Coalition®

Active Insurance in Action

Real stories of cyber claims, risk mitigation, and recovery

Protecting the Unprotected

Introduction

> **Don't click that email!**
>
> **Patch this software immediately!**
>
> **Never use the same password twice!**

Modern businesses have to be mindful of an exhaustive list of cyber risks that grows by the day. Not all risks are created equal in the digital world, but even a minor mistake can result in a major incident.

A cyber event can be a devastating and stressful experience, which means Coalition often sees policyholders on their worst days. Over the years, we've witnessed thousands of incidents, from ransomware to funds transfer fraud and everything in-between. These events impact businesses of all sizes, in every industry, and across all regions — and every time we think we've seen it all, something new pops up to surprise us.

Claims are a fundamental part of insurance. What good is an insurance policy if it doesn't uphold its promise to pay? Yet, cyber risk is unlike other insurance risks. It's detectable and manageable, which means we can work directly with Coalition policyholders to address cyber risk in three distinct ways:

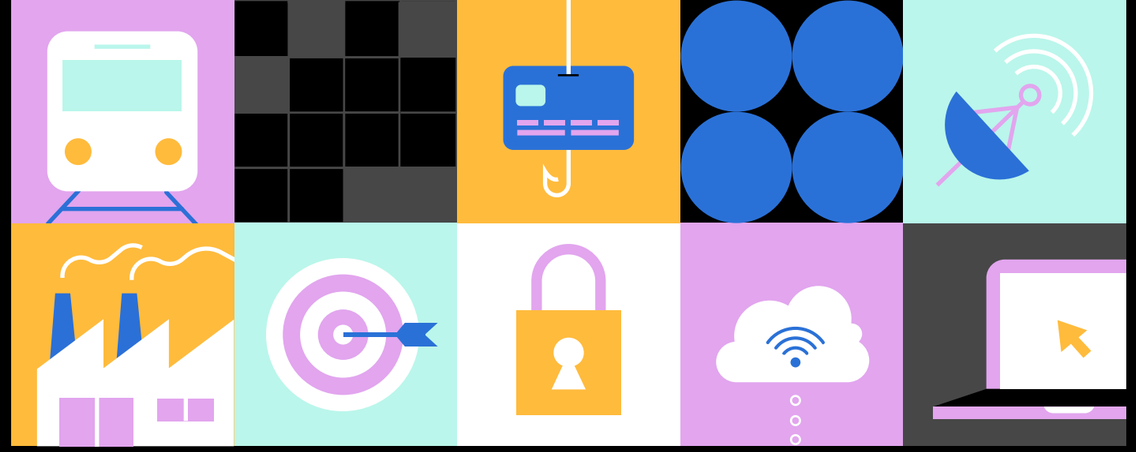
1. Coalition lessens the likelihood of a claim through preparedness and prevention, when possible.
2. Coalition mitigates the impact of a claim by being quick, decisive, and strategic.
3. When all else fails, Coalition policies consistently fulfill a promise to pay.

This is why Coalition exists. We've designed a new kind of protection to keep pace with the evolving nature of digital risks: Active Insurance combines best-in-class insurance and proactive cybersecurity tools to help businesses manage and mitigate cyber risk before it strikes.

We take pride in the reliability and humanity of our claims-handling process, never wanting businesses to feel shame or embarrassment after a cyber event. With a stated mission of "protecting the unprotected," we also strive to ensure that no cyber event leads to a business closing its doors.

No two cyber events are identical, but we believe there are valuable lessons to be learned in every case. This book showcases a compilation of memorable and compelling cyber incidents handled by Coalition. These stories illustrate not only how rapidly cyber risk evolves but also how effectively Active Insurance responds in every situation.

Table of Contents



Construction companies depend on technology to operate, yet many fail to recognize that weak or outdated security controls can increase their cyber exposure. Cyber attackers typically exploit everyday technologies, like email and passwords, as well as unsuspecting employees to gain unauthorized access and pursue malicious activities, underscoring the importance of strong security controls and cyber insurance.

ACTIVE INSURANCE IN ACTION
INDUSTRY SPOTLIGHT

Construction

INDUSTRY
CONSTRUCTION

EVENT TYPE
FUNDS TRANSFER FRAUD

REVENUE
$10M-$50M

EMPLOYEES
26-50

LOCATION
MASSACHUSETTS

Labor Union Avoids Massive Loss After Recovery of Fraudulent $5.5M Transaction

Wiring large sums of money is often a routine part of modern business. But letting your guard down, even for a moment, can welcome a world of financial hardship.

A construction labor union learned this the hard way while managing the investment funds of its members. The union received an email from its pension consultant recommending it make a sizable contribution into an investment fund. The email contained routing instructions and bank details. Days before the contribution was to be made, however, it received another email — only this email came from a different sender and included different information.

Unbeknownst to the union, a threat actor had gained access to its email account and spotted the initial email from the consultant. The threat actor then spoofed the second email, prompting the union to wire $6.4 million to a fraudulent account. The errant transaction went unnoticed for more than a week, until the intended recipient notified the union it had not yet received the money.

Working closely with government agencies, Coalition helped track the stolen money to an overseas bank account in Hong Kong. Nearly $5.5 million was frozen, diverted to a secure account, and eventually seized by U.S. law enforcement.

The union immediately contacted Coalition to file a claim and also filed reports with the FBI and its local police department. We quickly began working to trace the wire transfer and launched a forensic investigation of the union's email accounts with Coalition Incident Response. Working closely with government agencies, Coalition helped track the stolen money to an overseas bank account in Hong Kong. Nearly $5.5 million was frozen, diverted to a secure account, and eventually seized by U.S. law enforcement.

After Coalition recovered a majority of the stolen funds, the union was still short about $900,000 — that's when key policy coverages came into play:

- **Funds Transfer Fraud** covered some of the unrecovered losses.
- **Breach Response** covered the full cost of a forensic investigation.

In all, the labor union paid $500,000 in out-of-pocket costs to cover the remaining loss that exceeded its Funds Transfer Fraud limit on its policy — less than 10% of the initial loss.

LESSON LEARNED

Always Review Large Transactions

The threat actor gained email access and waited patiently for a large transaction before making a move, which points to a need for stronger email security controls. However, even after compromise, closer scrutiny of the fraudulent email should have raised suspicion. When performing a wire transfer, Coalition encourages all businesses to perform detailed reviews of all large transactions, including the account and routing numbers, as well as the email addresses of requestors.

INDUSTRY CONSTRUCTION
EVENT TYPE RANSOMWARE
REVENUE $100M+
EMPLOYEES 1-25
LOCATION TEXAS

High-Profile Client Requires Strict Protocol Following Data Theft

Ransomware is more than just a type of malware. It's a criminal business model that allows threat actors to profit by holding their victim's data hostage.

The day started like any other for a southwestern construction company. But when the IT director discovered its systems were inaccessible and files were encrypted, the business was confronted with the unimaginable: ransomware.

Forensic investigation determined the threat actor compromised a virtual private network used to facilitate remote access. Fortunately, the business had backups of its essential data and worked through the night to successfully restore systems in enough time for employees to resume work with minimal impact. Because the backups were deemed viable and unaffected by the ransomware, we advised the construction company that there was no need to pay the ransom for a decryption key. Instead, one of our forensic vendor partners installed an Endpoint Detection and Response (EDR) solution to monitor the systems and prevent reinfection.

After the company examined the exfiltrated data, breach counsel helped the company notify and set up credit monitoring for an estimated 850 current and previous employees who were impacted by the data breach.

An investigation revealed the threat actor exfiltrated more than 60,000 documents, which needed to be manually reviewed to determine if they contained protected information. Due to one high-profile client, the U.S. Department of Defense (DOD), the company had to follow stringent protocol and file a notification directly with the DOD. The company was also required to work with highly specialized counsel to protect the confidentiality of controlled unclassified information.

After the company examined the exfiltrated data, breach counsel helped the company notify and set up credit monitoring for an estimated 850 current and previous employees who were impacted by the data breach — and one key coverage helped tremendously:

- **Breach Response** covered numerous costs related to incident response, breach notification, and credit monitoring, including $43,000 for data mining.

