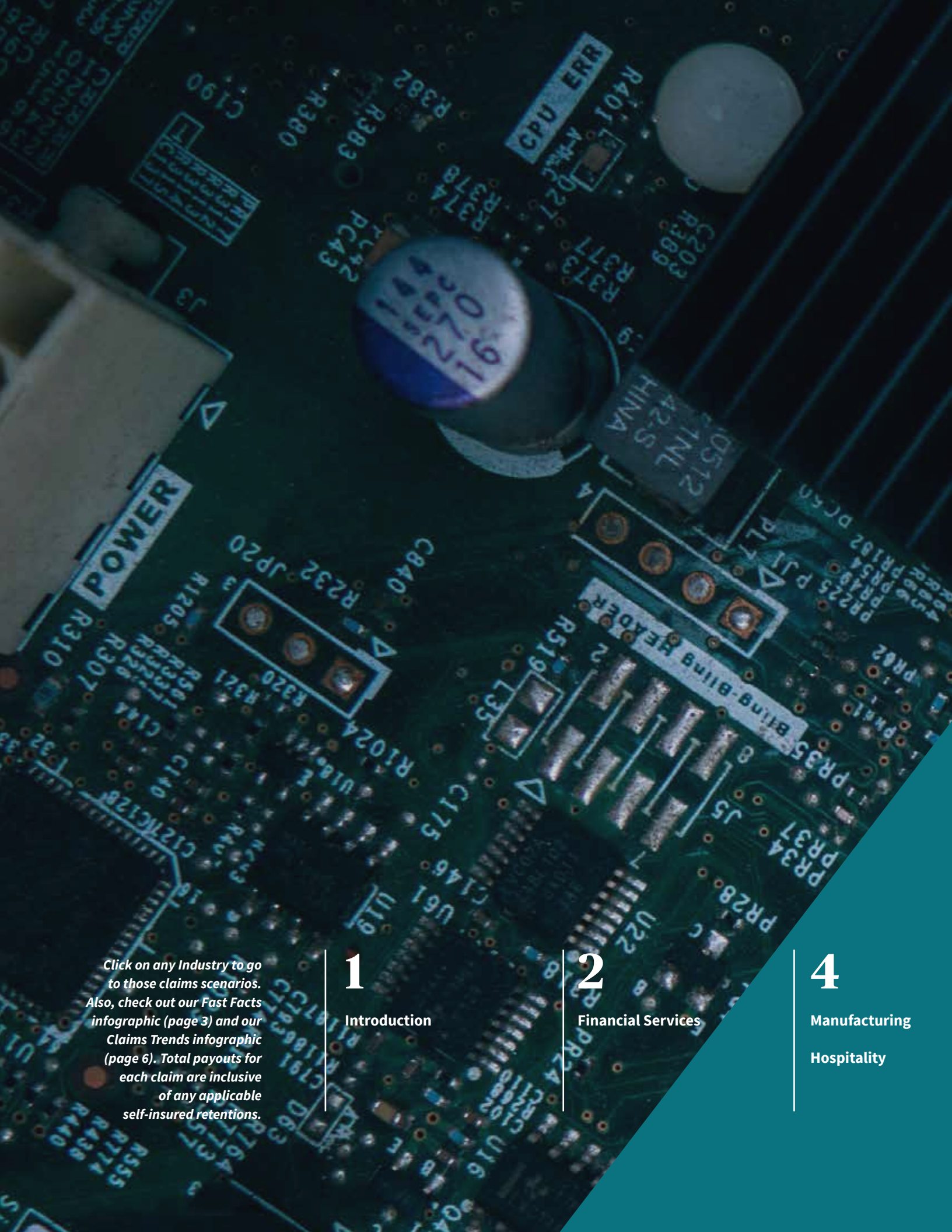
Cyber claims

Real-life AXA XL claims scenarios



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). Total payouts for each claim are inclusive of any applicable self-insured retentions.

The liabilities associated with cyber exposures can devastate your business. A single cyber-attack in the US costs companies, on average, $8.19 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.

