



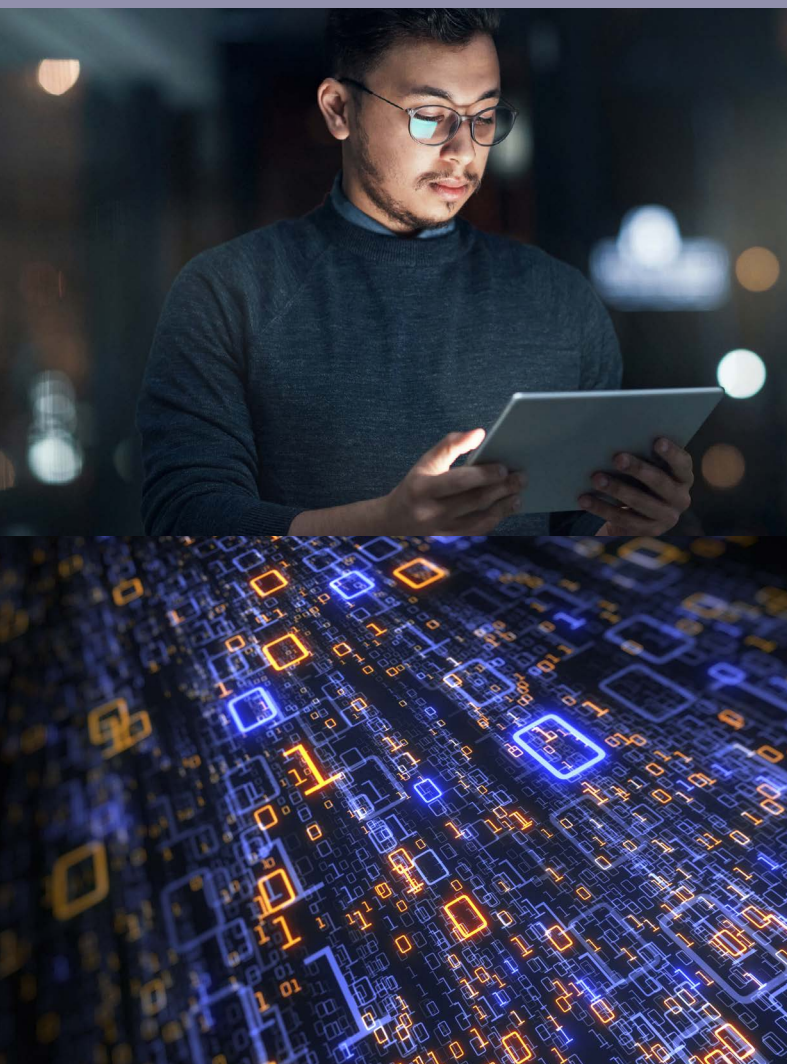
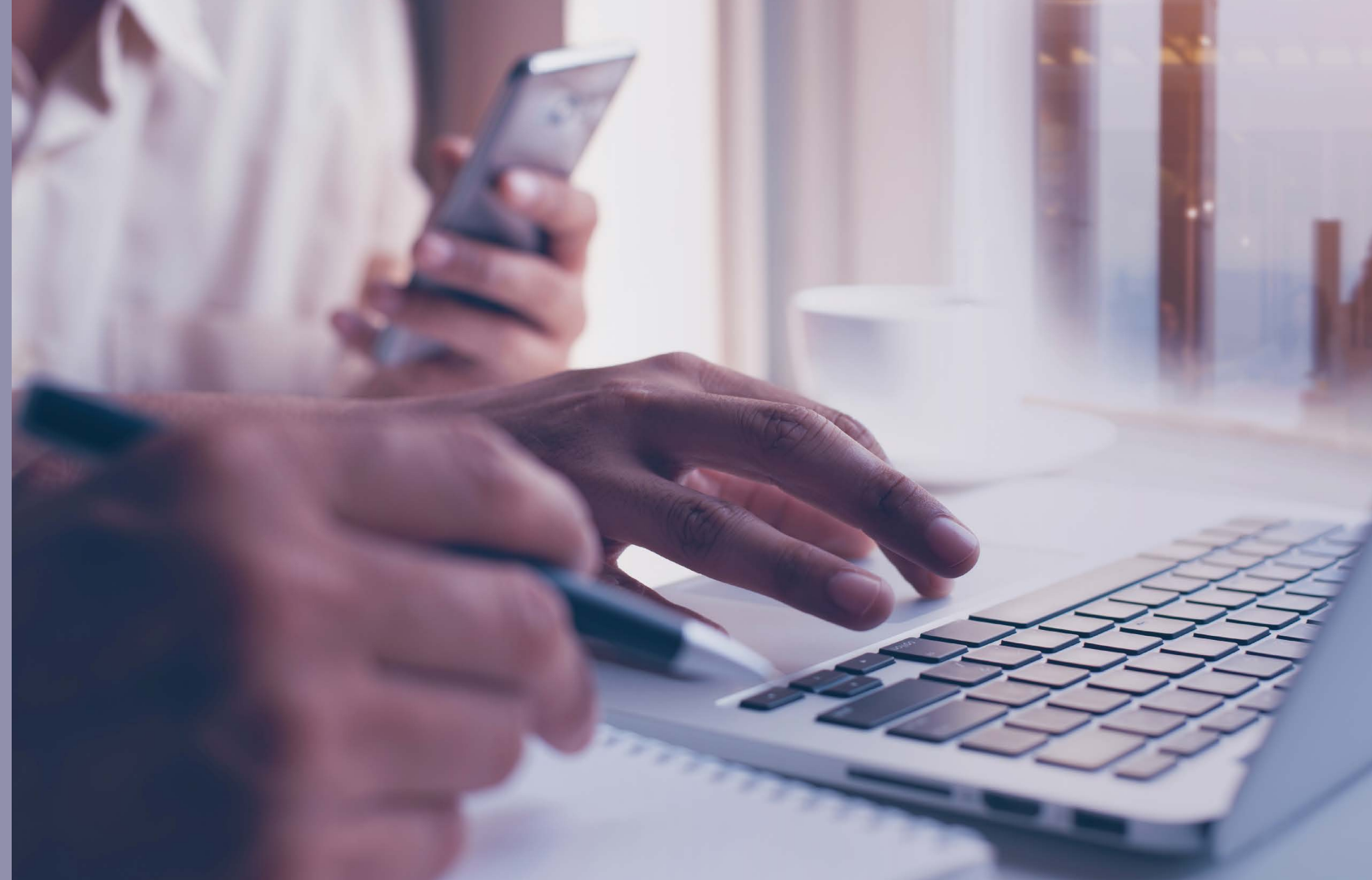
XL Insurance

