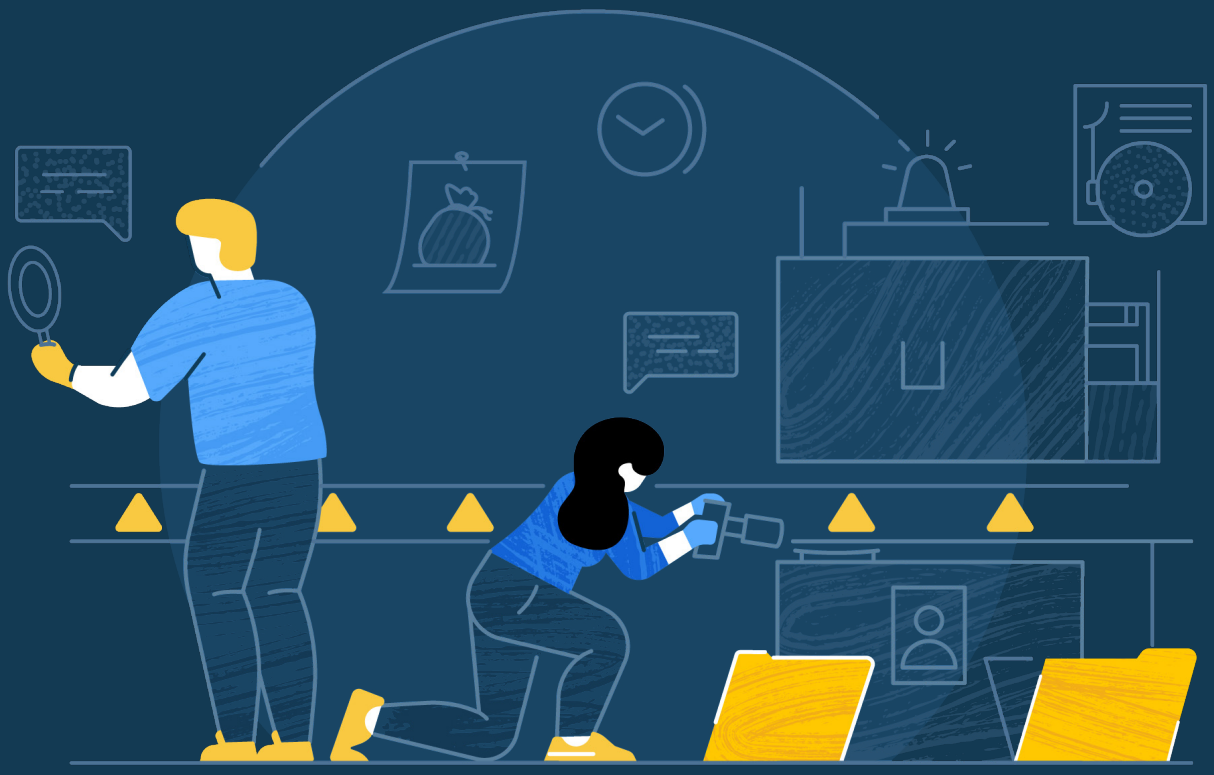
Coalition®

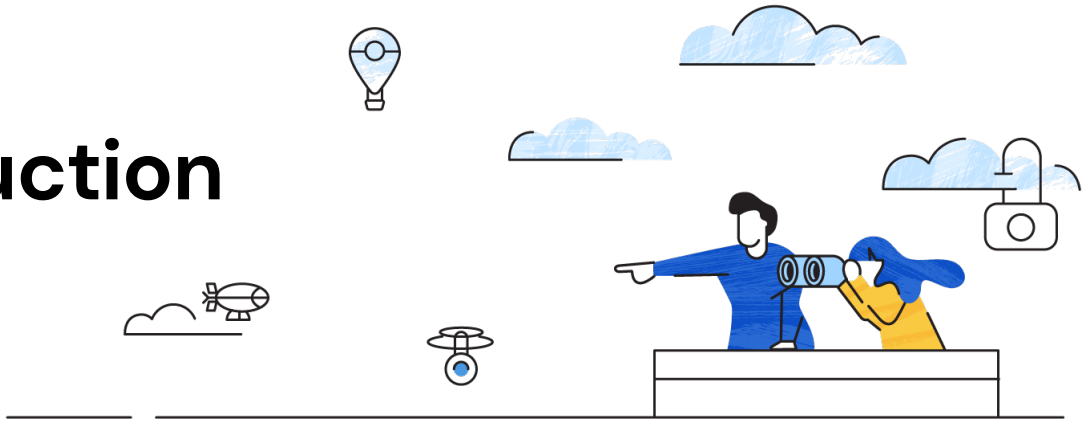
H1 2020

Cyber Insurance Claims Report



coalitioninc.com

Introduction



Coalition serves over 25,000 small and midsize organizations across every sector of the US and Canada. As the fastest growing provider of cyber insurance globally, we have the fortune (and misfortune) of seeing an ever-increasing number of insurance claims. After analyzing our claims data, a few things are clear when it comes to cyber risk:

- **Cyber losses are increasing in frequency and severity.** The broad adoption of technology by organizations across all sectors has created new opportunities for cybercriminals. This trend is only increasing with the changes many organizations have implemented to facilitate remote work during the COVID-19 pandemic, and cybercriminals are actively using this to their advantage. Although the number of cyber attacks hasn't increased dramatically, their rate of success has.
- **Nothing and no one is 100% secure.** Claims were made by small businesses, large businesses, for-profits, and nonprofits — across every industry and despite investments in cybersecurity.
- **The root causes of security failures are largely known and predictable.** The implementation of basic cybersecurity controls could have avoided a majority of the claims and losses reported to us. No-cost and low-cost controls, such as multi-factor authentication (MFA) and routine out-of-band backups would have eliminated a majority of losses experienced.
- **Cyber insurance works.** For each and every claim we processed, cyber insurance went beyond the promise to pay, and to make the insured financially whole. It also played a critical role in helping the insured recover operationally.

