Coalition®

H1 2021

Cyber Insurance Claims Report

coalitioninc.com

Cyber Insurance Claims Report

H1 2021

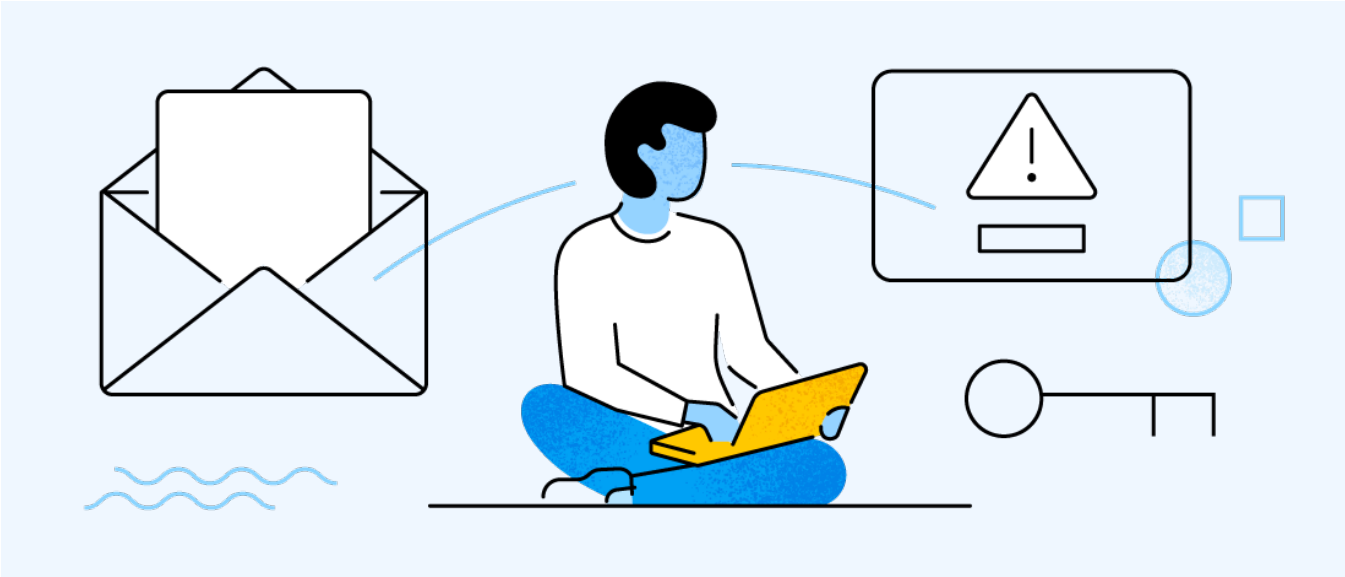
If the events of the past year are any indication, cyber risk is set to become the defining risk of our age. Never in history have organizations and individuals been as dependent on technology as they are right now. And yet, we must continue to rely on technology to build a more sustainable, efficient, and connected future. With the escalation of ransomware and other cyber crimes impacting everything from critical infrastructure to the corner store, one thing is clear: **addressing cyber risk matters for everyone**.

Cyber risks are also increasingly impacting *everyone*. The COVID-19 pandemic has transformed the way we work and live and, in the process, dramatically increased our collective reliance on information technology. Most organizations can no longer function without working computers and access to the internet. And if one organization loses access, it can impact many others in the same supply chain. As a result, the growing prevalence of ransomware and supply chain attacks are among the most significant risks we've observed over the last year. Ransomware attacks now make headlines daily, and the supply chain attacks against Solarwinds, Microsoft Exchange, Kaseya, and Codecov—to name only a few—have impacted thousands of businesses at once, including businesses that previously believed they were outside the crosshairs of criminals.

As one of the largest providers of cyber insurance, Coalition, together with the broader cyber insurance industry, is well positioned to fight cybercrime and help organizations embrace ongoing technological progress. On any given day Coalition performs billions of security scans, sends hundreds of critical security alerts, investigates reported cyber incidents, and helps our over 50,0000 customers navigate an increasingly fast-paced digital world. In that spirit we share this report to help all organizations solve cyber risk.