Cyber claims

Real-life AXA XL claims scenarios



The liabilities associated with cyber exposures can devastate your business. The global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years.*



Throughout 2023 and 2024, the AXA XL Cyber Claims team continued to see substantial ransom demands to its clients from threat actors. As organizations have become more cyber resilient, we are seeing an increased focus on cyber extortion demands for data suppression as opposed to system encryption. We continue to see “supply chain attacks” spreading to third party companies through software or connected networks, or as contingent business interruption exposure.

Looking ahead to the cyber insurance landscape for the remainder of 2024 and into 2025, several key trends continue on the first party side: the use of social engineering to get around Multi-factor Authentication (MFA), highly targeted attacks focused on obtaining large payouts (especially in the healthcare and financial industries) and continued attempts to divert funds to fraudulent accounts through scams and compromised email accounts.

Additionally, the AXA XL Cyber Claims team saw a marked increase in 2023, and 2024, of class action filings in the US. These class actions ranged from lawsuits filed following a data breach (including for ever decreasing class sizes), as well as many lawsuits arising out of alleged unauthorized collection and use – some arising out of newer statutes like California Invasion of Privacy Act (CIPA), Biometric Information Privacy Act (BIPA) and Genetic Information Privacy Act (GIPA), as well as older statutes repurposed for current privacy conditions, like the Virtual Power Purchase Agreement (VPPA), and various state wiretap statutes.