Before we dive into the data, a few quick caveats:

- The sample size of reported incidents and claims is still limited in strict statistical terms; we'll continue to regularly update and share our analysis to identify changing trends.
- Our underwriting and risk engineering capabilities are unique among cyber insurance providers, and our claims reflect this. Our policyholders experience fewer claims, on a relative basis, than the average across the market. As a result, we see less of certain claims types than others.
- We collect a *lot* of data. This isn't an exhaustive review of it. If you have any questions, please reach out to us. In the spirit of our mission to solve cyber risk, we'll share what we can.

table of contents

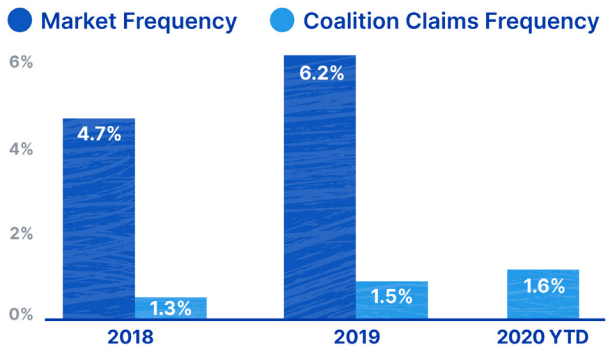
Cyber claims by the numbers

Coalition policyholders experience **less than one-fourth** the frequency of claims as of the rest of the market, due in no small part to our differentiated approach to underwriting and risk management.

Frequency & severity of claims

Our visibility into cyber incidents comes from three main sources. The first and principal source is from our own policyholders when they report incidents and claims to us. The frequency of claims reported to us, calculated as the number of reported claims where a payout was made divided by our earned policy count over the period, hovered under 2%, slightly increasing in 2020. In other words, ~2 out of every 100 companies experienced a cyber incident that resulted in a claims payout.

Coalition claims frequency vs. overall market



** 2020 NAIC data is not yet available*

The second source is data that is shared with us by the National Association of Insurance Commissioners (NAIC). Across the broader US market, the frequency of reported claims by US insurers increased by 32% between 2018 and 2019 from 4.7% to 6.2%, 4x greater than the frequency experienced by Coalition policyholders in 2019.

And finally, the third source of claims data is from the tens of thousands of insurance applications we receive each year in which we ask if an organization has previously reported a cyber insurance claim. Normalizing for time and first-time buyers, we

estimate that approximately 5% of organizations report an incident or claim to their insurance carrier each year in alignment with NAIC data.

It's worth noting that these figures are specific to organizations that purchase cyber insurance (most still do not), and only account for incidents where the organization filed a claim and the losses were above the organization's deductible (or the threshold asked on an insurance application, often $25K). The actual frequency of cyber incidents experienced by organizations is, consequently, higher, with some data sources estimating as high as 1-in-5.

However, whether it's a 1% or 20% chance of experiencing an insurable loss, it can be 100% devastating. In our experience, few companies are prepared, and the losses can be severe — even catastrophic. Claims reported by our policyholders ranged in size from $1,000 to well over $2,000,000 per incident. Those are some big losses, but we were there to support our policyholders in a time of need. Moreover, we planned for it, priced it accordingly, and are ready for the next time an incident happens. This is why insurance exists.

In addition to a rising frequency of claims across the US insurance market, the severity of claims has increased. The average severity of claims reported by Coalition policyholders increased by 65% from 2019 to 2020, in large part driven by the rising costs of ransomware (more details on page 8 of this report).

Together, the growing frequency and severity of claims translate into growing cyber risks faced by organizations of all sizes and in all industries. Cyber insurance claims are among the most frequent insurance claims made by small and medium-sized, and yet a substantial majority remain uninsured.

Claims by industry and size

In case you think claims only happen to certain types and sizes of businesses, think again. Cybercrime, privacy violations, technology failures, and even electronic media wrongful acts hit organizations of all shapes and sizes.

Certain industries, including consumer (retail, hospitality, and food), industrial (energy andmanufacturing), healthcare, and financial services industries are more frequent targets of cyber attacks. While these industry sectors are more frequently targeted by cybercriminals, cyber attacks were observed across nearly every industry segment.

We also observed a higher *frequency* of claims targeting large organizations, who are targeted by cybercriminals more often than smaller organizations. Large organizations (as defined by revenue and employee count) are more likely to be targets of choice, and deliberately targeted by criminal actors in pursuit of sensitive data, financial gain, or both.