This year, we saw a significant increase in ransomware claims in both frequency and severity. We also saw an increased number of claims for violations of the Biometric Information Protection Act ("BIPA"), business email compromises and social engineering attempts. Specifically, this year we saw our first eight figure ransom demand; and of our overall claims, social engineering and ransomware comprised just over 60%. Of the ransomware claims our team has handled, there was a large increase on those in the manufacturing and chemical company sector as well as those attacks spreading to third party companies that had connected networks.

Continue reading to find out more.

5

Healthcare

7

Professional Services

8

Municipal Services

10

Logistics

IT/ Technology Services

Industry:

Financial Services

Data heist

Type of company: **Financial services**
Total Payout: **$50,000**
Coverage Section: **Data Breach Response and Crisis Management Coverage**

A financial services company was the victim of a burglary, in which an unencrypted laptop was stolen. Coverage was triggered under the Data Breach Response and Crisis Management Insuring Agreement, as it was reasonably suspected that personally identifiable information may have been accessed on the device. The company immediately retained privacy counsel to assist with investigating the incident. Total costs in the matter were $50,000 due to the fact that the laptop was stolen and could not be recovered so no forensic costs ensued. The amounts incurred were reflective of legal costs and notification to a very small population. It should be noted that this matter was also reported to the Insured's Crime policy.

Phishing for credentials

Type of company: **Financial services/Insurance**
Total Payout: **$15,000**
Coverage Section: **Data Breach Response and Crisis Management Coverage**

An insurance company was the victim of a phishing incident. Specifically, a third party accessed the email account of an executive officer, by obtaining his credentials through a prior phishing incident. This third party used the compromised email account to send out an email containing another credential harvesting phishing attack to everyone in the executive officer's address book. The company retained privacy counsel, who determined there were no legal obligations to notify any individuals and total expenses were capped at $15,000.

Misdirected money

Type of company: **Financial services**
Total Payout: **$225,000**
Coverage Section: **Data Breach Response and Crisis Management Coverage; Social Engineering Financial Fraud Endorsement**

A financial services company was the victim of a social engineering event, which resulted in a fraudulent wire transfer of $200,000. Specifically, in June of 2018, the company transferred funds in connection with the closing of a property. The fund transfer was made pursuant to updated instructions that they allegedly received from their vendor. It was ultimately discovered that the wire transfer was fraudulent when the company was notified several months later by the intended recipient that they had not received the transfer. Coverage was triggered under the Data Breach Response and Crisis Management Insuring Agreement, as it was reasonably suspected that the company suffered an email compromise. The company retained privacy counsel and forensics to assist with investigating the incident. Additionally, this incident triggered the Social Engineering Financial Fraud Endorsement. Approximately $225,000 was incurred in connection with these costs and the fraudulent transfer. It should be noted that this matter was also reported to the company's Crime policy.

Fast Facts

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.

Percentage of data breach root causes in 2019:

52% Malicious or criminal attack

25% Human error

23% System glitch

The cost of data breach sets a record high:

In 2019 data breaches cost companies an average of

$242

per compromised record.

This is up from 2018's figure of $233. The total average organizational cost of data breach reached a record high of $8.19 million (up from $7.91 million in 2018).

Source: *IBM 2019 Cost of Data Breach Report: USA*

Industry:

Manufacturing

A costly faulty process

Type of company: **Gasoline engine manufacturer**
Total Payout: **$250,000**
Coverage Section: **Data Breach Response and Crisis Management Coverage; Social Engineering Financial Fraud Endorsement**

On March 29, 2019 a gasoline engine manufacturer discovered that a request for a change in wiring instructions was fraudulent. This happened even though the accounts payable department had a process in place for when a vendor changes banking instructions. The payment was approximately $250,000. A breach coach was retained who subsequently retained a forensic vendor to investigate. It was determined that no additional information was compromised, and coverage was triggered for forensic investigation and legal expenses.

Held for ransom

Type of Company: **Pharmaceutical manufacturer**
Total Payout: **$1M**
Coverage Section: **Data Breach Response and Crisis Management Coverage; Cyber Extortion and Ransomware; Business Interruption and Extra Expenses**

This matter involved a manufacturer specialized in equipment for pharmaceutical companies. Specifically, the company experienced a ransomware attack which infected their network. Operations ceased as a result of the ransomware and $500,000 in bitcoin was demanded for the decryption keys, which was ultimately paid. Coverage for this matter was triggered under the coverage sections for Data Breach Response and Crisis Management Coverage, Cyber-Extortion, Data Recovery and Business Interruption and Extra Expense(s). We worked vigorously to retain legal counsel, forensic vendors, and specifically, a vendor with the capability to provide a large amount of bitcoin within a short time period. The insured also had a Kidnap & Ransom policy which provided limited coverage for the cost of bitcoin and limited business interruption costs. Total costs in this matter were comprised of legal and forensic investigation costs as well as the $500,000 ransom payment.