Overall, the construction company paid $5,000 to cover its self-insured retention, while its policy covered the remaining $106,000.

LESSON LEARNED

Create a Detailed Incident Response Plan

Ransomware attacks often involve encrypting or deleting data stored on a business network. However, threat actors are increasingly opting to simultaneously exfiltrate data, transfer it to their external servers, and threaten its release if the ransom is not paid. A well-documented incident response plan in place before an incident occurs is essential and must include specific steps for dealing with data breaches and cybersecurity controls designed to reduce the likelihood and impact of a breach.

Education

Schools and educational organizations face a growing number of cyberattacks due to their reliance on technology, including online learning platforms and communication tools. This dependency creates vulnerabilities that can be exploited by cyber criminals to disrupt operations and compromise the availability of critical resources for both students and educators. Attackers may attempt to breach systems to access sensitive data, such as student records, Social Security numbers, and financial information, which is why educational institutions must prioritize cybersecurity measures to create a safe and secure learning environment.

Breach Response Coverage Empowers School Investigation Into Potential Data Compromise

Cyber events are often perpetuated by nameless, faceless threat actors on the internet. But they can also be carried out by people in one's immediate proximity.

A grade school became suspicious about a former employee and worried his actions might threaten the security of students and employees. The employee had been terminated, but the school believed he may have damaged property or stolen information prior to departure.

Using security camera footage, the school discovered the former employee had walked around the campus, plugged a USB device into various classroom computers, and accessed other areas he typically wouldn't have entered. The school also reported that the rogue employee used a mobile hotspot to broadcast vulgar Wi-Fi network names, raising alarm that the former employee had gained unauthorized access to the school's network.

INDUSTRY
EDUCATION

EVENT TYPE
INSIDER THREAT

REVENUE
$5M-$10M

EMPLOYEES
51-250

LOCATION
COLORADO

The school reported the incident to Coalition two months after the employee was terminated, and we immediately contacted the school to gather more details and investigate the issue. Because the students are all minors, the school expressed concerns about privacy issues relating to their Personally Identifiable Information, which could require notifications and lead to legal action.

Our team brought in breach counsel, and the school selected Coalition Incident Response (CIR) to investigate the incident. Following a thorough investigation, CIR found no improper access to the school's systems and determined that all of the files he downloaded were legitimate and work-related. Here's how one key coverage helped the school:

- **Breach Response** covered the costs of breach counsel and CIR investigation.

The school paid its $2,500 retention for coverage to kick in, and its policy covered the remaining $22,000.

Early intervention increases the likelihood that Coalition is able to mitigate damage, often at no cost to the policyholder.

LESSON LEARNED

Don't Wait to Report Suspicious Activity

The school was fortunate that the former employee's actions didn't result in harm, but the suspicious behavior could have been reported sooner. Had the actions proven to be damaging, any hesitation on the school's end could have created additional liability. Businesses should always report suspicious activity immediately. Early intervention increases the likelihood that Coalition is able to mitigate damage, often at no cost to the policyholder.

INDUSTRY EDUCATION

EVENT TYPE FUNDS TRANSFER FRAUD

REVENUE $10M-$50M

EMPLOYEES 1-25

LOCATION FLORIDA

Threat Actor Spends Months in Compromised Inbox Before Intercepting $1.3M Wire Transfer

Cyber events aren't always instantaneous. Attackers may opt to gather information and wait patiently for the right time to pounce, usually for large sums of money.

After sending a routine payment to a business partner, the finance director of an early childhood education program started noticing unusual email activity. Numerous employees reported receiving emails requesting gift cards. More importantly, the school never received the typical email confirmation that its monthly payment had been received. Something was off, so the director contacted Coalition.

We immediately launched an investigation with support from Coalition Incident Response (CIR). After identifying a compromised email account, changing its password, and forcing a global password reset, CIR began looking into the unconfirmed payment. The director had actually initiated two separate six-figure transfers, totaling $1.3 million, which CIR confirmed never made it to the intended destination.

CIR determined a threat actor had compromised the finance director's email account four months prior to the funds transfer fraud (FTF) event. But instead of attacking immediately, they waited patiently, searching the inbox for information related to payments and bank accounts. The threat actor also spoofed the school's email domain and set up inbox rules that would automatically forward legitimate emails to the director's junk folder. Lastly, they sent a fraudulent email to the finance director, posing as a business partner, with instructions to update their on-file banking information.

The money may have made it to the threat actor's bank account, but it wouldn't remain there for long. In coordination with government agencies, Coalition filed a report to freeze the stolen funds and stop them from being transferred. CIR also put in a takedown request to remove the fraudulent domain, which would prevent future fraudulent emails. In the end, we were able to successfully recover all but $500 of the stolen money — and here's how coverage responded:

- **Breach Response** covered costs related to incident response, including breach notification and credit monitoring for individuals whose data was compromised.

In the end, the school paid $25,000 toward its self-insured retention, which covered all of the costs related to the FTF event.

LESSON LEARNED

Beware of Changes to Banking Information

The best way to prevent an FTF event is to implement and follow best practices when performing large transactions. In this instance, the email request to update banking information is what enabled the fraud. Businesses rarely change their banking information, so this type of request should raise a red flag. If a vendor says it's updating banking information, always call a trusted person at the company using the last-known phone number to make sure the request is legitimate. Never use a phone number provided in the requesting email because it could be associated with a threat actor.

Financial Services

Businesses in the financial services industry are attractive targets for cyber criminals due to the vast amount of data they handle and the types of transactions they facilitate. Direct access to financial records, Social Security numbers, and other types of sensitive data puts the industry at increased risk of experiencing a cyber attack. Whether threat actors executing sophisticated cyber attacks or disgruntled employees with access to sensitive information, attackers can access and steal sensitive data, manipulate financial transactions, and even disrupt business systems — all of which can result in significant financial loss, reputational damage, and legal consequences.

INDUSTRY	FINANCIAL SERVICES
EVENT TYPE	RANSOMWARE
REVENUE	$10M-$50M
EMPLOYEES	26-50
LOCATION	TEXAS

Investment Firm Pays Fraction of Initial Ransom Demand to Protect Partner Data

Strong security controls are the most effective and affordable way to combat ransomware, but there are valid reasons to engage in ransom negotiations.

An investment firm knew something was awry. First, a regularly scheduled data backup failed. Then, the firm's antivirus software alerted its IT team about a high-level incident occurring on the primary file server. The final touch was a ransomware note, placed onto the file shares along with several malicious files. The note claimed a threat actor had stolen data and was awaiting contact to discuss the payment of a ransom for its return.

The IT team attempted to log into the firm's backup server but discovered the passwords to the domain administrator and local accounts had been changed. It also tried to disconnect the server from the network, but access was lost due to encryption. Soon thereafter, the firm contacted Coalition to report a claim and launch a forensic investigation.

After the firm engaged with one of our incident response partners, initial contact was made with the threat actor, who demanded $1.5 million to decrypt the environment and delete the stolen data. Hoping to avoid paying the ransom, the firm successfully restored its data from backups and resumed business operations. Everything seemed to be looking up, until a banking partner contacted the firm about a possible leak on the dark web.

The bank saw the firm's name on the dark web in connection with a potential compromise and became concerned about its own customer data leaking. To assuage its partner's worries, the firm quickly changed its stance on paying the ransom and pushed for quick resolution of the matter. Coalition successfully negotiated a $200,000 payment — an 87% reduction from the initial demand — and the threat actor delivered proof that the stolen data was deleted. Here's how key coverages helped:

- **Cyber Extortion** covered the entire ransom payment.
- **Breach Response** covered the cost of a full forensic investigation.
- **Business Interruption** covered the downtime and data restoration costs.

In all, the investment firm paid $10,000 to cover its self-insured retention, and its policy covered the remaining costs, totaling more than $200,000.

Coalition successfully negotiated a $200,000 payment — an 87% reduction from the initial demand — and the threat actor delivered proof that the stolen data was deleted.