Interestingly, while large organizations in our sample (with revenues of $100M-$250M) were 5x as likely to experience cyber claims as compared to smaller organizations, the severity of the losses (meaning, the total insurance payout following the incident) was often well into six figures, regardless

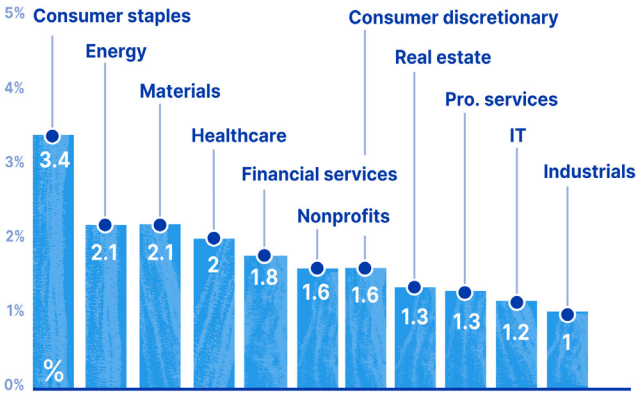
of the organization's size. Losses experienced by small businesses, although less frequent, were disproportionately more impactful. Without cyber insurance, they may well have been existential to the businesses survival. **Can your organization afford to pay for a $2M claim?**

Although it's commonly believed that cyber insurance is only useful if an organization possess or stores credit card data, personally identifiable information (PII), or private health information (PHI), the majority of claims reported to us didn't involve a breach of sensitive data at all. Organizations were no less likely to experience a claim based on whether they possessed sensitive data or not, and irrespective of whether these functions were outsourced to a third party provider.

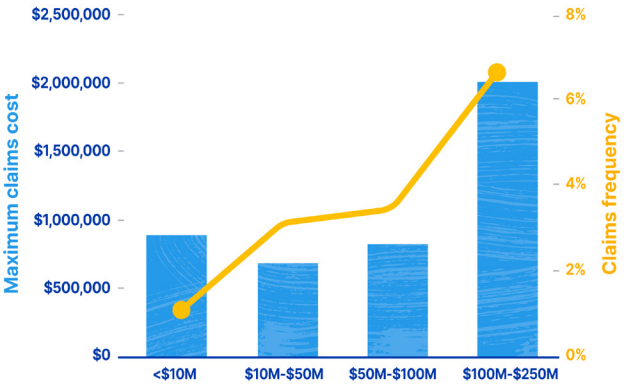
Cyber insurance policies, and cyber threats, have evolved well beyond data breaches to include coverage for fraudulent funds transfers and ransomware, insider threats and technology failures, among many other forms of loss. While data breaches involving sensitive data can be particularly costly, our claims data suggests that losses experienced by organizations perceived to be lower risks, because they don't collect sensitive data, can be equally, if not more, severe and operationally devastating.

What's really illuminating, if not terribly surprising to cybersecurity professionals, is why this is all happening. As much as we pride ourselves on helping our customers when they need us most, we'd much rather help them avoid a loss in the first place.

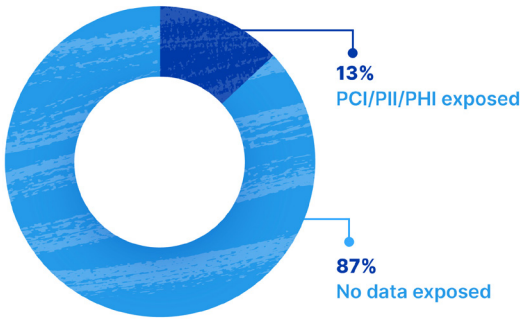
Annual claims frequency by industry



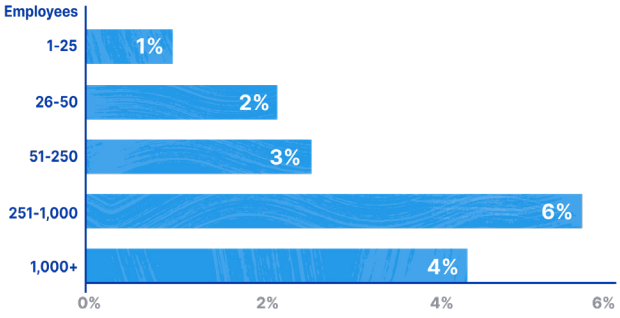
Claims trends by revenue band



Claims involving breaches of sensitive data



Claims frequency by employee count

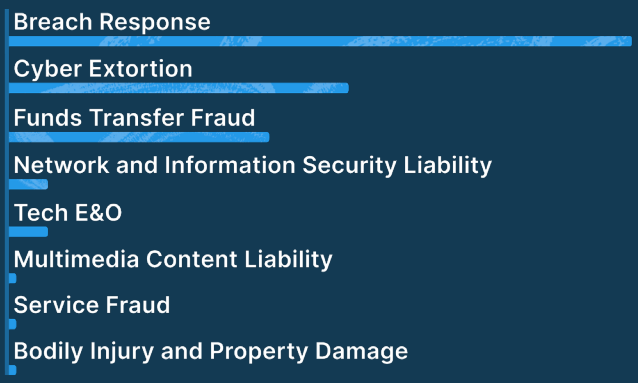


Cyber claims trends

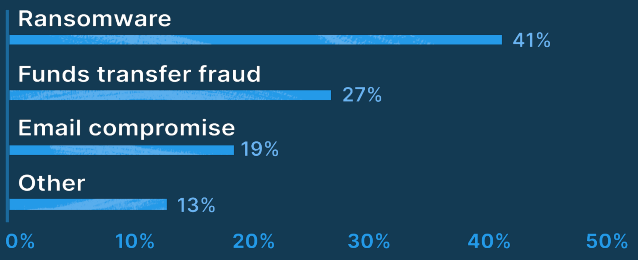
To date, we've classified 35 distinct forms of loss experienced by our policyholders following thousands of reported incidents — all of which are contemplated and covered by our comprehensive cyber insurance policy. However, despite the diversity of loss types, the majority of losses were picked up by three of the coverages on our policy: breach response coverage (which covers forensics and incident response costs, notification costs, etc.), cyber extortion costs (most directly applicable following a ransomware incident), and funds transfer fraud (resulting, largely, from social engineering). These three loss types accounted for 87% of reported incidents and 84% of claims payouts.