Finally, increased regulatory scrutiny of cybersecurity and privacy related issues were of paramount importance in 2023, and 2024, with the Securities and Exchange Commission (SEC), New York State Department of Financial Services (NYDFS) and various state attorneys general, among others, all maintaining oversight over cyber related issues.

Protect your business by understanding your cyber liability exposures and how AXA XL can help you effectively manage your risk and protect your reputation. Our global claims team is comprised of seasoned Cyber and Technology claims professionals, all former practicing attorneys, who collectively have several decades of experience. We partner with you to successfully investigate and resolve your covered claims fairly and accurately. Our experience covers claims of varying complexity, and the team has handled data breaches and third party claims across multiple industries and jurisdictions.

Continue reading for real-life examples of cyber global claims our team has responded to and managed, providing clients with peace of mind.

* IBM 2023 Cost of Data Breach Report, 2024

Click on any Industry to go to those claims scenarios. Also, check out our Fast Facts infographic (page 2) and our Claims Trends infographic (page 5). Total payouts for each claim are inclusive of any applicable self-insured retentions.

- 1** Introduction
- 3** Healthcare
- 4** Financial Services
- 5** Technology
- 8** Media
Retail
Government
- 9** Food and Beverage
Commercial Goods
Professional Services
Manufacturing

Healthcare

Total payout: \$2,400,000
Coverage section: Data Breach Response and Crisis Management, Privacy and Cyber Security, Privacy Regulatory Defense, Awards and Fines
Business size: Medium

A client organization experienced a business email compromise that led to first party data breach expenses, as well as a third party class action and civil investigative demand. The impacted population was under 200,000. The matter triggered various coverages under the policy. The organization retained a data breach coach and forensic vendor. In addition, counsel was retained on behalf of the client to defend the class action and civil investigative demand. The total payment for first and third party, including settlements, was \$2.4M.

Total payout: \$122,000
Coverage section: Privacy and Cyber Security
Business size: Medium

A client organization’s rogue employee released a patient’s protected health information on social media. The client retained defense counsel and the matter triggered Privacy and Security Liability Coverage. Approximately \$122,000 was paid for defense costs and settlement, excess of the \$100,000 retention.

Financial Services

Total payout: \$377,000
Coverage section: Privacy and Cyber Security
Business size: Large

A client organization that collects genetic information was sued in multiple putative class action lawsuits for alleged violation of the Illinois Genetic Information Privacy Act (“GIPA”). We assisted the client in its defense of the lawsuit, and it successfully dismissed the consolidated lawsuit, which was affirmed on appeal. AXA XL paid approximately \$50,000 following exhaustion of the retention in defense costs.

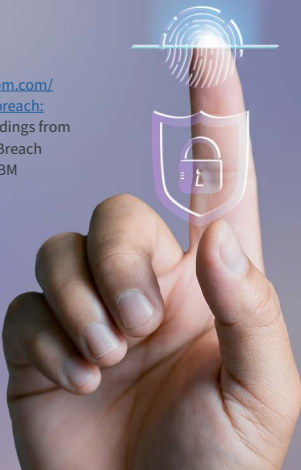
Total payout: \$4,000,000+ (ongoing - potential \$10M loss)
Coverage section: Data Breach Response and Crisis Management, Privacy Regulatory Defense, Awards and Fines, Privacy and Cyber Security
Business size: Medium

A client organization experienced a data breach whereby PII (personally identifiable information) was exposed. Notifications and credit monitoring were sent to over 100,000 potentially affected individuals. Following notification, the client was the subject of a putative class action lawsuit which was settled for approximately \$1M. There are ongoing investigations by both the New York State Department of Financial Services and the New York Attorney General with potential fines in excess of remaining policy limits.

A client organization that collects genetic information was sued in multiple putative class action lawsuits for alleged violation of the Illinois Genetic Information Privacy Act (“GIPA”).

