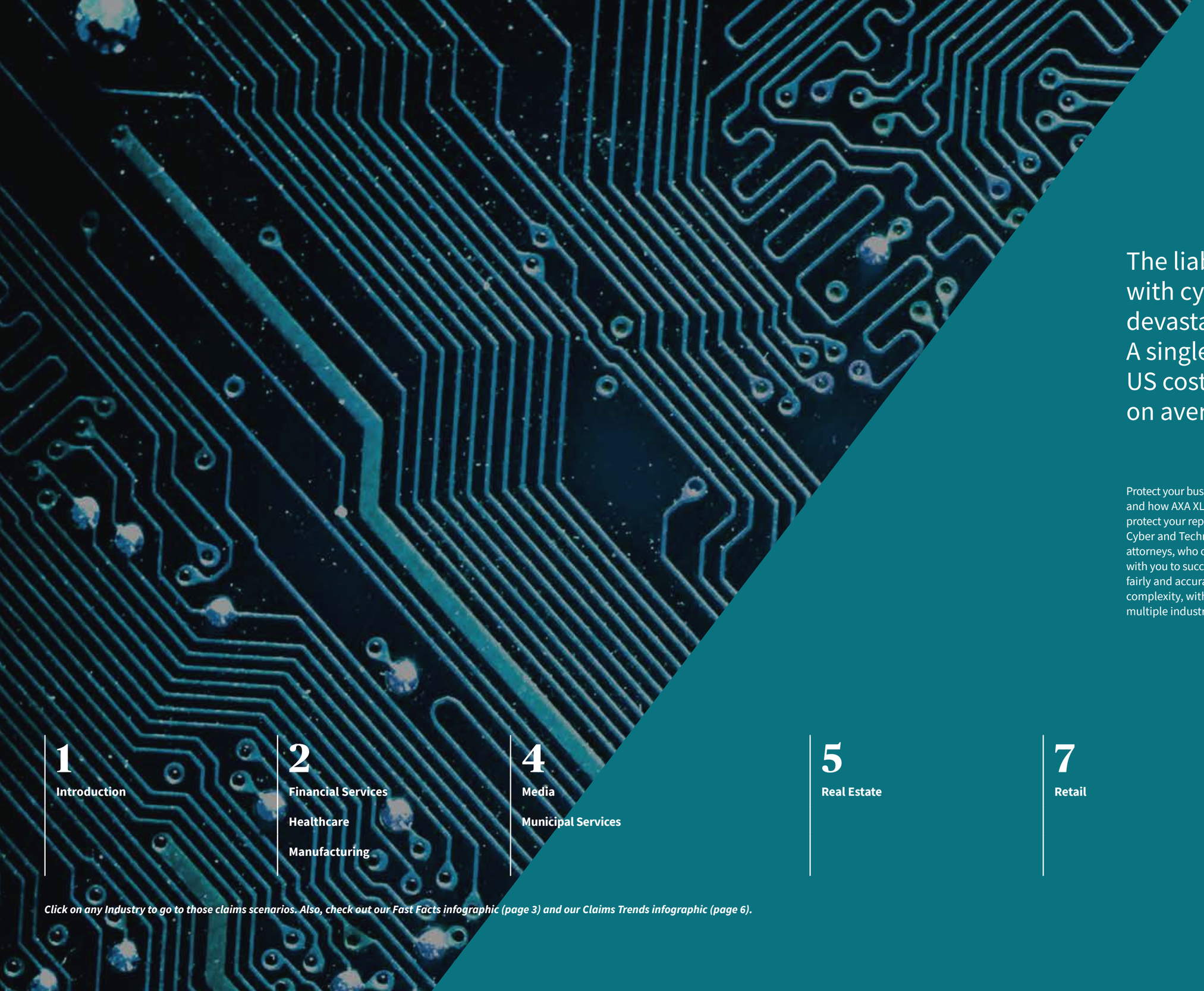
XL Insurance

Cyber Claims

Claims scenarios ripped from today's headlines



The liabilities associated with cyber exposures can devastate your business. A single cyber-attack in the US costs companies, on average, $7.91 million.

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 claims team is comprised of seasoned Cyber and Technology claims professionals, all former practicing attorneys, who collectively have 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, with the team having handled data breaches across multiple industries and jurisdictions.

Click on any Industry to go to those claims scenarios. Also, check out our Fast Facts infographic (page 3) and our Claims Trends infographic (page 6).