Similarly, the types of attack techniques criminal actors used to target our policyholders are also highly concentrated. Phishing, remote access, and social engineering attacks accounted for 89% of all known attack techniques.

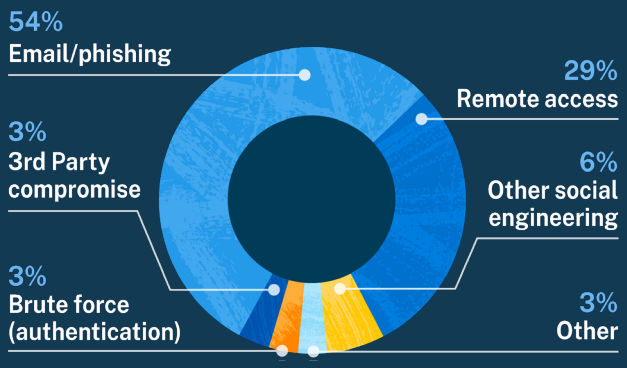
Claims reported by insuring agreement



Most common cyber incidents (% of reported claims)



Percentage of claims by attack technique



The rise of ransomware

Ransomware is taking organizations hostage (quite literally) by encrypting and disabling access to business-critical systems and data until a ransom payment is made. The ransomware business model is arguably the most significant innovation in cybercrime in recent history, and the sophistication of criminal actors is increasing. Traditionally, criminals would hold access to an organization's data hostage, but more recently a number of ransomware groups are now stealing an organization's data prior to encrypting it, and then threatening to publicly expose the stolen data if a ransom is not paid. If you care about access to business systems and data, or keeping your private data private, you very much need to care about ransomware.

Ransomware doesn't discriminate by industry. We've seen an increase in ransom attacks across almost every industry we serve. Organizations that are particularly vulnerable often manage sensitive data, enable Internet-exposed remote access tools (e.g., Remote Desktop Protocol), and use third-party IT providers.

Ransomware incidents tend to also be more severe than other reported cyber insurance claims by a factor of 2.5x. Ransomware attacks often result in significant interruptions to ongoing businesses activities, and the process to recover and restore business operations, even when system backups are readily available, can be complex and expensive.

Organizations without backups, or where the backups were similarly encrypted, face an even longer road to recovery.

Newer strains of ransomware, including DoppelPaymer and Maze, are particularly malicious. While the data exfiltration component of the attack increases the complexity, the additional leverage gained by the criminal actor allows them to demand much higher ransoms. The average ransom demand for Maze ransomware, for example, is 6x the overall average demand.

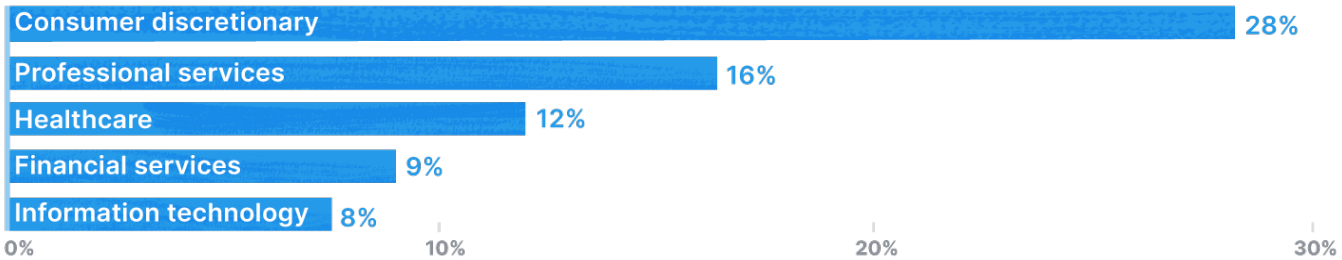
EFFECTS OF COVID-19

We've seen a sharp increase in ransom demands over the past quarter as threat actors have exploited COVID-19 and changes in company operating procedures. Although the frequency of ransomware claims has decreased by 18% from 2019 into the first half of 2020, we've observed a dramatic increase in the severity of these attacks. The ransom demands are higher, and the complexity and cost of remediation is growing. The average ransom demand amongst our policyholders **increased 100%** from 2019 through Q1 2020, and increased another 47% from Q1 to Q2 2020.