Fast Facts

<https://www.ibm.com/security/data-breach>
Figures and findings from Cost of a Data Breach Report 2023 - IBM



277 days

per compromised record
Average time to identify and contain a data breach

54 days

Organizations with both an IR team and IR plan testing identified breaches 54 days faster than those with neither.

IR strategies and tactics have been instrumental in reducing the impact of data breaches. The most effective IR strategy for reducing the duration of a data breach was to combine formation of an IR team with testing of the IR plan.

Top 5 industries

with the most expensive data breaches

with the most expensive data breaches

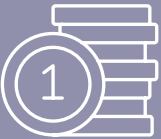
1

Healthcare



2

Financial



3

Pharmaceuticals



4

Energy



5

Industrial



Technology

Total payout: \$5,000,000
Coverage section: Data Breach Response and Crisis Management
Business size: Small

A client organization, which provides a free app, discovered unauthorized network activity with evidence of data exfiltration. After investigation, it was determined that PII (Personally Identifiable Information) of 20 million app users had been compromised, triggering notice obligations. The client was the subject to class actions, which ultimately settled for amounts well-above the \$5M policy limits.

Total payout: \$3,500,000+
Coverage section: Privacy and Cyber Security
Business size: Medium

A client organization’s former employee gained unauthorized access to a customer live camera feed. This generated claims and lawsuits from customers. Total exposure, including ongoing defense costs, is anticipated to be in excess of \$3M.

After investigation, it was determined that PII (Personally Identifiable Information) of 20 million app users had been compromised, triggering notice obligations.

Total payout: \$3,500,000
Coverage section: Privacy and Cyber Security
Business size: Large

The client is an organization that develops technology, including a tool which uses facial recognition. A class action lawsuit was filed, alleging violations of the Illinois Biometric Information Privacy Act (“BIPA”). Settlement was reached in the mid eight figures.

Total payout: \$1,720,000
Coverage section: Data Breach Response and Crisis Management, Business Interruption and Extra Expenses
Business size: Medium

A client organization suffered a ransomware attack which caused its e-commerce website to crash and go offline for several business days. The website crash prevented the sale of medical products and repair services. The organization did not pay the threat actor’s demand and instead opted to restore from backups. Additionally, approximately 1TB of data was exfiltrated in the incident. The client retained vendors to restore their network and assess the business interruption.

Claims Trends

The 4 most common initial attack vectors



16%
Phishing



11%
Cloud misconfiguration



15%
Stolen or compromised credentials



9%
Business email compromise

The costliest initial attack vectors

Malicious insider
\$4.90M

Phishing
\$4.76M

Business email compromise
\$4.67M

Stolen or compromised credentials
\$4.62M

<https://www.ibm.com/security/data-breach>; Figures and findings from Cost of a Data Breach Report 2023 - IBM



The organization conducted a preliminary internal review of its systems and identified hundreds of GBs of data transferred out its network through a firewall. We promptly connected the organization with breach counsel.



Media

Total payout: \$5,000,000

Coverage section: Media

Business size: Small

The client, an operator of an online platform, was sued for copyright infringement. Plaintiff filed suit alleging various violations, including DMCA (Digital Millennium Copyright Act) violations, copyright infringement, trademark infringement and unfair competition. Factoring in statutory damages available for copyright claims and the amount of works at issue, the potential exposure was well in excess of the \$5M policy.

Retail

Total payout: \$10,000,000

Coverage section: Cyber-Extortion and Ransomware, Business Interruption and Extra Expenses, Data Breach Response and Crisis Management, Privacy and Cyber Security

Business size: Medium

The client, a retailer with global locations, suffered a ransomware event that brought down its operations, including systems that manage inventory, pricing, shipping, etc. After evaluating options, the decision was made to pay the sizeable ransom to more quickly restore operations and mitigate business interruption loss. The incident ultimately triggered multiple first party coverages. In addition to first party loss, the client organization was the subject of multiple class action lawsuits and regulatory investigations. Ultimately, the \$10M limit of covered first party loss was paid out.