Industry:

Financial Services

An act of embezzlement

Type of company: Holding Company
Total Payout: $3.5M
Coverage Section: Professional Services

This matter involved a holding company with subsidiaries that provide a variety of financial services. Three of the Company's subsidiaries provided services in connection with an investment fund. The fund was ultimately being run as a Ponzi Scheme and the fund manager stole over $20 million from the Fund, which resulted in approximately six claims. Three of the claims made against the three subsidiaries alleged "wrongful acts" in their "professional services" as defined by the policy. The allegations were generally that, if the Company had been doing its job properly, the fraud would have been detected sooner or would not have been possible, so they breached their agreements and failed to perform the services. The demand was in excess of $20M. Ultimately, a global settlement was reached for $3.5M.

Industry:

Manufacturing

A pricey disagreement

Type of Company: Technology Manufacturer
Total Payout: $750,000
Coverage Section: Technology Products and Services

A lawsuit was filed against a technology manufacturer alleging negligence and breach of contract in connection with their procurement of technology products and services. The Plaintiff alleged that the manufacturer was contractually obligated to provide products and services through a certain time period, with which the manufacturer disagreed. Plaintiff alleged that failure of the manufacturer to procure their products and services resulted in Plaintiff losing business and defaulting on their contracts which incorporated the use of the Insured's products and services. Due to the potential liability and exposure in this matter, early resolution was sought unsuccessfully. However, once the motion for summary judgment was filed, again early resolution was attempted and ultimately, after both expert reports presented their findings on damages, the matter was settled for $500,000 (total payout includes defense costs in this matter as well as settlement).

Industry:

Healthcare

A test in discretion

Type of company: Hospital
Total Payout: $150,000
Coverage Section: Data Breach Response and Crisis Management Coverage

This matter involves a demand letter from an employee at a hospital. The claimant asserted allegations that the hospital violated her rights under: the Health Information Portability and Accountability Act; California Confidentiality of Medical Information Act; and/or other relevant privacy laws and regulations. Specifically, the employee contended that after arriving to work in an apparent state of intoxication, the employee may have been blood tested at the hospital, and that the results of this blood test may have been the basis of disciplinary action against the employee and accessible to unauthorized individuals at the hospital. The matter ultimately settled for $150,000.

Humans have moved ahead of machines as the top target for cyber criminals:

Human attack surface to reach

4 billion people

by 2020.

Human attack surface is the totality of all exploitable security holes within an organization that are created through the activities and vulnerabilities of personnel. Elements of an organization's human attack surface include negligence, errors, illness, death, insider threat and susceptibility to social engineering.

Ransomware damage:

It is predicted that a business will fall victim to a ransomware attack

Every 14 seconds

by 2019.

Further, ransomware attacks on healthcare organizations – the number 1 cyber-attacked industry – are predicted to quadruple by 2020

The cost of data breach sets a record high:

In 2017 data breaches cost companies an average of

$225

per compromised record.

This is up from 2016's figure of $221. The total average organizational cost of data breach reached a record high of $7.35 million. (up from $7.01 million in 2016)

Fast Facts

Industry:

Media

Unauthorized use

Type of company: Entertainment Company
Total Payout: $275,000
Coverage Section: Media

An entertainment company and their customer were sued for copyright infringement. Specifically, the Plaintiff alleged that her song was used in a clothing advertisement without her authorization. The insured and their customer presented strong defenses however due to the litigious nature of the Plaintiff and costly litigation upon filing a motion to dismiss the second amended complaint, a settlement was secured $35k which avoided any further defense expense as well as time consuming discovery. Total costs incurred were made up of defense costs in this action and the $35,000 settlement.

Inside Job

Type of Company: Online Media
Total Payout: $400,000
Coverage Section: Data Breach and Crisis Management Coverage

This matter involved an online media company who was contacted by the FBI informing them that a hacker used a former employee's credentials to access their network and steal 1.7 million email addresses and passwords of users of the website. Coverage was provided under the Data Breach and Crisis Management Insuring Agreement. Legal, notification, and forensics costs incurred totaled $400,000.

Industry:

Municipal Services

An emergency situation

Type of Company: Fire Department
Total Payout: $50,000
Coverage Section: Business Interruption and Extra Expenses

A local municipality's fire department was subjected to a malware intrusion. They required assistance to get their systems back up and running, particularly their 9-11 system as calls had to be re-routed to the county operator. The matter constituted a cyber security breach triggering First Party Liability Business Interruption and Extra Expense coverage. The costs to get back up and running totaled approximately $50,000.