47%

Percentage increase in the severity of ransomware attacks from Q1 to Q2 2020

Percent of ransomware claims by industry (top 5)



Case study

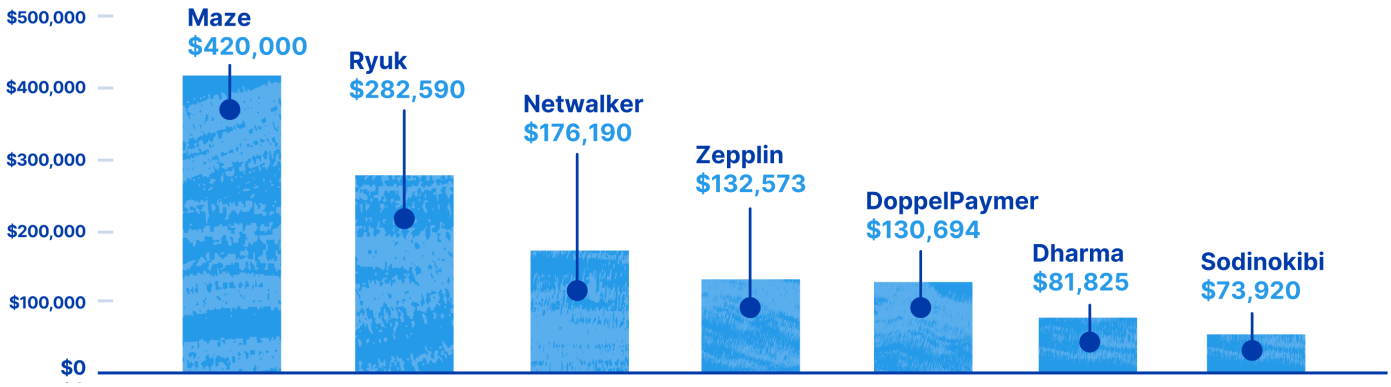
Industry: IT services

Revenue: <$10M

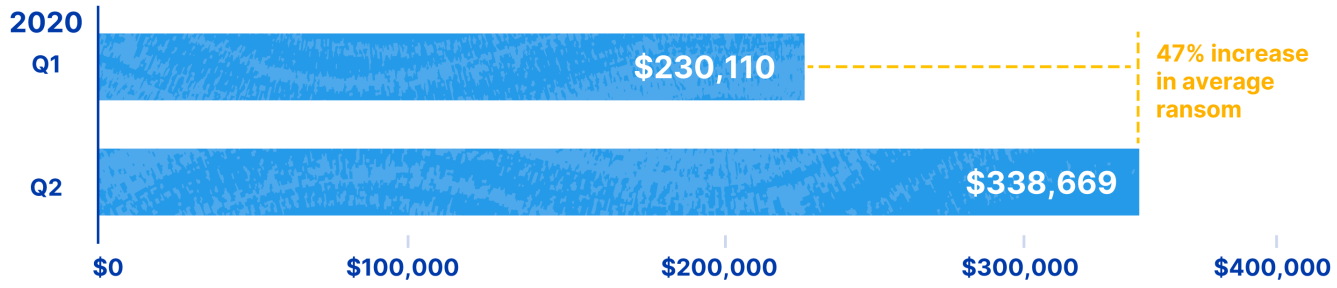
Employees: 26-50

After 25 years of continuous business operations, the business owner of a colocation and IT services firm awoke to discover that all of the company's computer systems and data, including data belonging to the company's customers, had been encrypted in an elaborate ransomware attack. Even worse, the ransomware encrypted the company's backups as well. Unable to afford the 25 bitcoin ransom (at the time, equivalent to roughly $200,000), the company was left with few options. In less than 24 hours a member of Coalition's security team (SIRT) was onsite to facilitate the decryption of the company's data. Total time to resolution was 48 hours from initial compromise. Fortunately, the insured's cyber insurance policy covered the business interruption loss, forensic and data restoration costs, as well as the cyber extortion itself.

Average ransom demand by malware strain



Average ransom demand



The (funds transfer) fraud that drains your bank account

Social engineering attacks resulting in funds transfer fraud, although far less sophisticated than ransomware, are also a leading cause of cyber insurance claims. These attacks typically involve some combination of business email compromise (of the insured or a vendor), email spoofing, and/or invoice manipulation.

Many organizations and their employees believe that email is a secure method of communication, but unfortunately it is not. It can be very difficult, if not impossible, to distinguish between a fraudulent and a real email. Even worse, many businesses have not instituted a process to verify wire instructions received electronically. A single mistake can cost an organization millions.

We observe funds transfer incidents across all industries, though they are particularly common among organizations that handle large sums of money, such as law firms, title companies, tax professionals, and financial advisors.

One unique aspect of funds transfer fraud losses is that frequently, with quick intervention, the funds can actually be recovered. In fact, in more than half of the funds transfer fraud cases reported by policyholders, Coalition's Security & Incident Response Team (SIRT) was able to recover a portion (or all) of the funds lost. In total, we've recovered 84% of all funds lost by our policyholders, and 95% of all funds lost in the first half of 2020.

EFFECTS OF COVID-19

We've observed a dramatic **35% increase** in funds transfer fraud and social engineering claims filed by Coalition policyholders since the onset of COVID-19. Reported losses have ranged from the low thousands to well above $1 million per event.

