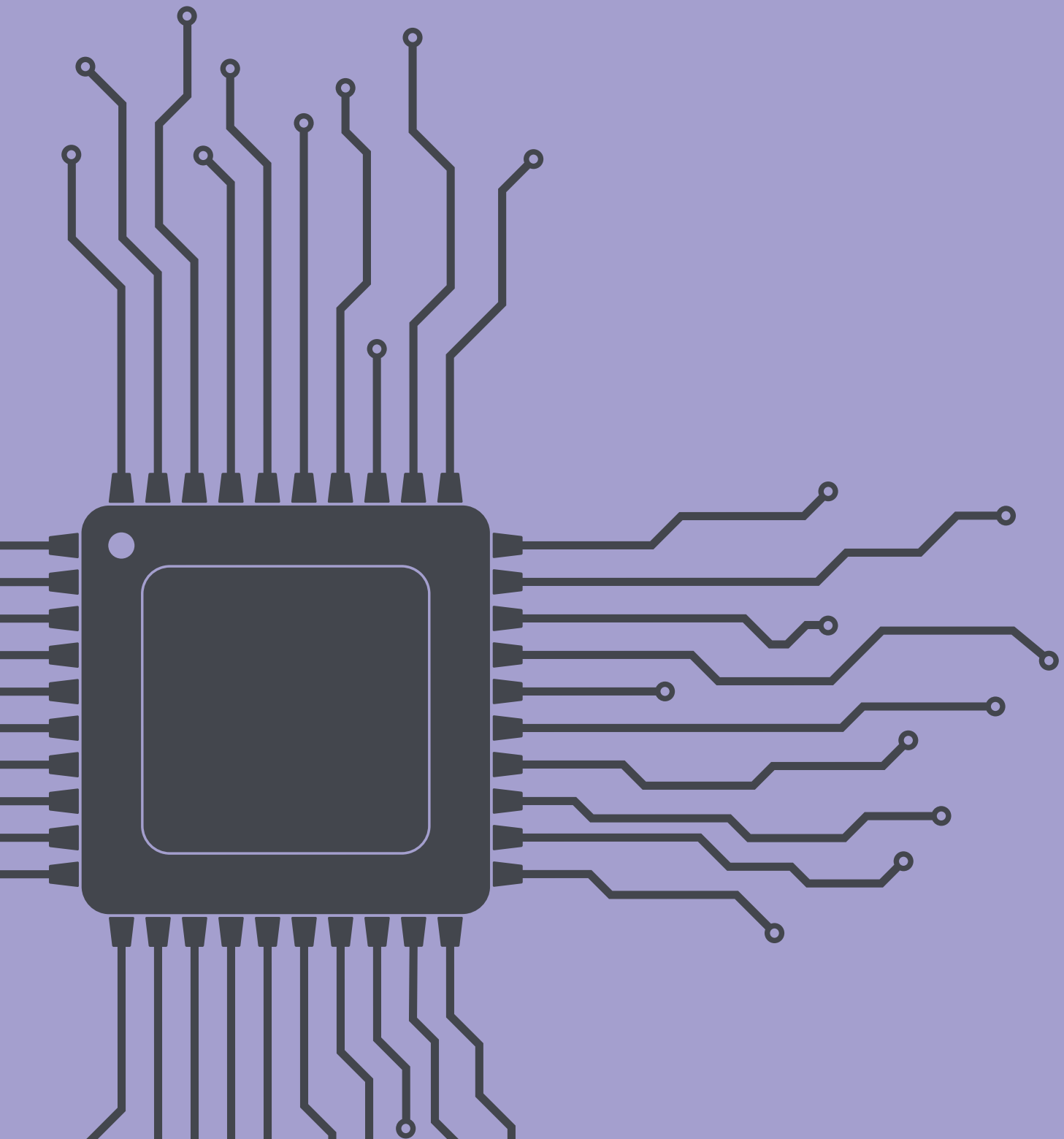
Cyber attacks: Claims scenarios ripped from today's headlines