Industry:

Real Estate

A close call

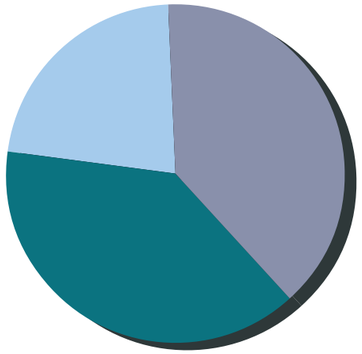
Type of company: Real Estate Company
Total Payout: $85,000
Coverage Section: Data Breach Response and Crisis Management Costs, Cyber Extortion

A real estate company detected suspicious activity on its server after it was discovered that the IT team had inadvertently activated malware which encrypted files on various servers. In doing so, a ransomware demand was made upon the Insured of $10,000. The system was immediately shut down in an attempt to keep the malware from spreading. The company contacted the Data Breach Hotline and our claims team worked to engage breach counsel and forensics to assist with responding to this incident. It was determined the company did not need to pay the ransom as they were able to restore the network from backups. After completion of the forensic investigation, it was determined that there was no compromise to any confidential information and otherwise, no reporting requirements.

"It was determined the company did not need to pay the ransom as they were able to restore the Network from backups."

Claims Trends

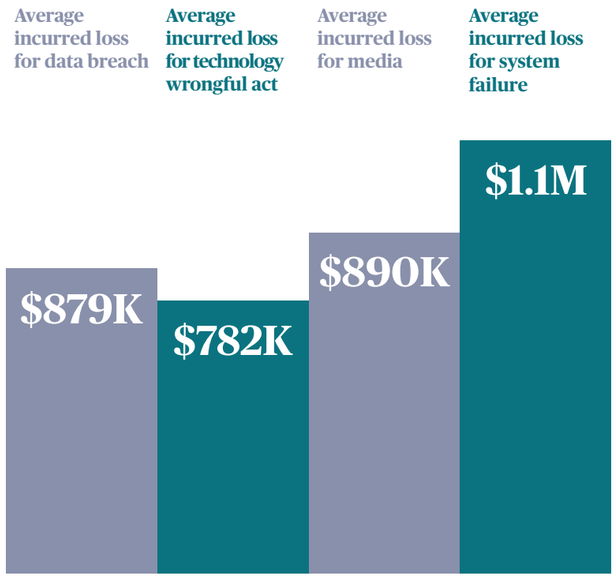
Percentage of losses incurred by cause of loss are approximately



39%
data breach related

39%
technology wrongful act

22%
media personal injury claims



*Claims trends based on AXA XL cyber claims with losses > $1M. Note that total payout includes any amounts incurred within the Insured's self insured retention.

Industry:

Retail

Theft in "real time"

Type of Company: Online retailer
Total Payout: $1,800,566 (inclusive of a $25,000 PCI Fine)
Coverage Section: Data Breach Response and Crisis Management Coverage and PCI DSS Coverage by Endorsement

An online retailer discovered unusual activity on its server, which prompted an investigation. The investigation revealed that an employee's credentials were stolen and then used to steal customer information in "real-time" as it was being entered into the retailer's "checkout" site. The hackers were able to steal information of approximately 50,000 customers, including customer names, billing address, credit card number, expiration date and CVV code.

Following the incident, we participated in numerous conference calls with the retailer to discuss the incident, recommend the appropriate vendors and facilitated calls with prospective vendors. Forensics was retained to confirm the scope of the incident and remediate the threat. Notifications were issued to the individuals and appropriate agencies were provided notice, a call center was set up and monitoring services were offered. Because notification was done in a timely manner, there were no third party claims arising from the incident. The retailer received a $25,000 fine for non-compliance with PCI-DSS.

Bubbling over with credentials

Type of Company: Soda Distributor
Total Payout: $125,000
Coverage Section: Data Breach Response and Crisis Management Coverage

Several employees at a soda distributor provided their email credentials to a hacker in response to a phishing email. The Data Breach Response and Crisis Management Coverage Insuring Agreement was triggered, and privacy counsel and a computer forensics vendor were retailed to investigate the scope of the breach. The investigation revealed that over 130 individuals needed to be notified that their personally identifiable information may have been compromised as a result of the incident. Credit monitoring services for the impacted individuals was also. The costs associated with this matter totaled approximately $125,000. Since the matter was handled promptly and notification was done in a timely manner, no third party lawsuits ensued.