LESSON LEARNED

Viable Backups Aren't Ransomware-Proof

Even with viable backups and a successful restoration, the firm opted to pay the ransom and protect its business partners from being impacted by a data breach. In the event of a ransomware attack, having reliable backups can give businesses more options and flexibility, but it won't guarantee a perfect resolution. Even after payment is made and proof of deletion is delivered, copies of stolen data can resurface on the dark web.

Financial Advisor Avoids Need to File Claim Following Clawback of Errant $3.5M Donation

Charitable contributions are a potential payday in the eyes of threat actors. So when large sums are involved, it's safe to say no good deed goes unpunished.

INDUSTRY
FINANCIAL SERVICES

EVENT TYPE
FUNDS TRANSFER FRAUD

REVENUE
$5M-$10M

EMPLOYEES
1-25

LOCATION
NEW YORK

A financial advisor attempted to make a sizable donation to one of its preferred charities but wound up lining the pockets of an opportunistic threat actor. The firm initiated two separate wire transfers totaling $3.5 million, but more than a week passed before it realized the money never arrived at the intended destination.

Following the fraudulent transfers, the firm notified the receiving bank and contacted Coalition. Though outside our recommended 48-hour reporting window for funds transfer fraud (FTF), we quickly started our attempt to recover the money. Meanwhile, the firm's in-house IT team launched an investigation into whether its network had been breached.

Following a forensic investigation by an external vendor, we discovered that the threat actor had intercepted emails between the firm and charity, then changed account information to divert the money. It was also determined that the email compromise did not occur on the firm's network, so it opted not to move forward with breach response services.

One of the keys to a successful FTF clawback is reporting time.

Working closely with government agencies, our team determined that recovery was possible. We jointly contacted the receiving bank and instructed it to freeze the stolen assets. One week later, the bank notified Coalition that all but $405 had been successfully recovered — and because of the high recovery rate, the firm didn't need to proceed with filing a claim with Coalition.

LESSON LEARNED

Prompt Reporting Increases Recovery Odds

One of the keys to a successful FTF clawback is reporting time. The sooner Coalition is able to initiate a recovery effort, the greater our chance of success. As we tell all of our policyholders, the first 48 hours after the fraudulent transfer are the most crucial. Nonetheless, we strongly encourage prompt reporting even if it's outside of the initial two-day window — a multimillion dollar recovery is never out of the realm of possibility.

ACTIVE INSURANCE IN ACTION

INDUSTRY SPOTLIGHT

Healthcare

In an industry where patient confidentiality is paramount, healthcare providers are entrusted to collect, transmit, and store health-related data, as well as personal and financial information. All of this sensitive data is often required to be available digitally, making it a frequent target of cyber criminals. Healthcare organizations must not only protect sensitive patient information but also maintain security and availability of data, as well as lifesaving technology. Even a minor breach or failure can have major cyber implications, potentially hindering the delivery of service and impacting the health and safety of patients.

INDUSTRY HEALTHCARE
EVENT TYPE RANSOMWARE
REVENUE $100M+
EMPLOYEES 1,000+
LOCATION UNITED STATES

Dental Group Restores Data From Backups to Avoid Engaging in Ransomware Negotiation

Digital risk knows no bounds. For businesses with multiple locations, even a single cyber event can spread rapidly with costly and far-reaching consequences.

A nationwide dentistry organization abruptly discovered that nearly 50 of its offices across the U.S. had been hit with a ransomware attack. Each location reported that all of the files on its server had been encrypted.

Upon discovery, the organization's IT department began shutting down its unencrypted servers. All of the impacted servers were kept on separate domains, and the only commonality between them was a managed service provider (MSP) that provided support to each location. After receiving prompt notification about the incident, we helped them engage with breach counsel, as well as one of our panel vendors for incident response.

Fortunately, the organization maintained viable data backups at each location, so it began restoring data at the impacted offices to avoid paying the ransom. However, the organization also experienced a distributed denial-of-service (DDoS) attack during the restoration process. The incident response firm had deployed endpoint monitoring as part of its response to the ransomware attack, which contributed to a quick remediation of the DDoS attack and ensured no further damage was done.

Due to a complicated data restoration process, the organization was unable to operate for an extended period of time. It was also required to send notifications to impacted patients and report the incident to both Health and Human Services and the state attorney general — and that's when key coverages kicked in:

- **Business Interruption** covered five days of downtime and data restoration costs.
- **Cyber Extortion** covered the costs of responding to the ransomware event.
- **Breach Response** covered the cost of patient notification.

In all, the dental organization paid $25,000 to cover its self-insured retention, while its policy covered more than $430,000 in total costs.

When implementing backups, businesses should always maintain at least two sets of data, including one that's completely offline from the primary network.

LESSON LEARNED

Maintain Credible Data Backups

By maintaining credible data backups, the dental organization was able to avoid paying the ransom all together. When implementing backups, businesses should always maintain at least two sets of data, including one that's completely offline from the primary network. Additionally, backups should be updated regularly (daily, weekly, etc.) and tested every three months to ensure viability.

Former Contractor Disrupts Operation After Stealing Devices From Company

Cyber events can render organizations completely inoperable. Business interruption costs can pile up quickly, which is why it's crucial to closely monitor incurred losses.

Hours after a healthcare company terminated a contractor, employees found themselves locked out of the network. The business suspected that the former contractor had taken devices that were critical to the infrastructure of its network and quickly contacted Coalition to help resolve the issue.

We connected the company with breach counsel, and Coalition Incident Response (CIR) launched a forensic investigation. CIR verified that the company's suspicions were correct and that the former contractor was responsible for the security failure. Our team attempted to contact the former contractor about returning the stolen devices, but he did not respond.

INDUSTRY
HEALTHCARE

EVENT TYPE
INSIDER THREAT

REVENUE
$1M-$3M

EMPLOYEES
1-25

LOCATION
NEW YORK

Ultimately, CIR determined the best recovery option was restoration. The company purchased new hardware and worked with a managed service provider (MSP) to install the new devices and upload missing data to help the company resume operations.

The healthcare company claimed it lost more than $3 million in revenue during its downtime but was only able to provide proof of loss for $8,000. After a lengthy discussion, we came to an agreement of $25,000 to settle the business interruption costs. Here's how coverage responded to the claim:

- **Breach Response** covered the cost of CIR forensics investigation and claims counsel fees.
- **Business Interruption and Extra Expenses** covered a portion of payroll and lost revenue during the security failure, as well as the costs of replacing stolen hardware and the MSP's work on restoring the systems.

After the healthcare company paid its $5,000 self-insured retention, its policy covered the remaining $204,000.

LESSON LEARNED

Keep a Detailed Account of All Impacts Related to a Cyber Event

Cyber events can be chaotic, but remaining level-headed is essential to recovery. This includes documenting everything that transpires, before, during, and after an event — it can also be part of a business' incident response plan. Businesses that experience business interruption must keep track of any lost income and be able to provide proof to an insurance carrier for full coverage.

Manufacturing

To operate efficiently and at scale, manufacturers rely significantly on both emerging and legacy technologies. The critical nature of these technologies, however, make them a frequent target of cyber attackers looking to disrupt businesses and capitalize on high-value, often unprotected assets. The manufacturing industry faces increased cyber risks due to the use of operational technology for automation and remote access, as well as interconnected systems, all of which are critical to the manufacturing process. Ransomware attacks can knock these systems offline, causing serious delays, disruptions, and even unauthorized access to sensitive data and equipment, as well as the possibility of physical damage to manufacturing equipment.

Manufacturer Facing Double Ransom Denied Decryption Keys After Paying Threat Actors

Choosing to engage in ransom negotiations can be a gamble, as there's no way to know how a threat actor will respond after receiving payment.

A pet supply manufacturer suffered a ransomware attack that prohibited the business from being able to ship and fulfill orders. The company opted to contact a third-party IT vendor to help with regaining access to its encrypted systems. For multiple days, the manufacturer and IT vendor debated contacting a decryption company for assistance, but eventually called Coalition instead.

Worried that the decryption company was potentially malicious, we recommended the manufacturer pursue other options. Instead, the business selected Coalition Incident Response (CIR) to launch a forensics investigation. CIR discovered that the manufacturer was actually double encrypted by two separate ransomware groups.