XL CATLIN



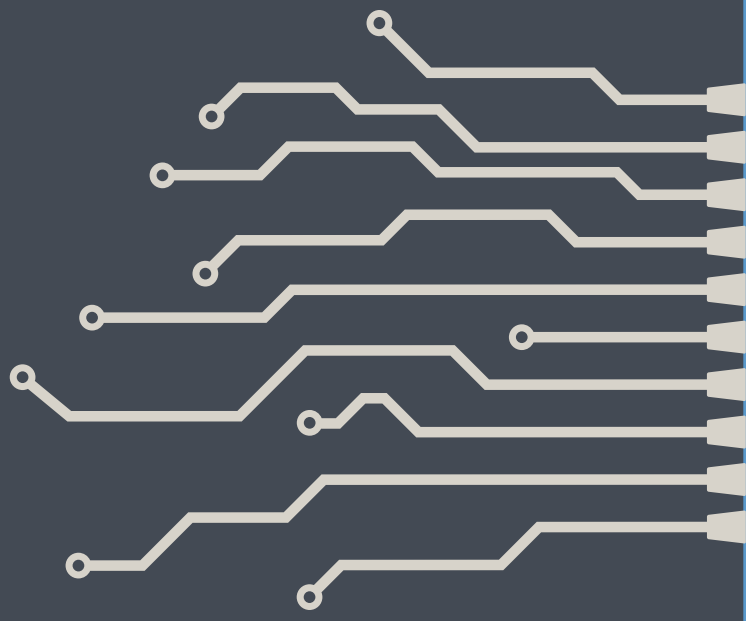
The liabilities associated with cyber exposures can devastate your business. Cyber-attacks cost companies, on average, USD 4 million.

Protect your business by understanding your cyber liability exposures and how XL Catlin 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.

The following recent claim examples demonstrate some of the ways in which XL Catlin's Cyber and Technology Liability Coverage protects business across a wide range of industries, including:

Click on any Industry to go to those claims scenarios

Also, check out our Fast Facts infographics on pages 03 and 05!



THE INDUSTRY:

FINANCIAL SERVICES

A big boo-boo

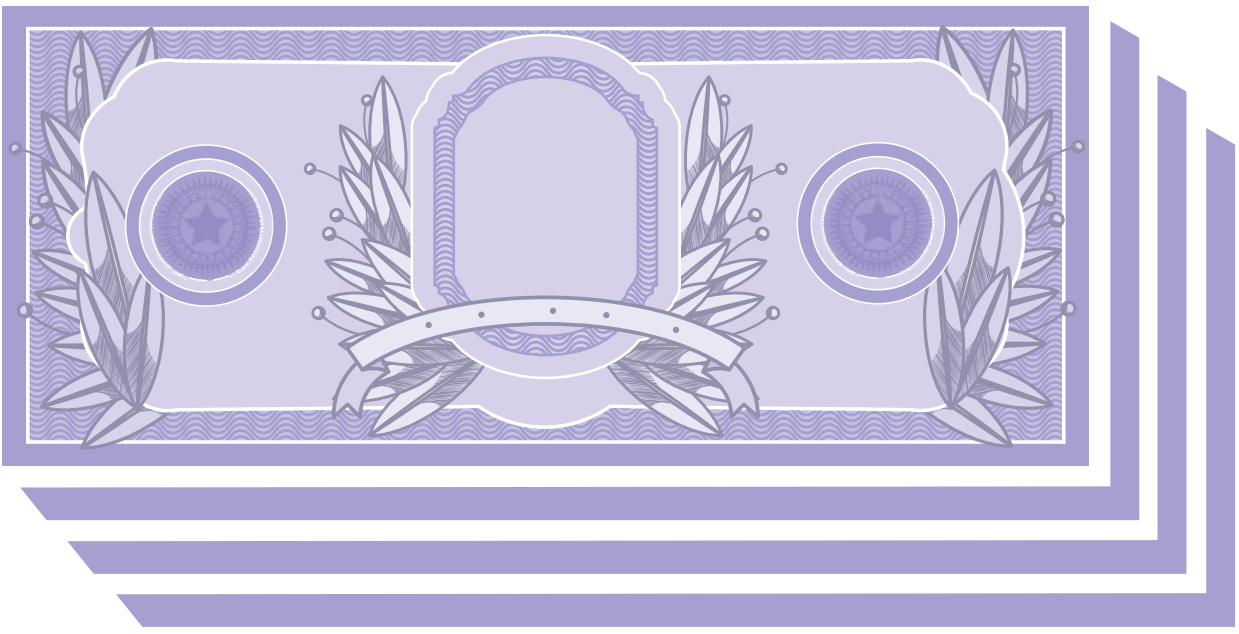
Type of Company: **Hospital Billing Provider**
Total Payout: **USD 1.3M**
Coverage Section: **Professional Services**

