2	68.6%	101.1%	389
2022 Q3	38.3%	47.2%	447
2022 Oct...	20.1%	23.6%	101

Percentages displayed represent the 25th and 75th percentiles.

# Critical cybersecurity controls

---

# *Security control requirements and best practices*



Identity access management



Multifactor authentication



Backup policies



Cybersecurity awareness and training



Endpoint detection and response tools



Incident response and business continuity plan

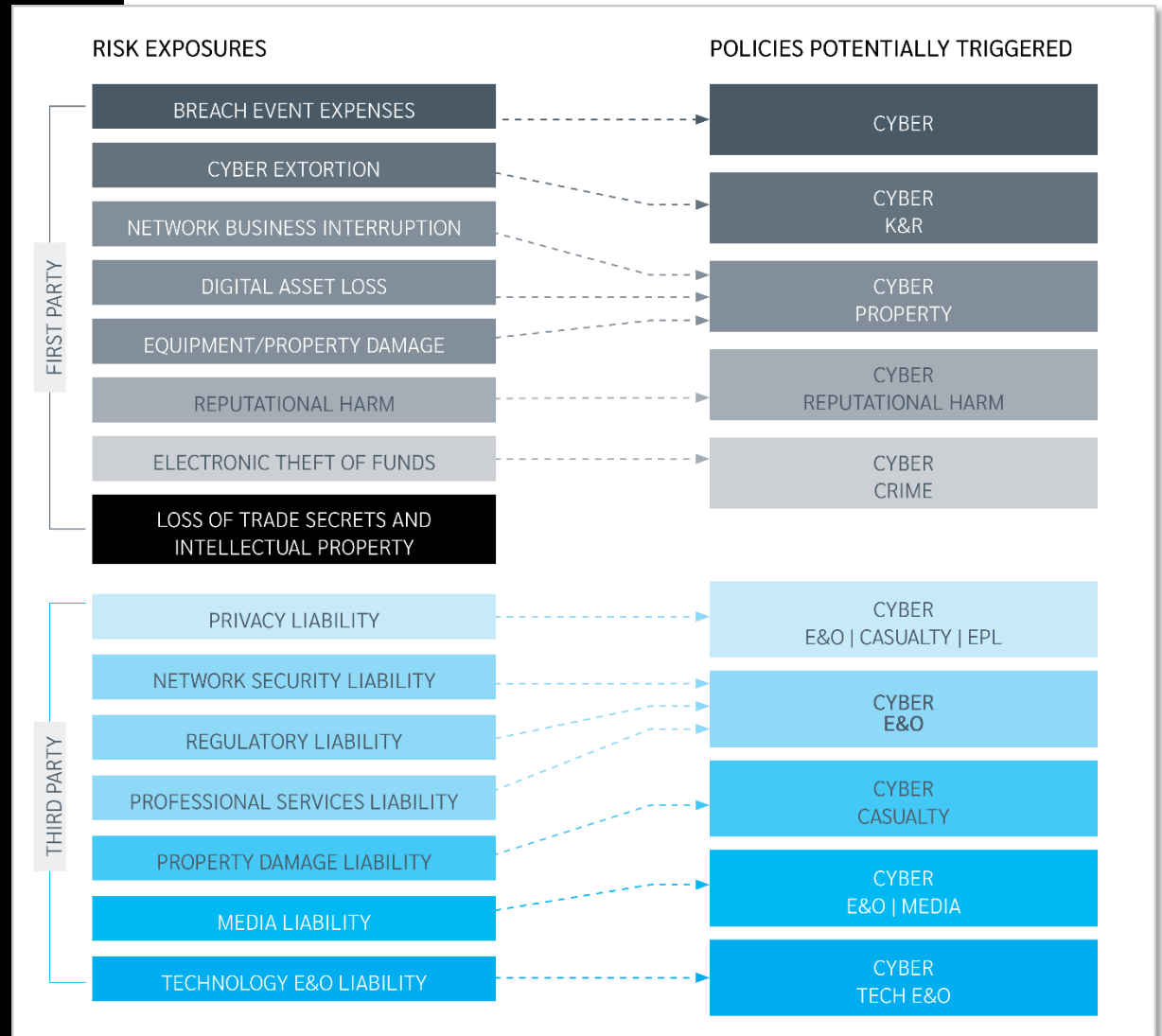


Zero trust methodology

# Cyber liability coverage

---

# Insurance & risk transfer



# *Claims best practices*



## **TIMELY INSURER NOTIFICATION**

Insurers will routinely not pay for expenses incurred prior to receiving notice.



## **COLLABORATE, COOPERATE & COMMUNICATE**

Obtain insurers' consent on a proposed course of action, retention of vendors, rates, and settlement offers. Select appropriate vendors in conjunction with counsel, who should lead the vendor retention process.



## **DESIGNATE KEY DECISION-MAKERS**

One person within the organization should be responsible for communicating with the insurer. For large losses, retain forensic accounts who know how to prepare a proof of loss and what information to include to ensure timely payment.



## **ENGAGE YOUR BROKER**

Claims professionals can provide guidance and support throughout the cyber claims process.