CIR recommended that the manufacturer restore from data backups, but the company was eager to resume business operations and concerned that restoration would take longer than paying the ransoms. Ultimately, all parties came to an agreement, and CIR negotiated payments to both ransomware groups, totaling more than $127,000.

INDUSTRY
MANUFACTURING

EVENT TYPE
RANSOMWARE

REVENUE
$10M-$25M

EMPLOYEES
51-250

LOCATION
CALIFORNIA

After the payments were delivered, the threat actors did not provide decryption keys, and the manufacturer had no choice but to restore from backups. We hired a firm to help with the restoration process, and the manufacturer regained access to its systems three weeks after the initial attack. Here's how coverages responded:

- **Cyber Extortion** covered the cost of the ransomware payments.
- **Breach Response** covered the costs for breach counsel and forensic investigation.
- **Business Interruption** covered the lost revenue when the manufacturer was inoperable.
- **Digital Asset Restoration** covered the costs for the firm that assisted with restoring from backups.

After the manufacturer paid a $10,000 self-insured retention, the policy paid out $326,000.

Even after a ransom payment is made, threat actors maintain the upper hand, whether it's a promise to provide a decryption key or to delete exfiltrated data.

LESSON LEARNED

Paying a Ransom Isn't a Guaranteed Fix

The goal of any ransomware event is to avoid paying the ransom. However, payment is sometimes the only option. When a business chooses to pay a ransom, it's a choice to trust threat actors. Even after a ransom payment is made, threat actors maintain the upper hand, whether it's a promise to provide a decryption key or to delete exfiltrated data. Businesses are encouraged to maintain data backups that are updated frequently and tested regularly.

Manufacturer Chooses to Pay Ransom Upon Discovering Compromised Data Backups

The decision of whether to engage in ransomware negotiations can be easier if backups are available, but only if the data is maintained and tested regularly.

INDUSTRY
MANUFACTURING

EVENT TYPE
RANSOMWARE

REVENUE
$100M+

EMPLOYEES
251-1,000

LOCATION
OHIO

An industrial machinery manufacturer had its systems encrypted by an advanced ransomware group. As soon as it encountered the ransom note, the manufacturer reached out to Coalition and selected Coalition Incident Response (CIR) to lead the forensics investigation and restoration process to get back to business as soon as possible.

CIR deployed endpoint monitoring and initiated response efforts in less than four hours, exploring the viability of any data backups. The manufacturer hoped to use its backups to restore data and resume operations without paying the threat actors. The company maintained backups across two different cloud technologies, but more than half of the data in one cloud repository had been compromised and encrypted.

Unable to fully resume necessary operations, the manufacturer also became worried that data with client information might be leaked by the threat actor. After careful consideration, all parties agreed to enter negotiations. The threat actor initially demanded $1.5 million, but CIR successfully negotiated the final payment down to $235,000. Once payment was received, the threat actor provided the decryptor and confirmed with evidence that it had deleted the stolen files.

Ultimately, CIR was unable to determine a definitive root cause of the ransomware attack due to a lack of logs maintained by the systems. However, CIR suspected that it was likely a breach from the manufacturer's virtual private network firewall because it showed evidence of unauthorized access. Here's how the manufacturer's coverages responded:

- **Cyber Extortion** covered the cost of the ransomware payment.
- **Breach Response** covered the costs for breach counsel and CIR.

All in all, after a self-insured retention of $25,000, the manufacturer's policy covered more than $900,000 in costs related to the claim.

LESSON LEARNED

Follow the 3-2-1 Data Backup Rule

Even though the manufacturer had data backups, they were not properly segregated from its network and, thus, were encrypted during the ransomware attack. When it comes to maintaining data backups, we recommend following the 3-2-1 Rule. First, maintain three copies of critical business data (one original, two backups). Next, ensure both backups are stored on two different media types to ensure one failure doesn't destroy both copies. Lastly, always store one copy of the backups at an offsite location so it can't be accessed and encrypted.

Nonprofit

Nonprofit organizations face unique cyber risks due to their handling of sensitive individual data and reliance on donations. The financial and personal data typically possessed by these organizations make them an attractive target for attackers seeking to exploit the valuable data for monetary gain. Nonprofits also often have limited resources and tight budgets, which can hinder their ability to invest in comprehensive cybersecurity solutions and respond to cyber threats effectively.

A cyber attack targeting a donation system or website can severely impact a nonprofit's ability to raise funds and even expose donors to becoming victims of scams or fraud. Cyber incidents involving technology, like client intake or case management systems, could expose sensitive data and lead to costly data breaches, not only damaging the reputation and credibility of the organization but also resulting in significant financial losses.

Nonprofit Stuck With Exorbitant Bill After Cryptojacking Event Went Unnoticed for Weeks

Cyber events aren't always obvious, and costs may not accrue all at once. Threat actors can be stealthy, siphoning away small amounts that add up over time.

A nonprofit organization experienced a cryptojacking event for nearly two months before realizing it had been breached. First, the threat actor compromised its cloud computing platform. But instead of stealing sensitive data or disrupting services, they used the account to mine cryptocurrencies on the nonprofit's dime.

Eventually, the organization noticed the usage rate and invoices for services were much higher than usual, but the damage had been done by that time. Upon discovery, the nonprofit immediately shut down the account that had been used in the breach and removed all of the resources associated with the cryptojacking activity. They alerted the platform provider's fraud and security team, then contacted Coalition to initiate a claim.

INDUSTRY
NONPROFIT

EVENT TYPE
CRYPTOJACKING

REVENUE
$50M-$100M

EMPLOYEES
251-1,000

LOCATION
UNITED KINGDOM

Our team investigated the attack and calculated the impact based on the nonprofit's typical usage rates across multiple billing cycles. We determined the threat actor consumed thousands of dollars worth of computing resources by deploying six machine learning clusters. Factoring in additional costs, the total loss amount was more than $48,000 — but one key coverage helped immensely:

- **Service Fraud** covered a significant portion of the losses due to cryptojacking.

Ultimately, the nonprofit paid $24,000 to cover its self-insured retention, and its policy covered the remaining $24,000.

Businesses should implement a process for routine monitoring of digital assets, including spending and usage rates, and establish baseline numbers to help identify changes and anomalies.

LESSON LEARNED

Closely Monitor Usage of Digital Assets

The fact that the threat actor was able to breach the cloud computing platform points to a potential need for stronger remote access controls. Nevertheless, cryptojacking events underscore the importance of remaining vigilant and hyper-aware of how resources are being deployed. Businesses should implement a process for routine monitoring of digital assets, including spending and usage rates, and establish baseline numbers to help identify changes and anomalies.

International Nonprofit Faces Data Privacy Fallout Following Widespread Software Breach

Businesses that operate in multiple countries must stay in compliance with their respective laws and regulations regarding data privacy issues.

An international nonprofit organization was one of the thousands of organizations impacted by a zero-day vulnerability in a popular file-transfer tool. More than 600 unique files related to individuals from the United Kingdom, United States, Canada, Australia, Germany, and the Netherlands were exfiltrated in the event. Due to concerns about legal obligations and other regulatory requirements, the nonprofit contacted Coalition for assistance.

Coalition Incident Response (CIR) quickly launched a forensics investigation to review the extent of the event, as the compromised data included donor names, addresses, credit card numbers, phone numbers, email addresses, and bank account details. At the same time, we established breach counsel in each impacted region to review regulations and affected data.

INDUSTRY
NONPROFIT

EVENT TYPE
DATA BREACH

REVENUE
$50-$100M

EMPLOYEES
51-250

LOCATION
WASHINGTON, D.C.

CIR determined that the threat actor's activity was limited to the server running the file-transfer software and found no evidence of lateral movement or additional malicious software on other systems. CIR's findings were also consistent with other organizations impacted by the zero-day vulnerability and didn't require extensive restoration on the nonprofit's end. Here's how one key coverage responded to this data breach:

- **Breach Response** covered the cost of numerous local breach counsel and a full forensic investigation.