A billing provider outsourced by a hospital was sued in a putative class action. The plaintiffs alleged that the company qualified as a debt collector and failed to provide certain disclosures required under the Fair Debt Collection Practices Act when contacting patients about unpaid bills. Coverage was provided under the Professional Services Liability Insuring Agreement. The matter settled for a combination of injunctive relief and a payment of USD 1.3 million.

TMI! TMI!

Type of Company: **Online lending company**
Total Payout: **USD 200K**
Coverage Section: **Data Breach and Crisis Response**

After a routine review of an on-line lending company's web server logs, the company noticed log lines containing customer's personal information, including names, social security numbers, addresses and phone numbers. Upon further investigation, it was determined that there was a client-side website error on the webpage where a customer would enter their personal information. The error triggered the browser to redirect the user to a different page, in which their personal information was included as part of that webpage's address or URL, and inadvertently sent the data to a third party. Breach counsel and forensic investigators were retained on the Company's behalf to properly identify the issue and determine the scope of the incident. Approximately 13,000 individuals were affected across 18 states. A third-party vendor was retained to assist with notifications, set up a call center and provide monitoring services to the affected individuals. The breach response costs were USD 200,000.



THE INDUSTRY:

GOVERNMENT AGENCIES

Wipe out!

Type of Company: State County Housing and Redevelopment Authority
Total Payout: USD 250K
Coverage Section: Privacy and Cyber Security / Data Breach and Crisis Management

A State County Housing & Redevelopment Authority (SCHRA) was the victim of a ransomware attack. Prior to tendering notice, SCHRA had its third-party IT vendor review the impacted server. In doing so, the vendor wiped the system. Unfortunately they also deleted the metadata and evidence relative to the breach. SCHRA retained Counsel, who contracted a forensics firm to review the impacted server and associated workstations. The forensics firm concluded that the Personally Identifiable Information (PII) on the systems could have been accessed as a result of the malware. Forensics subsequently performed a data mining review across the affected systems to identify relevant PII. This data mining process was time consuming and, as a result, SCHRA incurred most of its costs in this area. 6,893 individuals were notified, along with applicable regulators and HUD. A firm was retained to handle mailing of notice letters and establishment of a call center. A Public Relations firm was retained for limited crisis communication services. Credit monitoring services were also retained. Total payout was USD 250,000.

Decoding a disaster

Type of Company: State County Government
Total Payout: USD 125K
Coverage Section: Cyber Extortion and Data Recovery

Twenty servers of a State County Government became infected with ransomware. The county government was unable to conduct any business on its computers because the ransomware had encrypted all of the server data. Privacy counsel and a forensics vendor were retained. Because the data for the District Attorney's office was stored on the county servers and was not backed up, the county was forced to pay the ransom to decrypt its data. Coverage was provided under the Cyber-Extortion Insuring Agreement and the Data Recovery Insuring Agreement. Between legal fees, forensics fees, the ransom payment, and data recovery costs, the total amount incurred exceeded USD 125,000.

This is a hold up!

Type of Company: County Government
Total Payout: Approximately USD 75K
Coverage Section: Cyber Extortion, Data Breach and Crisis Management

A county Police Department was the victim of a ransomware attack on its computer system. After a preliminary scoping call, the decision was made to retain a Forensic Investigations Firm to assist in paying the ransom demand of 4.6 bitcoins (approximately $5,500, at the time) and retrieving the decryption key to restore the files. A forensic investigation into the nature and scope of the attack was also undertaken to determine if any confidential information was exposed. Costs incurred inclusive of ransom demand and forensic investigation costs were approximately USD 75,000.

THE INDUSTRY:

GOVERNMENT CONTRACTORS

Spies among us

Type of Company: Government Contractor
Total Payout: USD 250K
Coverage Section: Privacy and Cyber Security / Data Breach Response and Crisis Management

A government contractor providing engineering, logistics support, supply chain management, sustainment, foreign military sales, management sciences, information technology, energy and environmental support, and facilities management received a report from the FBI. Given the information the FBI had gathered during an investigation, they believed a foreign government had accessed the contractor's computer system to obtain more information on the United States Department of Defense. Breach counsel and forensic vendors were retained on the contractor's behalf and matter was resolved for USD 250,000.