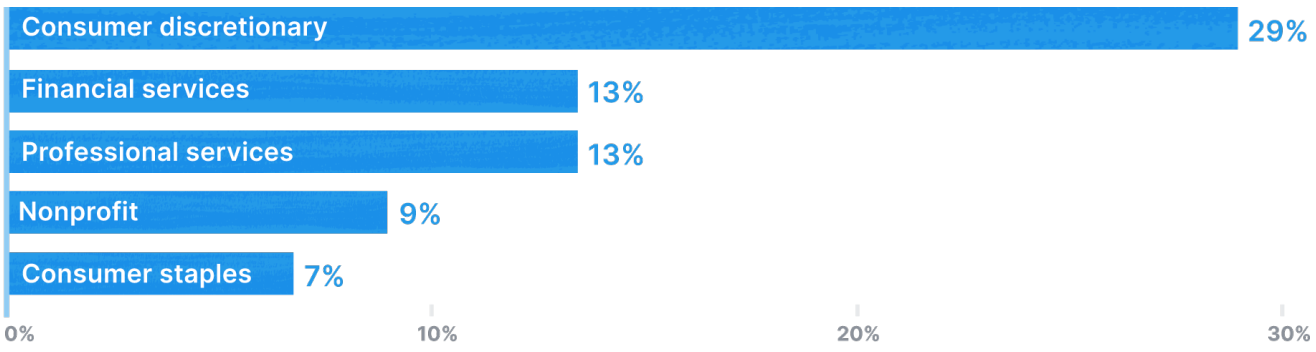
Many organizations have been forced to make abrupt changes to their operating procedures, which threat actors have exploited through targeted campaigns.

35%

Percentage increase in the frequency of funds transfer fraud attacks from 2019 to 2020

The root cause of loss for funds funds transfer fraud incidents incidents include business email compromise, invoice manipulation, and domain spoofing, although social engineering attempts via telephone were also reported.

Percent of funds transfer fraud claims by industry (top 5)



Case study

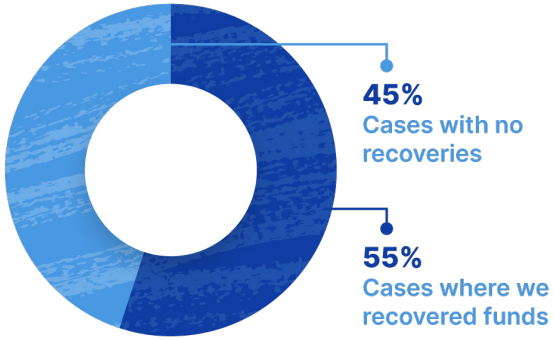
Industry: Nonprofit

Revenue: $10 - $50M

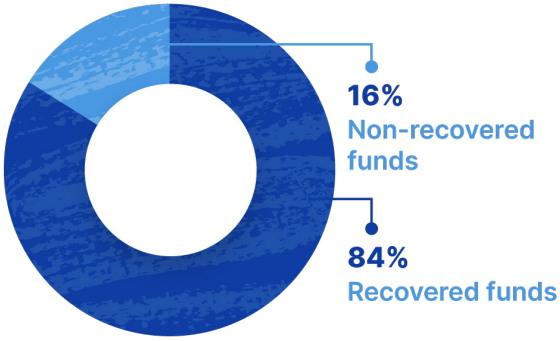
Employees: 1-25

A nonprofit organization providing child and family services grants to other nonprofits received a wire change instruction from a nonprofit partner. Only the email they received had been spoofed, and only appeared to be from the nonprofit partner. The spoofed email claimed that, due to COVID-19, funds sent to the partner could no longer be received by check, and instead should be sent by ACH transfer. Two days, and $1.3 million dollars later, the insured realized they'd been duped and phoned Coalition's claims and security incident response team (SIRT). Within 5 minutes, Coalition's SIRT went to work with law enforcement and the financial institutions involved to recover the stolen funds, successfully recovering all but $250 of the $1.3 million originally lost. Coalition SIRT is available to all policyholders at no cost, and is unique across the cyber insurance industry.

Percent of incidents where Coalition has recovered funds



Percent of funds recovered by Coalition



Coalition recovered lost funds in over half of reported incidents, recovering **84% of all lost funds**

COMMON SOCIAL ENGINEERING TECHNIQUES

Invoice manipulation

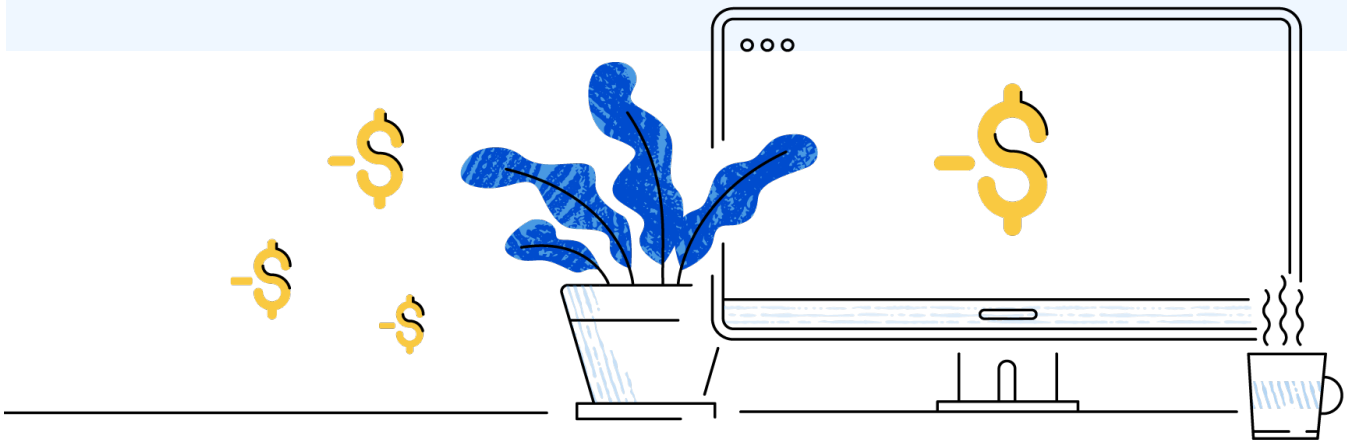
Invoice manipulation is a variant of social engineering. Traditionally, an employee of a company is tricked via a business email compromise or phishing attack to voluntarily part with money, products, services, or goods. Invoice manipulation is more devious. It can occur when the customers or vendors of an organization are tricked by a criminal actor using a legitimate email or data of the insured to get the customer or vendor to alter a payment or deliver products, services, or goods to a location that is controlled by the criminal actor. Unlike run-of-the-mill phishing attacks, invoice manipulation takes time observing an organization's processes and habits with third parties.