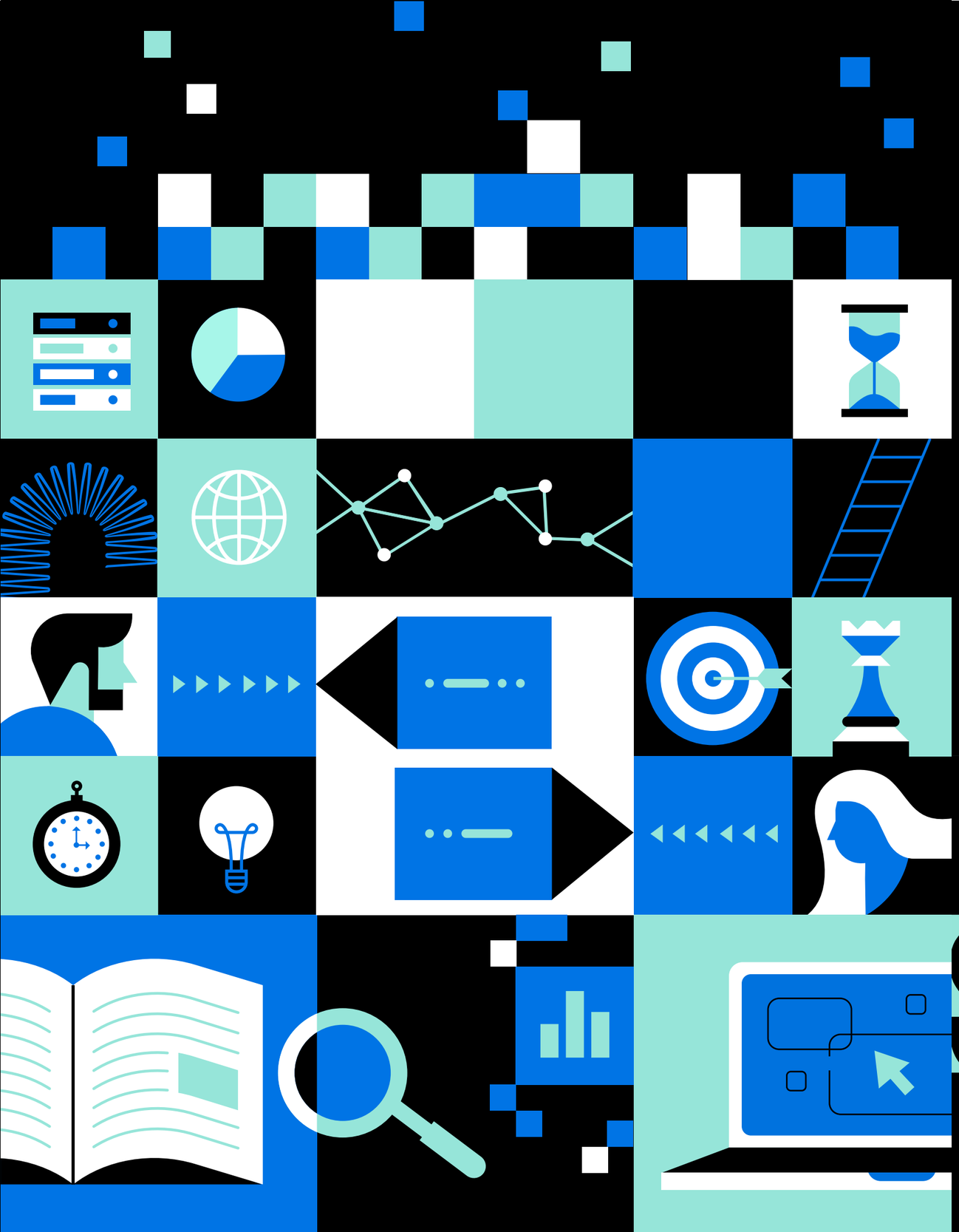
After the nonprofit paid its $25,000 self-insured retention, its policy covered more than $35,000 in costs related to the claim.

While the expectation is that businesses are always in compliance with applicable local regulations, they should also anticipate additional costs when it comes to responding to a cyber event, like a data breach.

LESSON LEARNED

International Businesses Face Increased Scrutiny Over Data Privacy

When data is shared across jurisdictions, it can be subject to different data privacy regulations. International businesses that operate in many regions typically face increased scrutiny over their data privacy practices. While the expectation is that businesses are always in compliance with applicable local regulations, they should also anticipate additional costs when it comes to responding to a cyber event, like a data breach.



Professional Services

Maintaining trust and security is a major concern for the professional services industry. Due to their privileged access to client information and reliance on technology, these businesses prioritize data privacy and cybersecurity to help avoid costly breaches and incidents that could damage their reputation or way of doing business. Operating based on competency, trust, and confidentiality, professional services organizations may be ethically bound to become and remain technologically competent, which includes keeping up with changes in technology or data protection laws that may affect these businesses. A breach or security incident that is handled improperly can have major implications that go beyond direct expenses and cross into cyber liability and, in some cases, professional liability territory.

Law Firm Chooses to Pay Ransom and Protect Client Information Due to Data Theft

When customer data is at stake, the decision to pay may seem like the safer option. Just remember the threat actor has all of the leverage, even after the ransom is paid.

VINDUSTRY	PROFESSIONAL SERVICES
EVENT TYPE	RANSOMWARE
REVENUE	$10M-$50M
EMPLOYEES	51-250
LOCATION	CONNECTICUT

After experiencing a ransomware attack, a law firm took measures into its own hands and attempted to restore its systems from backups. Working with a managed service provider (MSP), the firm thought things were under control until it learned the threat actor had exfiltrated its data and threatened to leak it. That's when the company contacted Coalition.

Initially, the law firm was hesitant to investigate the matter but suddenly felt an urgency to pay the ransom and protect their client data. The firm selected Coalition Incident Response (CIR) to begin the forensics investigation. The threat actor claimed to have stolen more than 100 GB of data, but CIR suspected it could be much more.

To determine what data was exfiltrated and which individuals would need to be notified, CIR engaged the threat actor and requested evidence of the stolen data. Ultimately, CIR negotiated the six-figure ransom down to less than half of the initial demand. The threat actor also provided video confirmation of the files being deleted.

CIR concluded that no additional data had been compromised beyond the amount the threat actor initially claimed was stolen. Here's how the law firm's policy kicked in:

- **Cyber Extortion** covered the entire ransom payment.
- **Breach Response** covered the costs of breach counsel and CIR investigation.

After the law firm paid its $5,000 self-insured retention, its policy covered more than $250,000 in costs related to this claim.

LESSON LEARNED

Every Business Has Its Own Priorities

Ransomware events often come down to a choice between paying the ransom or restoring from backups. Of course, that outcome is dictated by the threat actors demand and the viability of a business' backup data — but underlying priorities can have a significant influence on the final decision. In some cases, businesses opt to pay the ransom in an attempt to protect the data of their customers or partners, even if a full recovery from backups is possible. These situations require close collaboration between the business, claims, counsel, and the carriers to address all coverage implications.

Threat Actors Collect Fraudulent Tax Refunds After Stealing Filings From Accounting Firm

Cyber events can be seasonal and opportunistic. Choosing the right time to attack can help threat actors go undetected and lead to a larger payday.

When engaging with new vendors, businesses should exercise caution and scrutinize the security practices of their partners, particularly those that have access to data and other privileged information.

INDUSTRY
PROFESSIONAL SERVICES

EVENT TYPE
CYBER TAX FRAUD

REVENUE
$1M-$3M

EMPLOYEES
1-25

LOCATION
PENNSYLVANIA

A small accounting firm discovered signs of a cyber event after the tax filings for nearly two dozen clients were flagged as fraudulent and blocked by the Internal Revenue Service. Months earlier, a threat actor had stolen and submitted the filings, rerouting the tax refunds to another account for financial gain. Unaware of any compromised accounts, the firm contacted Coalition to explore the matter.

After selecting to work with Coalition Incident Response (CIR), the firm's tax filing software was investigated to determine if credentials had been compromised or if a threat actor had accessed the firm's actual network. CIR discovered that illegitimate user accounts had been created within the firm's software account and that an unauthorized computer was used to submit the fraudulent tax returns.