Industry:

Hospitality

An inhospitable intrusion

Type of Company: **Hospitality (hotel chain)**
Total Payout: **$80M**
Coverage Section: **Data Breach Response and Crisis Management Coverage; Privacy and Cyber Security; PCI DSS Endorsement**

This matter involves a credit card breach occurring at a hotel chain. Specifically, in September of 2016 and March of 2017 the hotel was notified by Visa of a potential credit card breach at the hotel. The hotel engaged a law firm who retained a forensics company to carry out a forensic investigation which identified a window of intrusion from March 2016 to October 2016, and November 2016 to April 2017, impacting approximately 315,000 credit cards.

Total costs incurred were reflective of notification to affected individuals, defense costs and settlements and PCI fines and penalties.

Houston, we have a problem!

Type of Company: **Hospitality (airline)**
Total Payout: **$80M (approx.)**
Coverage Section: **Business interruption; System Failure Endorsement Coverage**

In July of 2016 an airline experienced a technology outage which impacted commercial and operational applications. Their systems were offline for nearly twelve hours and even once materially back online they continued to experience major disruptions. The total amount of loss incurred as a result of the incident was nearly $80M, which was quantified by the airline through a forensic accounting firm. The loss claimed was comprised of lost revenue, extra expenses and non-continuing expenses.

Industry:

Healthcare

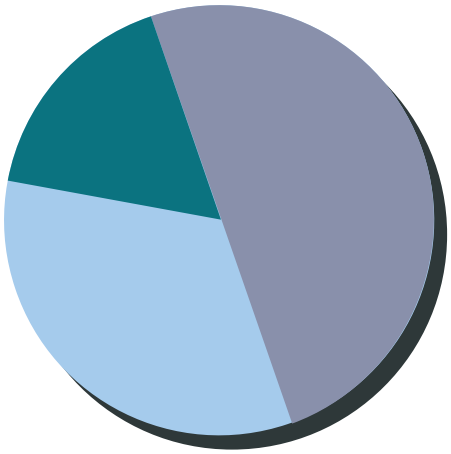
Privacy, please!

Type of company: **Healthcare agency**
Total Payout: **$100,000**
Coverage Section: **Data Breach Response and Crisis Management Coverage**

A healthcare agency was contacted by a patient's mother after she discovered multiple pages of protected heath information and personally identifiable information that did not belong to the patient in his discharge paperwork. She asked the company to confirm that her son's information was not in the possession of other agency patients. After the agency provided her with confirmation, she allowed the agency to retrieve the documents that she improperly received. The information related to five additional individuals. The data breach response and crisis management coverage insuring agreement was triggered as result of this matter. The individuals whose information was improperly disclosed were notified of this matter, and they were offered identity and credit protection monitoring, as their social security numbers and banking information was among the inadvertently disclosed information. Data breach response and crisis management costs totaled $100,000.