Look-alike domains

Look-alike domains are domain names that closely resemble the domain name of a trusted website, for example by swapping letters around or substituting common characters. In this day and age, most of us are weary about clicking links that we don't trust, and so look-alike domain names are designed to make it non-obvious that a link or message is coming from a malicious domain or sender. In advance of a social engineering attack, it is common to see criminal actors registering domains similar to the victim's to ultimately phish the victim, or to perpetuate funds transfer fraud or business email compromise.

Email spoofing

Email spoofing is the creation of an email with a forged sender address. Criminals spoof emails in the hopes of duping the recipient (i.e., the victim) into thinking the email originated from a trusted source. In the context of funds transfer fraud it is a technique that is used to spear phish, impersonating the email of a CEO/executive, vendor, or customer in an effort to trick the victim into wiring funds, or purchasing and sharing gift card PIN numbers.



You've got deception: business email compromise

One thing all of our policyholders have in common is their use of email. While many believe their digital front door is their website, to a cybercriminal, it is an organization's email inboxes. Business email compromise (BEC) was the initial point of entry for 60% of the claims reported to us, and resulted in a wide variety of claims including funds transfer fraud, ransomware, and data breaches.

Despite popular belief, email is *not* a secure form of communication, and all organizations (and individuals) should use caution when sending or verifying any sensitive information by email. Malicious actors have developed sophisticated techniques that can be very difficult, if not impossible, for the trained eye to detect.

Any organization that uses email is susceptible to BEC. However, our claims data shows that organizations which rely on email to conduct financial transactions (e.g., title & escrow companies, realtors, brokers, etc.), as well as individuals with access to banking information (e.g., finance and accounting staff), are unsurprisingly targeted with considerably greater frequency.

Interestingly, our data demonstrates that the likelihood an organization experiences a BEC is also correlated to the email provider used. Our policyholders that used Microsoft Office 365 were more than **three times** as likely to report a business email compromise as compared to our policyholders that used Google Gmail.

3.2x

Organizations that use Microsoft Office 365 are more than three times as likely to experience a business email compromise when compared to Google Gmail

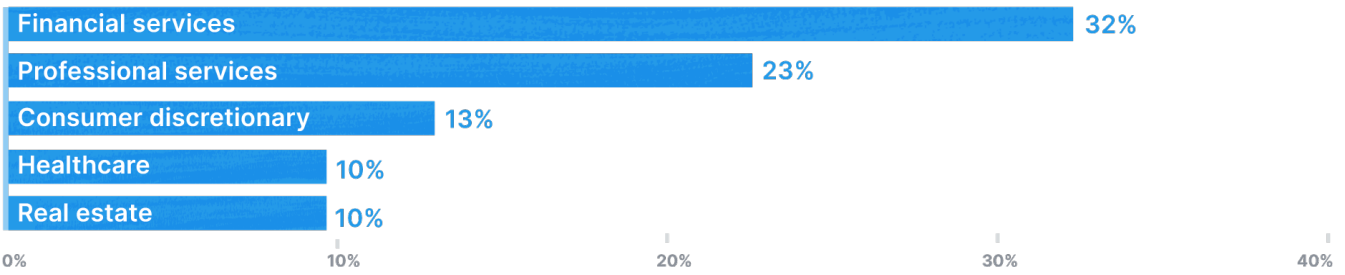
EFFECTS OF COVID-19

BEC attacks have increased 67% from 2019 to 2020, and their success rate has increased dramatically. Criminal hackers are taking advantage of changes in behavior as organizations respond to the dislocations caused by the COVID-19 pandemic to increase their success rates. For example, it is common to see social engineering attempts where a criminal actor asks for payment to a fraudulent ACH instruction due to the closure of an office or ability to receive mailed checks. The recipients of these requests, believing the request to be legitimate given the circumstance many businesses find themselves in, often don't think twice.