To avoid detection and bypass administrative permissions, the threat actor created a lookalike domain and email address to mimic that of the firm. The firm claimed the software provider should've flagged these actions, while the software provider claimed it sent an email alert — but there was no trace of any such communication.

Ultimately, CIR found evidence of business email compromise but was unable to connect it to the tax fraud due to the amount of time that lapsed between the event and its discovery. While the firm was dismayed that the threat actor was able to operate so freely within the software platform without being noticed, one key coverage came into play:

- **Breach Response** covered the cost of forensic investigation, as well as the notification costs and credit monitoring for clients whose data was compromised.

After the accounting firm paid its $2,500 self-insured retention, its policy covered the remaining $31,000.

LESSON LEARNED

Exercise Security Diligence When Partnering With Third-Party Vendors

Businesses that are dependent upon third-party applications and software, especially those that are smaller or with fewer resources, often assume that strong security controls are built into the vendors' products and procedures. When engaging with new vendors, businesses should exercise caution and scrutinize the security practices of their partners, particularly those that have access to data and other privileged information.

Real Estate

Digital innovation in the real estate industry has enabled faster transactions, precise property searches, and more efficient client communications. However, these advancements have introduced new risks, as attackers are increasingly targeting the sector to exploit weaknesses in IT infrastructure and data security protocols. With access to a wealth of personal and financial data, real estate professionals must be mindful of how the technologies they depend on daily can be compromised and the data privacy issues associated with cyber breaches. If an attacker gains unauthorized access to sensitive information, such as property details, contracts, or client data, it can lead to costly fines, significant reputational damage, and loss of clients.

INDUSTRY
REAL ESTATE

EVENT TYPE
FUNDS TRANSFER FRAUD

REVENUE
$1M-$3M

EMPLOYEES
1-25

LOCATION
CALIFORNIA

Property Manager Wires $180K to Threat Actor Due to Compromised Vendor Invoice

A threat actor was able to intercept emails sent to the property manager and manipulate an invoice to include alternative account information.

A business' security is only as strong as its weakest link. Third-party compromise, whether a vendor or client, can still result in direct loss.

A property management company was planning to purchase a new property to expand its portfolio. In preparation for the transaction, the business exchanged multiple emails with its bookkeeper about the details of the deal. When it came time to pay, the property manager wired more than $180,000 to complete the transaction — but as soon as the funds were sent, the fraud was apparent.

The property manager contacted Coalition the following day to report the incident. Upon initial contact, our team immediately contacted the receiving bank and attempted to locate and freeze the stolen funds. Unfortunately, our recovery efforts were unsuccessful.

Upon further investigation, it was determined that the bookkeeper's email account had been compromised. A threat actor was able to intercept emails sent to the property manager and manipulate an invoice to include alternative account information. Because the property manager was unaware of the compromise, the payment went directly to the threat actor's bank account. Fortunately, that's when some of the property manager's key coverages kicked in:

- **Funds Transfer Fraud** covered losses related to the errant payment.
- **Breach Response** covered the costs of investigating the incident.

In the end, after the property manager paid its $12,500 self-insured retention, its policy covered more than $167,000.

LESSON LEARNED

Require Two-Party Reviews When Transferring Money

Although the initial compromise occurred on a third-party system, this event could have been prevented with stronger controls and stricter security practices. Coalition recommends implementing security protocols when performing large financial transactions, most notably requiring two or more people to review and approve all wire transfers.

Real Estate CEO's Business Email Compromise Leads to Customer Data Leak

INDUSTRY
REAL ESTATE

EVENT TYPE
DATA BREACH

REVENUE
$10-50M

EMPLOYEES
51-250

LOCATION
MASSACHUSETTS

Holidays are the perfect distraction for threat actors looking to cause chaos and capitalize on businesses that are busy, stressed, and taking time away from work.

A real estate company was embroiled in a cyber standoff just a few days before Christmas. A threat actor had gained access to the CEO's email account and numerous other applications. After resetting the passwords and enabling multi-factor authentication, the threat actor began sending the CEO threatening messages and demanded payment in exchange for returning the accounts. The company worked with its regular attorney to communicate with the threat actor initially before contacting Coalition a few days later.

The company was connected with breach counsel and selected Coalition Incident Response (CIR) to investigate the cyber attack. CIR discovered a breach stemming from the CEO's email account that enabled the threat actor to move laterally through the real estate company's digital environment. We sourced a data mining company to determine the extent of the breach and identify which documents or systems were impacted.

Meanwhile, CIR worked to regain control of the accounts and expel the threat actor from the company's network. Because personally identifiable information had been accessed, the company needed to notify impacted individuals, so we lined up a vendor to help with notifications and credit monitoring for those affected.

By working with its own attorney before contacting Coalition, the company failed to obtain the written consent required to work with outside forensics or breach coaches. However, the company reasoned that it was an extra expense incurred in order to reduce impacts to their systems and regain access to their accounts. Ultimately, we agreed to cover the attorney's fees. Here's how other coverages came into play:

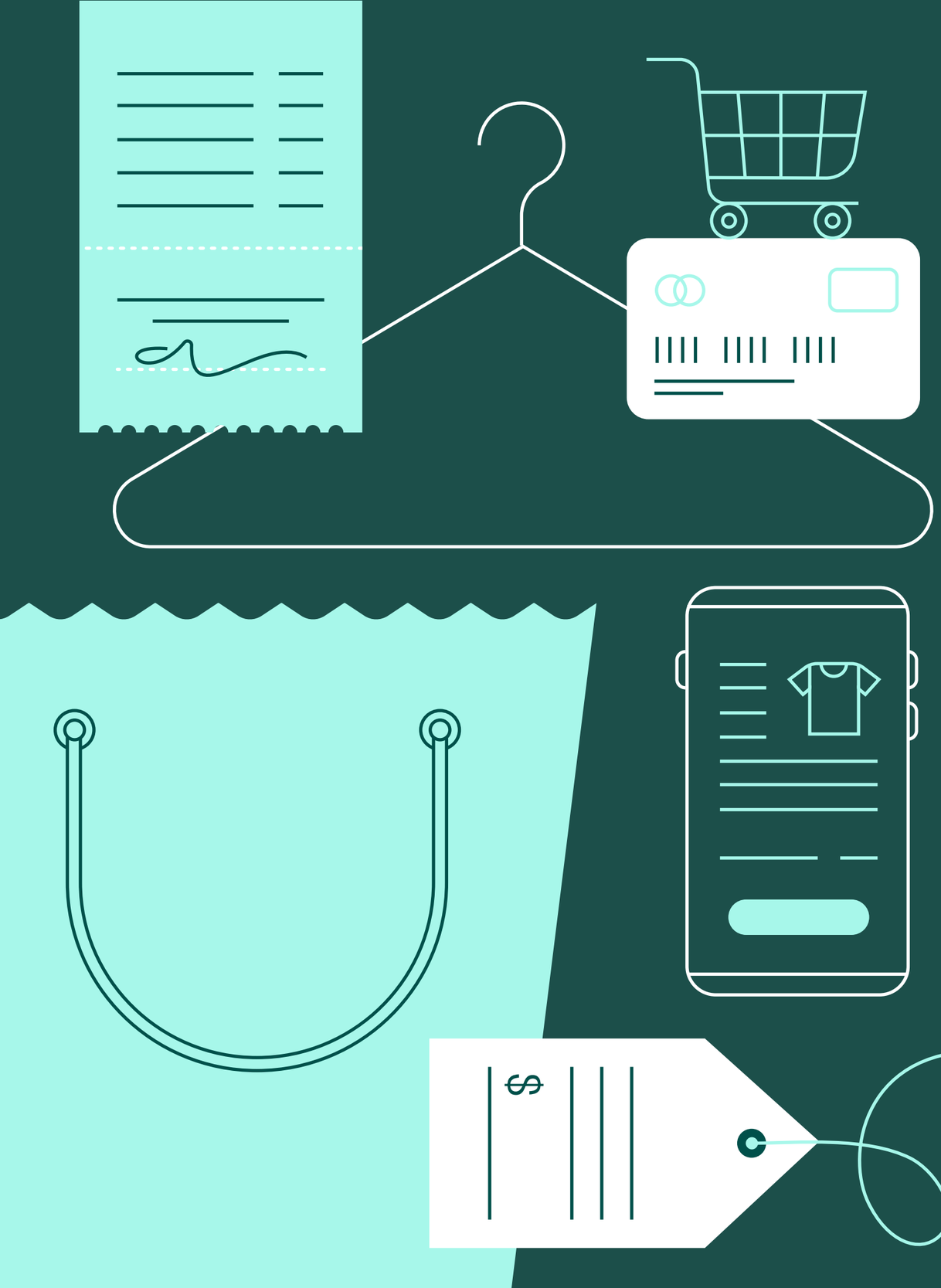
- **Breach Response** covered the costs for breach counsel, CIR's forensic investigation, data mining, notifications, and credit monitoring.
- **Business Interruption** covered the cost of the initial attorney.