Claims Trends

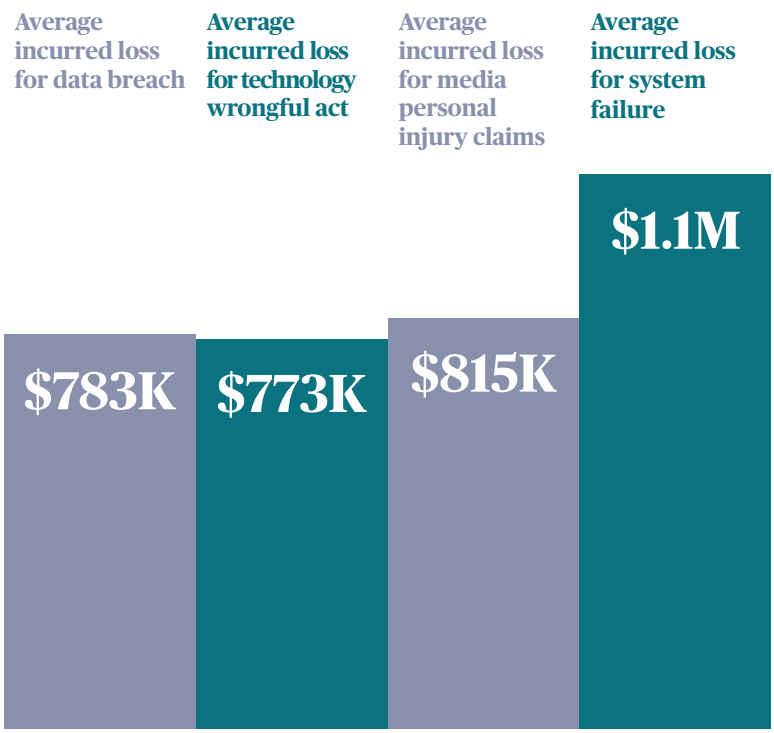
Percentage of losses incurred by cause of loss are approximately



49%
data breach related

34%
technology wrongful act

17%
media personal injury claims



Industry:

Professional services

Unauthorized use

Type of company: **Debt collection agency**
Total Payout: **$15,000**
Coverage Section: **Data Breach Response and Crisis Management Coverage**

This matter involved a debt collection agency. Specifically, the company was the victim of unauthorized access of two employees' Microsoft Office 365 email accounts. This led to the exposure of 300 consumer records, though there was no indication that any of the records were exfiltrated. The Insured retained privacy counsel and sent a notice for credit monitoring for all affected individuals. Since only four individuals enrolled, total expenses were $12,750 plus nominal forensic and legal expenses.

A close call

Type of company: **Accounting firm**
Total Payout: **$0**
Coverage Section: **Data Breach Response and Crisis Management Coverage**

This matter impacted an accounting firm. Specifically, a phishing email was sent to an employee asking for a spreadsheet providing "current open payables as of a specific date." The employee responded on the same day by sending the requested information on amounts owed to the insured by 74 of their clients/vendors. Fortunately, the scam was discovered on the same day and the firm contacted all 74 clients/vendors telling them not to respond to any changes in banking or any other financial information and called all of their impacted customers. Due to their swift response, no payments were made to the wrong payee as a result of the scam.

Taken for a ride by a temp

Type of company: **Professional services firm**
Total Payout: **$350,000**
Coverage Section: **Data Breach Response and Crisis Management Coverage**

A lawsuit was filed against our insured, who provides staffing services, arising from alleged damages sustained as a result of negligent work done by a temporary employee. Specifically, the company recommended a candidate to its customer to serve as their interim Chief Financial Officer. The client ultimately gave the temporary employee significant responsibilities and allowed her to overhaul their billing department and billing process. The client alleged that the employee was actually unqualified and caused approximately $1.75 million in damages, in part, because they failed to timely bill its customers resulting in the inability to collect money that was owed to them. Despite the demand, settlement was reached for $300,000 and additional costs incurred were reflective of defense costs.

Industry:

Municipal Services

Back-ups save the day

Type of Company: **Municipality**
Total Payout: **$60,000**
Coverage Section: **Data Breach Response and Crisis Management Coverage; Cyber-Extortion and Ransomware Coverage; Data Recovery Coverage**

A municipality was the victim of a ransomware event, which resulted in the encryption of multiple devices on its network. Coverage was triggered under the First Party Coverages for Data Breach Response and Crisis Management, Cyber-Extortion and Ransomware and Data Recovery, given the nature of the attack and the reasonable suspicion that there was personal identifiable information on the network. The municipality retained privacy counsel and forensics to assist with investigating the incident. $60,000 was paid in connection with these costs due to the Insured having viable back-ups of its network, therefore not requiring payment to the malicious actor.

Unleashing the code

Type of Company: **Municipality**
Total Payout: **$150,000**
Coverage Section: **Cyber-Extortion and Ransomware Coverage; Data Breach Response and Crisis Management Coverage**

The Insured is the police department of a township which was infected with ransomware. It was determined after a forensic investigation that all files on the network were encrypted, rendering them inaccessible. A ransom demand for $50,000 was made and subsequently paid for in order to obtain the decryption key. Total costs in this matter were $150,000 and were reflective of privacy counsel, forensic expenses and the ransom payment.