67%

Percentage increase in the frequency of business email compromise attacks from 2019 to 2020

Percent of BEC claims by industry (top 5)



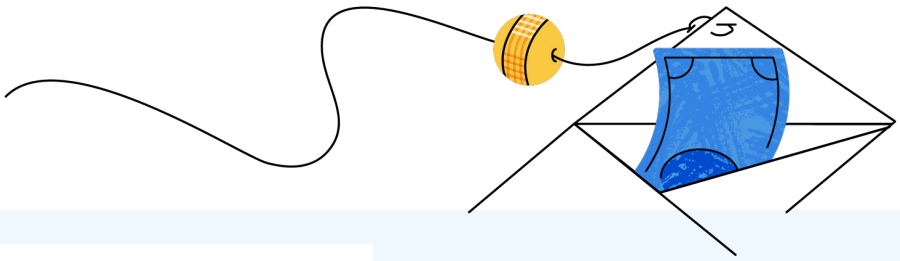
Case study

Industry: Law firm

Revenue: $160,000,000

Employees: 251-1,000

An administrative assistant at a leading law firm received an invoice in his inbox, only this invoice included a banking trojan designed to steal passwords and deploy ransomware. Fortunately, within 15 minutes of the infection, Coalition's threat intelligence platform alerted the policyholder of the infection, and within 1 hour Coalition SIRT coordinated with the policyholder to examine the logs of the infected device, collect the malware, examine all email activity, and re-image the employee's computer *before* any damage was done. Coalition is the only cyber insurer to provide 24/7/365 monitoring to policyholders to prevent claims from happening in the first place, and at no additional cost.



COMMON BUSINESS EMAIL ATTACKS

Spoofing

Email spoofing is the creation of an email with a forged sender address. Criminals spoof emails in the hopes of duping the the recipient (i.e., the victim) into thinking the email originated from someone or somewhere other than the intended source. It is one among many social engineering tactics to steal information or funds from an organization.

Phishing

Phishing is the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords, and credit card details by disguising oneself as a trustworthy entity in an email, text message, or other electronic communication. Phishing attempts are often disguised as messages from trusted parties such as banks, colleagues/executives, social media websites, etc. used to deceive users.

Spear phishing

Unlike ordinary phishing, spear phishing is a targeted attempt to steal sensitive information such as account credentials or financial information from a specific victim, achieved by acquiring and using personal details of the victim to increase the credibility of the social engineering attack.

Recommendations to solve cyber risk

Cyber incidents are costly and incredibly disruptive for any business. However, most cyber incidents and security failures (particularly the ones targeting small businesses) are preventable. In our experience, the most effective methods to mitigate cyber risk are all no-cost or extremely low-cost to implement. Our top five recommendations to mitigate cyber risk are as follows:

Multi-factor Authentication

Turn on multi-factor authentication (MFA) for all business-critical services including corporate email accounts, VPNs, financial accounts, and any other application where sensitive information is stored. While it is nearly impossible to prevent phishing entirely, using MFA can stop criminals in their tracks.

Email Security

Implement basic email security measures including SPF, DKIM, DMARC, and an anti-phishing solution. Email is the single most targeted point of entry into an organization for a criminal hacker, and the implementation of these email security measures can be done quickly, and for free.

Routine Backups

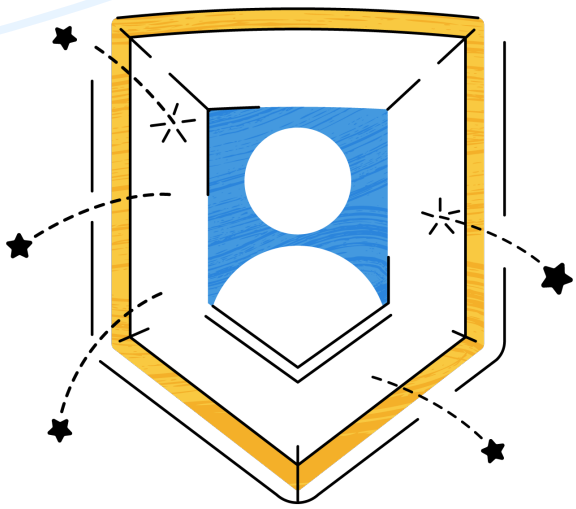
Regularly back up your systems and information, and store backups in an "offsite" location. Offsite doesn't have to mean physically offsite, but in a location that is not connected to your main business network. This will make it far more difficult for a criminal hacker to delete or encrypt your backups.

Wire Transfer Verification

Implement a dual-control process when making funds transfers. Today, it is no longer safe to assume that email is a secure means of communication. Call the intended recipient of the transfer before you make it to confirm any wire instructions provided — and make sure you have an accurate phone number!

Password Management

Encourage employees to use a password manager (e.g., Lastpass, 1Password, or the password managers built into web browsers like Chrome or Safari). Using strong, unique passwords for each of the services you use can help prevent common criminal techniques such as "brute forcing" or "credential stuffing."



Why you need cyber insurance

What do all of our policyholders have in common? They were insured. We regret that some clients were harmed in the making of this report, but we've stood by 100% of them, and many have been kind enough to share their experiences. This is why Coalition was founded with the singular mission to *solve cyber risk* — to proactively help organizations prevent incidents, to provide emergency first response when they occur, and to help them recover operationally and financially in the aftermath.

Whether you purchase cyber insurance from Coalition, or you're new to the cyber threat landscape, there are quite literally millions of reasons (and dollars) to protect your organization. If you have any questions about this report, need assistance with an ongoing incident, or would like to learn more about cyber insurance, our team is on hand to assist.

Cyber Risk, Solved.®

coalitioninc.com

@SolveCyberRisk
help@coalitioninc.com

1160 Battery St. Suite 350
San Francisco, CA 94111