After meeting its $1,000 self-insured retention, the real estate company's policy covered $93,000 of costs associated with their data breach.

LESSON LEARNED

Be on High Alert During the Holidays

Threat actors are highly aware of holidays and other events that cause businesses to lower their guards, even for just a few moments. To help protect against seasonal attacks, businesses are encouraged to have employees shut down nonessential internet connected devices and also perform updates before leaving for extended periods of time.



ACTIVE INSURANCE IN ACTION

Retail

INDUSTRY SPOTLIGHT

Retail businesses face numerous cyber risks that can potentially harm their operations and reputation. Cyber criminals routinely target retailers to steal credit card information, which can lead to financial loss, identity theft, and other legal consequences — a risk that's further heightened during online transactions. Retailers often rely heavily on their websites for sales and customer interaction, making them attractive targets for attackers seeking to disrupt services. Ransomware and distributed denial of service (DDoS) attacks can interrupt a retail business' operations, resulting in financial losses, reputational damage, and loss of customer trust.

DDoS Attack Prevents Coffee Company From Operating During Busy Black Friday

Cyber events may seem perfectly calculated to take advantage of businesses in their most vulnerable moments, but they can also be random and inexplicable.

A coffee company had one of its worst nightmares become a reality just as the holiday season began. After noticing something was amiss with its website on Black Friday — perhaps the single-largest shopping day of the year in the United States — the company asked its IT firm to look into the matter. The following day, the company contacted Coalition.

The IT firm determined the coffee company was experiencing a Distributed Denial of Service (DDoS) attack. A threat actor flooded the company's website with visitors to disrupt operations and, presumably, to leverage the attack into a ransom payment. However, a ransom was never demanded, and the attack ceased after three days.

INDUSTRY
RETAIL

EVENT TYPE
DDoS

REVENUE
$50M-$100M

EMPLOYEES
51-250

LOCATION
WASHINGTON

A threat actor's path to a payday is fairly obvious for ransomware and funds transfer fraud, but not every cyber attack is straightforward.

Interestingly, the DDoS attack paused between midnight and 6 a.m. every day, but the coffee company still suffered nearly three days of interrupted sales during one of the busiest weekends of the year. By comparing prior years of Black Friday weekends, we were able to work with the company and estimate how much money it lost as a result of the DDoS attack. Here's how key coverages came into play for this claim:

- **Breach Response** covered the cost of breach counsel and a forensics investigation.
- **Business Interruption** covered the lost revenue and extra expenses for data and site restoration.

After the coffee company paid its $10,000 self-insured retention, its policy covered the remaining $188,000.

LESSON LEARNED

Not Every Cyber Attack Has a Clear Motive

A threat actor's path to a payday is fairly obvious for ransomware and funds transfer fraud, but not every cyber attack is straightforward. The fact that the cyber event occurred during Black Friday weekend suggests it was intended to inflict damage, but this DDoS attack is a good reminder that motive isn't always apparent. Regardless of intent, Coalition always encourages businesses to be on high alert during holidays and other times of year when people are often preoccupied.

INDUSTRY RETAIL

EVENT TYPE DATA BREACH

REVENUE $50M-$100M

EMPLOYEES 251-1,000

LOCATION TEXAS

Breach Compromises Credit Card Data of More Than 13,000 Restaurant Customers

Businesses with access to large amounts of financial information must be vigilant in their protection efforts, as even the smallest mistake can lead to a costly leak.

After receiving an unexpected phone call, a restaurant group learned it was experiencing an ongoing cyber attack. But it wasn't a threat actor on the other end of the line — it was the Federal Bureau of Investigation.

The FBI notified the business that data from four of its servers had been compromised: three corporate servers and one restaurant server containing customer credit card information. Considering it processes more than $8 million in credit card transactions annually, the restaurant group immediately notified Coalition in hopes of minimizing the damage and exposure.

Within 48 hours, incident responders utilized script collectors to identify how the threat actor was accessing the servers and what data was impacted. Coalition's breach response partner ejected the threat actor and reclaimed control of the network. Unfortunately, even with quick action, the breach compromised customers' credit card data.

Our investigation determined the incident began with a simple phishing email. Once the threat actor entered the network, they elevated their own credentials to access other accounts. With unfettered access, the threat actor was able to compromise credit card data for more than 13,000 individuals. The data breach eventually resulted in a class-action lawsuit, but one key coverage reduced the business' cost to a fraction of the overall amount:

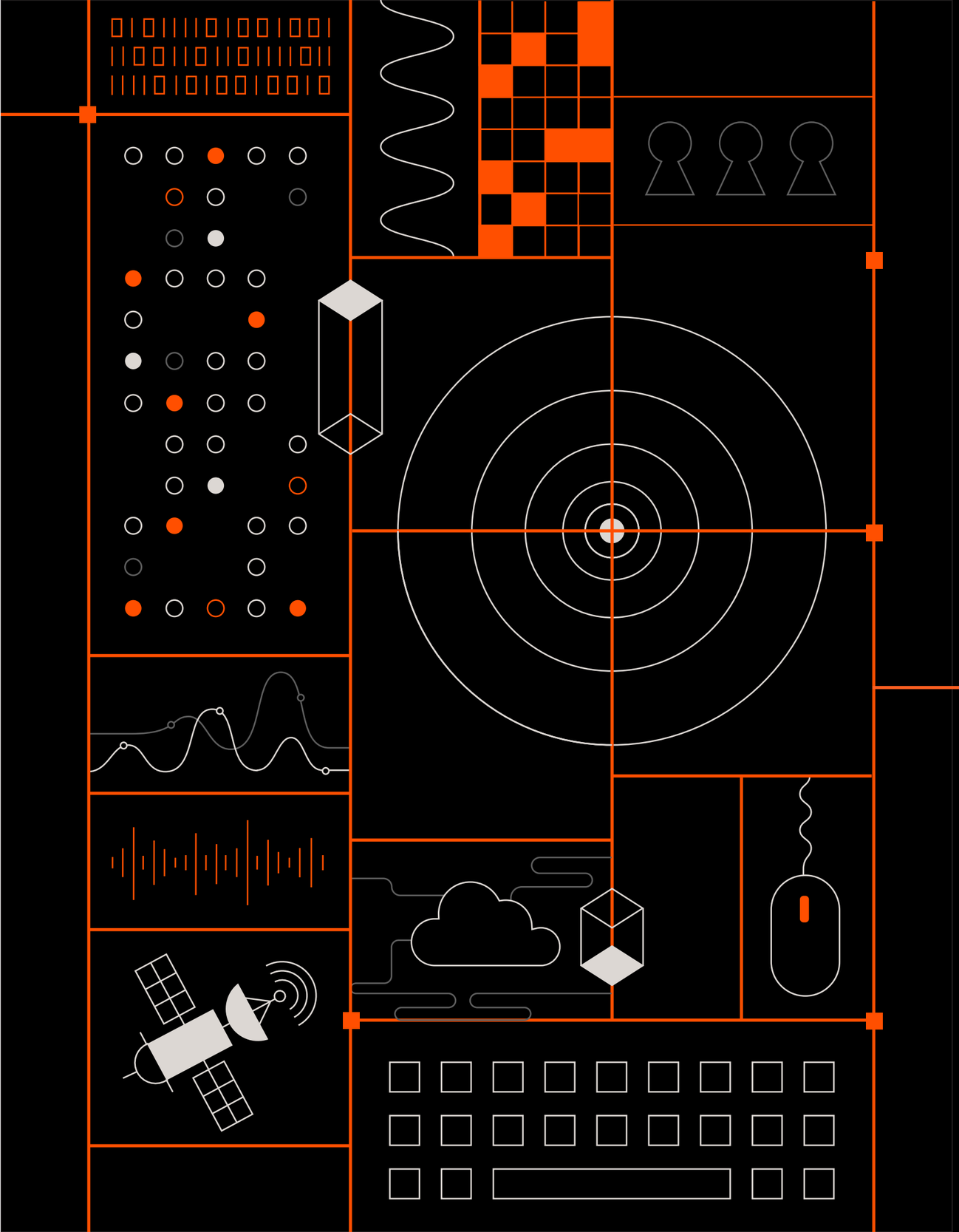
- **Breach Response** covered the costs of notifying customers about the data breach, as well as costs related to litigations, depositions, and negotiations during the lawsuit.