Government

Total payout: \$1,000,000+

Coverage section: Cyber-Extortion and Ransomware, Data Breach Response and Crisis Management, Data Recovery

Business size: Small

On an early Saturday morning, we received a hotline call from a client organization informing us that a few hours ago it had received an alert from its external cybersecurity vendor regarding unusual behavior observed on a server. The organization conducted a preliminary internal review of its systems and identified hundreds of GBs of data transferred out its network through a firewall. We promptly connected the organization with breach counsel. Counsel warned the organization that these were the early steps of threat actors preparing to launch a ransomware attack, and it may wish to consider turning off its network. The organization considered this step but decided to wait for a call with a federal law enforcement agency the next day for additional guidance.

The next morning, just hours after a late-night consultation call, the organization discovered encryptions of its systems by the threat actor. We assisted the organization with the engagement of multiple breach response providers for the incident response, forensic investigation and data restoration. The organization did not engage with the threat actor and did not pay a ransom. Total budgets for this response and restoration well exceeded \$1M.

Food and Beverage

Total payout: \$10,000,000
Coverage section: System Failure
Business size: Large

The client, a food company, experienced a system failure that caused outages which impacted production and sales for several weeks. The coverage for system failure was triggered. After forensic accountants reviewed the submission, the entire limit of \$10M was paid out.

Commercial Goods

Total payout: \$10,000,000
Coverage section: Business Interruption and Extra Expenses, Data Breach Response and Crisis Management
Business size: Medium

The client, a commercial goods vendor, sustained a ransomware attack. They submitted a business interruption claim as the incident impacted the client’s production, warehousing, distribution, and finance systems. AXA XL paid its limit of \$10M.

Professional Services

Total payout: \$4,200,000+
Coverage section: Data Breach Response and Crisis Management, Cyber-Extortion and Ransomware, Business Interruption and Extra Expenses, Privacy and Cyber Security, Privacy Regulatory Defense, Awards and Fines, Technology E&O
Business size: Medium

The client organization, which provides customer support services, suffered a ransomware attack which rendered its business inoperable for a week, resulting in substantial investigation, restoration and notification services. Following the incident, a class action lawsuit was filed by current and former employees of the organization, resulting in a class settlement. Additionally, customers filed suit alleging that the organization failed to provide sufficient cyber security, resulting in damages. Further, counsel was employed to respond to intensive state Attorney General investigations regarding the incident and the organization’s security policies and practices, resulting in fines.

Manufacturing

Total payout: \$5,000,000
Coverage section: Privacy and Cyber Security, Business Interruption and Extra Expenses
Business size: Large

The client, a worldwide manufacturer, was impacted by a ransomware event. As a result of the attack, factories in multiple countries were shut down for over a week. The organization did not pay the eight-figure ransom demand, and instead worked on restoration of the impacted servers. First party coverage was triggered under Privacy and Network Security and Business Interruption Loss insuring agreements. The Insured retained a forensic accountant to calculate the business interruption which ultimately exceeded AXA XL’s limit.

The client, a worldwide manufacturer, was impacted by a ransomware event. As a result of the attack, factories in multiple countries were shut down for over a week.



AXA XL

axaxl.com

@AXA_XL

The information contained herein is intended for informational purposes only. Insurance coverage in any particular case will depend upon the type of policy in effect, the terms, conditions and exclusions in any such policy, and the facts of each unique situation. No representation is made that any specific insurance coverage would apply in the circumstances outlined herein. Please refer to the individual policy forms for specific coverage details. AXA XL is a division of AXA Group providing products and services through three business groups: AXA XL Insurance, AXA XL Reinsurance and AXA XL Risk Consulting. In the US, the AXA XL insurance companies are: Catlin Insurance Company, Inc., Greenwich Insurance Company, Indian Harbor Insurance Company, XL Insurance America, Inc., XL Specialty Insurance Company and T.H.E. Insurance Company. Not all of the insurers do business in all jurisdictions nor is coverage available in all jurisdictions. Information accurate as of September 2024.

AXA, the AXA and XL logos are trademarks of AXA SA or its affiliates. © 2025