// The county government was unable to conduct any business on its computers because the ransomware had encrypted all of the data on its servers //

Facts

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)

Growth of new malware:

It's never been easier to make your own ransomware. There were

4.3x more ransomware variants

in Q1 2017 than in Q1 2016.

Ransomware innovations:

Remote desktop is the new "in"

2/3 of ransomware infections

in Q1 2017 were delivered via

Remote Desktop Protocol (RDP)

Sources: https://blog.barkly.com/cyber-security-statistics-2017 & Ponemon Institute 2017 Cost of Data Breach Study USA

THE INDUSTRY:

HEALTHCARE

A dreaded shred

Type of Company: **Healthcare**
Total Payout: **USD 2.5M**
Coverage Section: **Privacy and Cyber Security / Data Breach Response and Crisis Management**

A healthcare company provides health plans through Medicaid, Medicare and the health insurance marketplace, as well as other health solutions through specialty services companies. The company became aware that hard drives used for a data project to improve the health outcomes of their members could not be accounted for. The company determined the hard drives contained personal health information of 950,000 individuals who received laboratory services, including name, address, date of birth, social security number, member ID number and health information. The hard drives did not include any financial or payment information.

Breach counsel and forensic vendors were retained on the healthcare company's behalf and it was discovered that an employee of the company shredded the hard drives. This reduced the severity of the case significantly and the matter was resolved for USD 2.5 million.

A little privacy, please

Type of Company: **Medical Records Firm**
Total Payout: **USD 10M**
Coverage Section: **Privacy and Cyber Security / Data Breach and Crisis Management, Privacy Regulatory Defense, Awards and Fines**

A third-party provider of electronic medical records services to healthcare providers experienced a server breach. This impacted approximately 4 million people and exposed medical records and information in three primary categories: (1) clinical, which includes diagnostic information, lab results, medications and other treatment information; (2) demographic, which includes name, social security number, address/zip code and date of birth; and (3) financial, which is primarily comprised of claim information.

Vendors were retained on the company's behalf for forensics, legal, public relations, credit monitoring and call center services, and notifications were issued via U.S. Mail and substitute notice to the potentially impacted individuals. Counsel was retained to defend against putative class actions, as well as regulatory inquiries initiated by the FTC, OCR/HHS and a number of state Attorneys General. Total payout was USD 10 million.

THE INDUSTRY:

HOSPITALITY

Locking down loyalty

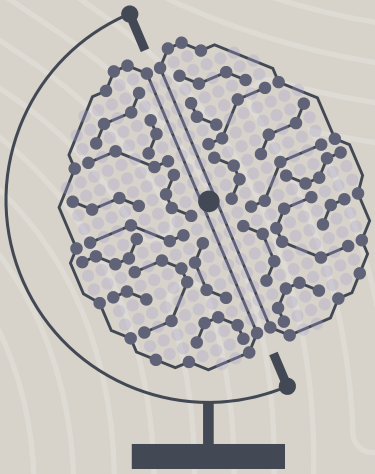
Type of Company: **Hospitality Company**
Total Payout: **USD 2.5M**
Coverage Impacted: **Privacy and Cyber Security/ Data Breach and Crisis Management**

A hospitality company that provides hotel accommodations identified suspicious account log-in activity involving its online customer loyalty program website. Specifically, the company noticed unauthorized parties attempting to access individual customer accounts. 541 customer accounts were impacted. The information that the hackers were able to obtain included personal information such as names, addresses, phone numbers, point balances, and the last four digits of credit card numbers for customers of their loyalty program. The company locked the affected customer accounts, notified affected customers of the incident and advised them to reset their passwords.

Breach counsel and forensic vendors were retained on the company's behalf and the matter was resolved for USD 2.5 million.

// The information that the hackers were able to obtain included personal information such as names, addresses, phone numbers, point balances, and the last four digits of credit card numbers for customers of their loyalty program //

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.