In the end, the restaurant group only paid $21,000 out of pocket, while its policy covered the rest of the $3 million claim.

LESSON LEARNED

Segregate Networks and Require Multi-Factor Authentication

Without the right security controls in place, one errant click on a phishing email can quickly transform into a multimillion dollar data breach. Network segregation can limit the impact of intrusion by making it significantly more difficult for a threat actor to locate and gain access to sensitive information. Similarly, enforcing multi-factor authentication for administrative access to internal networks can make initial entry significantly more difficult.



INDUSTRY SPOTLIGHT

Technology

ACTIVE INSURANCE IN ACTION

Technology businesses face cyber exposures due to the data they possess and the technologies they use to support operations. They often store and process sensitive information on behalf of clients and may have direct access to customer applications and systems, making them prime targets for cyber criminals.

Many technology businesses may also rely on third-party software and services to build their products, which can expose them to additional risks if the components have vulnerabilities. These companies typically have a broad attack surface due to their complex and interconnected IT infrastructures, creating a greater opportunity for adversaries to exploit vulnerabilities, gain unauthorized access, and disrupt services.

Environmental Technology Company Duped in Highly Coordinated Social Engineering Scam

A well-orchestrated scheme can weaponize a business' attentiveness and use it against them, especially when large amounts of money are involved.

INDUSTRY
TECHNOLOGY

EVENT TYPE
FUNDS TRANSFER FRAUD

REVENUE
$5M-$10M

EMPLOYEES
1-25

LOCATION
CALIFORNIA

An environmental technology company found itself entangled in a web of deception and fraud with six-figure implications. It all started when a company executive received text alerts and a follow-up phone call from the bank about authorizing a wire transfer and requests to add new users to the bank account. The executive denied the requests, providing authentication codes to verify authorization in the process.

After conducting an internal investigation, the company discovered the executive was communicating with a threat actor and had never been in contact with the bank. During that time, a second threat actor was on the phone with their bank, impersonating an employee. Working in tandem, the two threat actors manipulated the bank into sending a security code to the executive for verification, which they then relayed back to the bank to gain access to the company's bank account and authorize transactions.

More than two months passed between the initial compromise and its discovery. In that time, the threat actors initiated five fraudulent wire transfers totaling nearly $476,000. The company contacted Coalition to report the incident, but our recovery efforts were unsuccessful due to the lapse in time. Fortunately, one key coverage came into play:

- **Funds Transfer Fraud** covered the full loss amount.

After the company paid its $5,000 self-insured retention, its policy covered the remaining $471,000.

LESSON LEARNED

Establish and Follow Protocols for Large Transactions

Even highly coordinated social engineering scams can be combated if businesses enact strict protocols when performing large wire transfers. Coalition recommends implementing a multi-step process for verification of requests, which includes calling the last-known valid phone number of the party requesting the transaction and requiring at least two-party reviews and approvals for transferring funds.

Technology Company Unable to Operate for Weeks Following Ransomware Attack

INDUSTRY TECHNOLOGY

EVENT TYPE RANSOMWARE

REVENUE $50M-$100M

EMPLOYEES 1,000+

LOCATION NEW YORK

Downtime is often just as expensive and disruptive as a ransom payment. An incident response plan can help businesses quickly bounce back after a cyber event.

A transcription service company experienced a ransomware attack that rendered their business inoperable. The company wasted no time and immediately contacted Coalition to file a claim, selecting Coalition Incident Response (CIR) to respond to the incident.

Due to the nature of its business and clientele, the company was eager to engage with the threat actor and pursue the most expedient recovery option available, in hopes of minimizing downtime. With support from CIR, our claims team cautioned the company against immediately opting to pay a ransom. Instead, we sought to explore all recovery options, including any available data backups.

Having been impacted by the ransomware, the backups were deemed unusable. However, the company was able to create a workaround to recover its data — the problem was that the recovery process would take at least one week. Upon careful consideration, all parties agreed to engage in negotiations with the threat actor.

The threat actor initially demanded $2.5 million, but CIR successfully negotiated it down to $1 million. After a thorough investigation, CIR was unable to identify a phishing email or any unauthorized entry, though sensitive data was compromised as a result of the incident. Here's how the company's coverage responded:

- **Cyber Extortion** coverage covered the cost of the ransom payment.
- **Business Interruption** covered lost revenue while the business was inoperable.
- **Breach Response** covered the cost of legal fees, CIR fees, and data mining.
- **Crisis Management** covered the costs of a public relations firm to communicate with third-party vendors and customers.

After the technology company paid its $100,000 retention, its policy covered more than $1 million in costs related to this claim.

Having prior knowledge of all mission-critical data, networks, and assets is essential to responding to a cyber event and resuming operations.

LESSON LEARNED

Identify Essential Data and Systems Prior to a Cyber Event

Maintaining viable data backups is a proven strategy for recovering from a ransomware event, but backups can still be damaged during an attack. This is why Coalition encourages all businesses to prepare an incident response plan that documents how to respond during an incident. Having prior knowledge of all mission-critical data, networks, and assets is essential to responding to a cyber event and resuming operations.

Prevent Risk Before It Strikes with Active Insurance

A unified approach to help protect against cyber threats

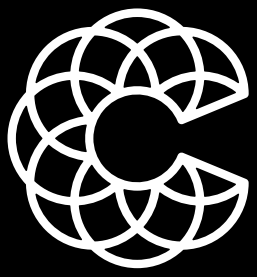
Traditional insurance wasn't built to keep pace with the evolving nature of digital risks. Modern businesses need more than a passive insurance policy — they need an active partner that not only provides support after an attack but also one that can help prevent and mitigate risk before and during an attack.

Active Insurance is the first cyber defense bringing together active cyber risk assessment, proactive protection, expert response, and comprehensive cyber coverage. Coalition pioneered Active Insurance to address the challenges of cyber threats in ways that traditional insurance can't.

How businesses can get the most out of Active Insurance

Our mission at Coalition is to protect the unprotected. As the world continues to digitize, we actively partner with businesses, brokers, and security professionals to help them stay one step ahead of digital risk.

To learn more about Coalition, visit coalitioninc.com.



Coalition®

COALITIONINC.COM

The claim scenarios described here are intended to show the types of situations that may result in claims. These scenarios should not be compared to any other claim. Whether or to what extent a particular loss is covered depends on the facts and circumstances of the loss, the terms and conditions of the policy as issued and applicable law.

Insurance products are offered in the U.S. by Coalition Insurance Solutions Inc. ("CIS"), a licensed insurance producer and surplus lines broker, (Cal. license # 0L76155) acting on behalf of a number of unaffiliated insurance companies, and on an admitted basis through certain carriers. See licenses and disclaimers.

Coalition Incident Response services provided through Coalition's affiliate are offered to policyholders as an option via our incident response firm panel.

44 MONTGOMERY STREET, SUITE 4210
SAN FRANCISCO, CA 94104