Phishing for payroll info

Type of Company: Private leading food distributor
Total Payout: $100,000
Coverage Section: Data Breach and Crisis Management Coverage

This matter involved a private leading food distributor. Several of its employees replied to a phishing email and provided their log-in credentials. Hackers then used the credentials to access an employee portal for health and welfare benefits and payroll information and were able to change the employees' direct deposit account information so that payments were redirected to accounts controlled by the hackers. However, due to quick remedial actions taken by the company's internal IT Security and HR departments, only a handful of employees' payments were sent to the hackers' accounts, resulting in a loss of approximately $5,000. The company retained a breach coach to comply with data breach notification requirements and total expenses incurred were approximately $100,000.

Industry:

Tech/Telecom

A costly defect

Type of company: Technology Company
Total Payout: $1.5 million (in defense costs)
Coverage Section: Technology Products and Services

A claimant filed a lawsuit against a technology company arising from the failure of the company's technology product to properly perform. It is alleged that the company failed to detect a defective component which they designed, manufactured and distributed. The claimant alleged that it suffered tens of millions in damages, including costs to replace the nonconforming goods, settlements with its retail customers, loss profits and goodwill and loss of future business opportunities. There were several causes of action, however, most relevant were claims for breach of contract and breach of warranty. Coverage was triggered under the Technology products and services insuring agreement due to the company's Technology Product failing to work properly, resulting in damages. After several unsuccessful mediations, this matter went to trial and a verdict was received in favor of the technology company.

A costly cabling mess

Type of company: Telecommunications Company
Total Payout: $1.1M
Coverage Section: Technology Products and Services

A demand letter was sent to a telecommunications company for alleged wrongful acts in their professional services. Specifically, it was alleged that the company incorrectly configured wires at its customers location, leading to a service outage. Their customer received several claims from its end-customers. Claimant sought various damages against the company, including indemnity for its end-customers' claims and damage to its reputation. Coverage was triggered coverage under the Technology and Professional Services insuring agreement and ultimately this matter was settled for $1.1 million.

A malicious infiltration

Type of company: Internet Services Company
Total Payout: $5M
Coverage Section: Business Interruption and Extra Expenses Data Breach Response and Crisis Management

A malicious actor infiltrated the network of an internet services company and obtained the personally identifiable information of millions of the site's users. The incident triggered the Business Interruption and Extra Expenses Insuring Agreement and the Data Breach Response and Crisis Management Coverage Insuring Agreement. Coverage was provided for privacy counsel fees, computer forensics fees, notification costs, identity theft monitoring fees, fees for a public relations firm, and fees to operate a call center to answer questions from impacted individuals as well as associated extra expenses enabling the company to resume operations. The total amount incurred was approximately $5 million.

Irreparable consequences

Type of Company: Software Developer Company
Total Payout: $550,000
Coverage Section: Technology Products and Services

A software developer was sued for alleged defective software that claimant contained could not be fixed. The claimant further contended that they the defective software was detrimental to its customers and employees. As a result, the claimant requested compensation for lost profits, cost of nonproductive billed consultant time, and annual maintenance on a product that could not be effectively supported in an amount of $1.9 million. The matter ultimately settled for $550,000.

Pervading points of contact

Type of Company: Computer Network Services Company
Total Payout: $200,000
Coverage Section: Data Breach and Crisis Response Coverage

A computer network services company discovered that the email accounts of two finance employees had been hacked. After forensics were retained, evidence demonstrated that the accounts had been accessed via IP addresses in Ireland and eastern Europe, but neither employee was in those locations. The email account of the UK-based employee contained personally identifiable information of the insured's employees, including first and last names, UK identity numbers, passport numbers, and bank account numbers. All of this information would have been visible to the hackers. Coverage was provided under the Data Breach Response and Crisis Management Coverage Insuring Agreement. Breach counsel was retained to ensure that appropriate notice was provided to the affected employees as well as credit monitoring so that affected employees were adequately protected.

To learn how AXA XL Cyber coverage can protect your business, please contact your AXA XL Cyber Underwriter.

"A malicious actor infiltrated the network of an internet services company and obtained the personally identifiable information of millions of the site's users."

5231_01/2019