Cybercrime damage costs:

The cybersecurity community and major media have largely concurred that

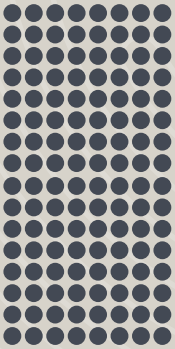
cybercrime damages will cost

the world a predicted

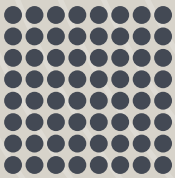
USD 6 trillion annually by 2021,

up from USD 3 trillion in 2016.

2021
USD 6 trillion



2016
USD 3 trillion



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 No.1 cyber-attacked industry – are predicted to quadruple by 2020.

Source: www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html

THE INDUSTRY:

MANUFACTURING

In a momentary disruption

Type of Company: **Paper Goods Manufacturer**
Total Payout: **USD 2M**
Coverage Section: **Business Interruption/System Failure**

A paper goods manufacturer contracted a vendor to perform a system software upgrade at one of their factories. The system upgrade failed, causing all of the company's systems to malfunction on the same day. This unintentional and unplanned outage resulted in the suspension of the company's business in excess of the waiting period in the policy. The Policy covered costs that would not have incurred but for the interruption, and the costs for continuing normal operating expenses. Insurance carriers worked with the company on subrogation issues, so that the software service vendor continued to provide repairs and other needed services to the company. Total payout was USD 2 million.

One big costly oops!

Type of Company: **Technology Manufacturer**
Total Payout: **USD 1M**
Coverage Section: **Technology and Professional Services**

This matter arose out of a technology manufacturer allegedly providing non-conforming technology products to its direct customer, causing damage to the customer as well as down-stream vendors that incorporated the company's alleged faulty product into their end product. A demand letter was sent to the Company seeking USD 6.8 million in damages. This matter settled for a USD 1 million cash payment and approximately USD 1.6 million in service credits and other offsets. The defense obligation was triggered under the Technology and Professional Services insuring agreement and coverage was available for third party damages suffered by the Claimant. Total costs incurred inclusive of settlement were USD 1 million.

THE INDUSTRY:

MEDIA

Foreign intervention

Type of Company: **Media Company**
Total Payout: **USD 60M (Company's total tower of insurance)**
Coverage Section: **Privacy and Cyber Security, Data Breach and Crisis Management and Business Interruption/Extra Expense**

A media company was the target of a cyber-breach attributed to a foreign country which caused an extended business interruption. The company had to secure their network, notify individuals, interact with the media and government officials, and was the subject of various class actions and governmental inquiries. This matter triggered several insuring agreements under the company's policy including business interruption, event management, and security and privacy liability.

Blinded by the negative light

Type of Company: **Advertising Firm**
Total Payout: **USD 1.8M**
Coverage Section: **Technology and Professional Services**

A competitor filed a lawsuit filed against this online advertising media company. The lawsuit referred to an anonymous online post which put Plaintiff in negative light. The plaintiff, believing that the defendant was the source of the anonymous post, filed a lawsuit alleging various causes of action including defamation. Costs incurred represented defense costs in this matter.

Inside job

Type of Company: **Job Postings Website**
Total Payout: **USD 360K**
Coverage Section: **Data Breach and Crisis Management**

The FBI contacted the insured and informed it that a hacker used a former employee's credentials to access the company's network. The former employee stole 1.7 million email addresses and passwords from users of the website. Coverage was provided under the Data Breach and Crisis Management Coverage Insuring Agreement. Legal, notification, and forensics costs totaled USD 360,000.

THE INDUSTRY:

PROFESSIONAL SERVICES FIRMS

Straining to recover

Type of Company: **Construction and Design Services**
Total Payout: **USD 300K**
Coverage Section: **Cyber Extortion**

The company reported notice of a ransomware attack. Privacy counsel and an onsite forensic vendor were retained. The attack was on the company's servers AND its backup servers, which made restoration difficult. The forensic firm identified the ransomware as a variant of the Mamba strain, which encrypts the entire hard drive, rather than encrypting individual files like most ransomware variants. Because Mamba was a relatively new strain of ransomware, no decryption tool was available to address this attack. As a result (and because restoration from backups was not a viable option), it was determined that paying the ransom (20 bitcoin) would be the quickest way to address the situation. The forensic firm worked with a bitcoin broker to secure the necessary funds and coordinated the exchange with the attacker. Because of the way in which the encryption was done, decryption required significant assistance from the forensic firm, which also monitored the decryption process to ensure that the attacker was not able to regain access to the environment and re-encrypt any of the affected machines. There was no evidence that information had been stolen from the company's systems before, during or after the attack and, therefore, no legal notification obligations were triggered by this incident. Total payout including privacy counsel, forensics and the ransom payment was approximately USD 300,000.