Duped!

Type of Company: **Municipality**
Total Payout: **$200,000**
Coverage Section: **Data Breach Response and Crisis Management Coverage; Cyber-Extortion and Ransomware Coverage; Social Engineering Financial Fraud Endorsement**

The Insured is a county in Florida who made a fraudulent wire transfer of two payments totaling $184,534.85 to its vendor after receiving a social engineering email with new ACH information. Upon receiving the fraudulent information requesting that the funds be sent to a new ACH address, the county followed its procedures of sending an ACH transfer form to a third party, who sent it back containing the (fraudulent) signature of the vendor's vice president. The Insured's internal IT department determined the fraud was a result of an intrusion on the vendor's computer system. After retaining privacy counsel and a forensics company, it was determined that no other parts of the network were compromised, and total costs were just under $200,000 consisting of the two payments, legal and forensic investigation costs.

A call for backup

Type of Company: **Municipality**
Total Payout: **$25,000**
Coverage Section: **Cyber-Extortion and Ransomware**

The Insured is a police department in New Jersey which experienced ransomware on two police servers, three infected workstations and the two backup drive files which had been infected by an external attacker. The Insured determined that given the age of the equipment and the need to resume functionality, the department needed to replace two servers, three workstations and two external hard drives. No ransomware was paid, and the incurred losses were $23,018.

Getting schooled by a hacker

Type of Company: **Municipality (school district)**
Total Payout: **$225,000**
Coverage Section: **Data Breach Response and Crisis Management Coverage**

After numerous users reported reboot issues with their computers, it became apparent that a significant number of the school district's 6,000 end points and approximately 100 servers were impacted by a Trickbot infection. First party coverage under the Data Breach Response and Crisis Management Costs insuring agreement was triggered. The insured engaged privacy counsel and forensics to investigate and remediate. Notification, call center services, and credit monitoring were subsequently provided to impacted individuals, and the matter was reported to the state AG. Privacy counsel also assisted the insured in responding to a request for information under state law from a local newspaper. Total costs incurred were approximately $225,000.

Due to their swift response, no payments were made to the wrong payee as a result of the scam.

Industry:

Logistics

Pointing fingers

Type of company: **Logistics**
Total Payout: **$600,000**
Coverage Section: **Privacy and Cyber Security Liability**

This matter involves a putative class action alleging violations of the Biometric Information Privacy Act ("BIPA"). Illinois enacted the Biometric Information Privacy Act, 740 ILCS 14/1, et seq. ("BIPA") to regulate companies that collect and store Illinois citizens' biometrics, such as fingerprints. The BIPA establishes standards for how employers must handle Illinois employees' biometric identifiers and biometric information, and ultimately mandates that reasonable safeguards are put in place. The insured provides operations and management services to senior living communities throughout the United States, including numerous facilities in Illinois. In doing so, they use a biometric time tracking system that requires employees to use their fingerprints as a means of authentication, rather than key fobs or identification cards. As such, employees are required to have their fingerprint scanned to enroll in the database. Plaintiff, on behalf of the class, alleged that the Insured did not comply with BIPA in connection with its collection and use of the fingerprints.

This matter triggered coverage under the Privacy and Cyber Security Liability Coverage Section. An early settlement in this matter was reached and total Defense costs plus the settlement on a class basis totaled approximately $600,000.

Industry:

IT/Technology services

Phishing phonies

Type of Company: **IT service management company**
Total Payout: **$25,000**
Coverage Section: **Data Breach Response and Crisis Management Coverage**

This matter impacted an IT service management company. Specifically, an employee responded to a phishing email asking for 700 W-2s. As a result, the company sent employee communications and formal notice letters to employees and relevant state authorities and arranged for 24 months of Credit monitoring for employees. The company also notified the FBI and IRS. They investigated internally, and no malware was found. As a result, costs were kept to $25,000 which was comprised of notification and credit monitoring, as well as privacy counsel.

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

We worked vigorously to retain legal counsel, forensic vendors, and specifically, a vendor with the capability to provide a large amount of bitcoin within a short time period.

5231_12/2019