And the survey says...

Type of Company: **Corporate Survey Company**
Total Payout: **USD 500K**
Coverage Section: **Media**

An individual named the insured – a corporate survey company – and other related parties in a Class Action complaint filed in the United States District Court. She alleged that the company called her cell phone using an automated telephone dialing system to advertise services without her express consent, in violation of the Telephone Consumer Protection Act ("TCPA"). Claimant sought, on behalf of the proposed class, statutory damages in the amount of USD 500 per violation and USD 1,500 for each willful violation, as well as attorney's fees and costs.

Because the Policy contained a defense only sublimit for TCPA claims, defense costs paid were approximately USD 500,000.

THE INDUSTRY:

RETAIL

Theft in "real time"

Type of Company: **Online Retailer**
Total Payout: **USD 1M**
Coverage Section: **Privacy and Cyber Security/ Data Breach and Crisis Response**

An online retailer discovered unusual activity on its server, prompting 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. Coverage was triggered under the First Party Coverage Section for Data Breach Response and Crisis Management Coverage. Privacy counsel and forensics were retained to notify the necessary individuals and agencies. Approximately USD 1 million was paid in connection to First Party Costs.

RETAIL continued

Badly burned!

Type of Company: **Retailer**
Total Payout: **USD 3.5M**
Coverage Section: **Technology and Professional Services**

Recording companies and music publishers filed a copyright infringement lawsuit against a large retailer. The retailer sold CDs supplied by a vendor who claimed to have valid licenses to the music. Due to the strict liability nature of copyright infringement law coupled with the vendor's inability to adequately indemnify the retailer, this matter was mediated relatively early on in the litigation process to bring about the most advantageous result for the retailer. This matter was handled under the Technology and Professional Services Insuring Agreement.

Restricted access

Type of Comany: **Clothing Retailer**
Total Payout: **USD 100K**
Coverage Section: **Privacy and Cyber Security**

The insured received a letter from a law firm representing disabled individuals. The law firm alleged that the insured's website failed to comply with accessbility requirements defined under the Americans with Disabilities Act, and that – due to those alleged failures – the firms clients were unable to review the website's privacy information and were unable to express their privacy choices on the site. Coverage was provided under the Privacy and Cyber Security Insuring Agreement.

THE INDUSTRY:

TECH/TELECOM

Service denied

Type of Company: **Information Services (Technology enabling accuracy of payment integrity across the healthcare and P&C industries)**
Total Payout: **USD 100K**
Coverage Section: **Business Interruption and Extra Expense**

An information services company was the target of a Distributed Denial of Service attack ("DDOS attack"), which caused its website, email and other systems to go down preventing the company from operating. The appropriate vendors were engaged to address the situation, primarily to bring the system up to its full functionality and to conduct a forensics investigation to ensure that there was no other threat on the network. Coverage was triggered under the First Party Insuring Agreement for the Business Interruption Section. Costs incurred were due to the retention of a forensics firm and privacy counsel. Additionally, an analysis of the company's potential reduction in business income was undertaken. Total costs paid were USD 100,000.

Missing expectations

Type of Company: **Technology Solution Provider**
Total Payout: **USD 900k**
Coverage Section: **Technology and Professional Services**

A complaint against a technology company alleged various causes of action including breach of contract and promissory fraud in connection with the development and implementation of software to help healthcare organizations keep electronic records and submit electronic billings. The tech company maintained that the software worked as originally contracted. However, due to change orders requested by the plaintiff throughout the project, the scope of the project far exceeded the budget. The parties were able to amicably resolve this matter after some necessary discovery was exchanged but before positions were too hardened. Coverage for this matter was triggered under the Technology and Miscellaneous Professional Services Liability Coverage Section of the Policy.

TECH/TELECOM continued

Pervading points of contact

Type of Company: Computer Network Services Company
Total Payout: USD 220K
Coverage Section: Data Breach and Crisis Response

A computer network services company discovered that the email accounts of two finance employees had been hacked. Evidence demonstrated that the accounts had been accessed via IP addresses in Ireland and Eastern Europe, where neither employee was located. The email account of the UK-based employee contained personally identifiable information of the company'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. Privacy counsel was engaged to ensure that appropriate notice was provided to the affected employees, as well as credit monitoring so that the affected employees were adequately protected. Total payout was approximately USD 220,000.

Hey! You! Get off of my cloud

Type of Company: Cloud Service Provider
Total Payout: USD 3M
Coverage Section: Media

A crowd-sourced online company provides a file sharing platform. Users who submit such items can navigate the site free of charge; others pay a monthly fee. Claimants are publishers who allege that there were massive instances of infringement under the Digital Millennium Copyright Act ("DMCA") on the company's website, and that the company knowingly permitted unauthorized publication of the publishers' works. Claimants, through counsel, demanded financial damages as well as information about the company's efforts to reduce or stop alleged infringement. Alleged statutory damages for willful infringement could have been in excess of USD 1 billion. The company was concerned that a lawsuit could imperil its entire business model. Counsel was retained on the company's behalf and to achieve a pre-suit settlement. Total payout was USD 3 million.

// Alleged statutory damages for willful infringement could have been in excess of USD 1 billion //

THE INDUSTRY:

SCHOOL BOARD/ EDUCATIONAL INSTITUTIONS

Schooled in extortion

Type of Company: School Board of Education
Total Payout: USD 25K
Coverage Section: Cyber Extortion

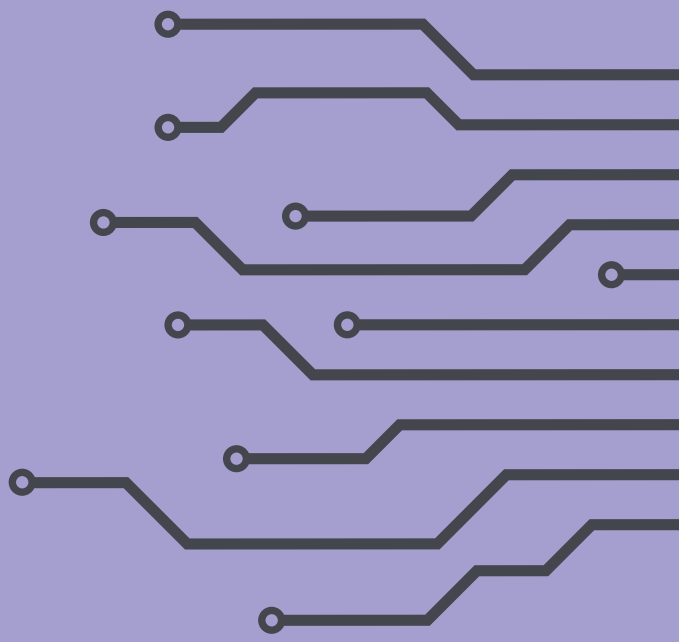
Computers in the school offices of a board of education became infected with ransomware after an employee inadvertently opened malware attached to an email. The ransomware affected multiple computers and a network drive. Coverage was provided under the Cyber Extortion Insuring Agreement. Privacy counsel was retained, who then retained a forensics company to conduct an investigation of the incident. The investigation was able to give the board of education the peace of mind that no data had been exfiltrated and that no additional malware had been introduced into to the network.

Phishing for information

Type of Company: University
Total Payout: Less than USD 25K
Coverage Section: Data Breach and Crisis Management

A university was the target of an email spear-phishing scam. The perpetrator spoofed valid email addresses of two university administrators so that they appeared to be internal messages. The perpetrator then initiated communications with two different university employee recipients, requesting W-2 information and earning summaries for all employees. One employee responded, forwarding attachments of W-2 forms, which resulted in the release of employee names, home addresses, Social Security Numbers, and earnings information. Privacy counsel and a forensic vendor were retained to confirm that the impersonation of employee email addresses originated from outside the university network, and that the event did not involve domain penetration, forced seizure of digital assets, or domain account/password hijacking. Appropriate credit monitoring and notification was also provided to those affected employees.

MAKE YOUR WORLD GO



905_01/2018