Analysis of our claims data through the first half of 2021 reveals a number of evolving trends:

- **Cyber crime is increasing like never before.** Business email compromise (BEC) incidents led the way with the frequency of reported incidents up 51% over the first half of last year. BEC incidents continue to be the most widespread as email is the dominant attack surface of most organizations. Funds transfer fraud (FTF) is the next most common incident type and increased 28% over the first half of 2020. Finally, ransomware incidents, after dipping slightly in the second half of 2020, began to increase again in 2021. However, worse than the growth in frequency is the growth in severity.
- **Ransomware is growing in severity.** The average ransom demand made to our policyholders in the first half of 2021 was $1.2 million. That is a large price to pay for any organization, and is a nearly 170% increase from the average demand in the first half of 2020. As the business impact of ransomware attacks has grown, so too has the leverage of criminals to demand larger ransoms. This has also made smaller businesses more attractive targets than they once were.
- **Criminals are taking advantage of dislocations in how we work.** The increase in remote work has meant fewer in-person interactions, more electronic funds transfers, and more opportunities for criminals to exploit changes in operational processes undertaken by many organizations in response to COVID-19. The average amount of funds stolen increased 179% from the first half of 2020 to 2021, from $116,842 to $326,264.
- **The rush to facilitate remote work has come at a large cost.** Many organizations turned to remote access protocols and tools such as Microsoft Remote Desktop (RDP) to facilitate remote work. However, left exposed to the internet, these access points have become favored targets of criminals. The number of organizations with RDP enabled when they applied for insurance nearly doubled from the first half of 2020 to 2021. The rate of policyholders who experienced a claim due to exposed RDP also increased from 29% to 40%, and the severity of these incidents increased by 103%.
- **Smaller companies are increasingly targeted.** As criminals are able to extort ever growing amounts from organizations following ransomware attacks,



and as attacks become increasingly automated, it has become more profitable for criminals to target more small and midsize organizations. The frequency of incidents reported for organizations with under 250 employees increased 57% from the first half of 2020 to 2021.

- **Cyber insurance works.** We've processed more claims across more organizations in the first half of this year than in any other period, and there wasn't a single organization that we weren't able to help successfully recover. We've also helped thousands of companies improve their baseline cybersecurity hygiene, including our own policyholders who continue to experience less than one-third the frequency of claims as the broader cyber insurance market.

While many things have changed since our last report, there was one constant: organizations continue to be targeted by criminals because they have made poor technological choices, often exposed to the public internet, that make them targets. It's more important than ever that companies take the time to understand their cyber risk, and it's never been easier with new tools like Coalition Control.

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

- The sample size of reported incidents and claims is 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 frequency reflects this. As a result, we may see different types of claims than others.
- Recently reported claims will continue to develop and mature. The report contains our current loss estimates through the first half of 2021, but these may fluctuate in overall severity in the coming months.
- This report contains predictions from our team of in-house experts. These are our opinions based on current market conditions and proprietary data. In most cases, we hope we are wrong (if only for the sake of our customers).
- This isn't an exhaustive review of the data we collect. 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.

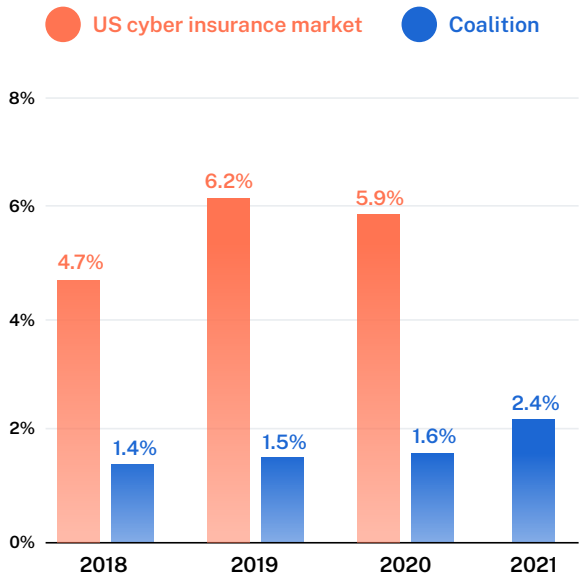
Table of Contents

New trends in cyber attacks

In 2020, many organizations were forced to transition to remote work. They often settled into the ease and reliability of remote working environments. The rush to get up and running quickly during the pandemic caused many organizations to overlook security risks. Many companies failed to recognize that what makes it easier for their employees to access accounts and sensitive information also makes it easier for hackers to target and access the same information. Criminals seized the opportunity, increasing the sophistication of their operations and evolving their tactics with precision. They started targeting new industries, smaller businesses, and smaller pockets.

Despite the shift in the threat landscape, the frequency of claims experienced by our policyholders in 2020 was significantly lower than the rest of the market. Our claims frequency, which is calculated as the number of reported claims where a payout was made divided by the number of policies we earned over the period, rose to 2.4% of policyholders in 2021. This reflects a 51% increase in business email compromise claims, 28% increase in funds transfer fraud claims, and more widespread supply chain attacks in 2021.

Claims frequency: US cyber insurance market and Coalition



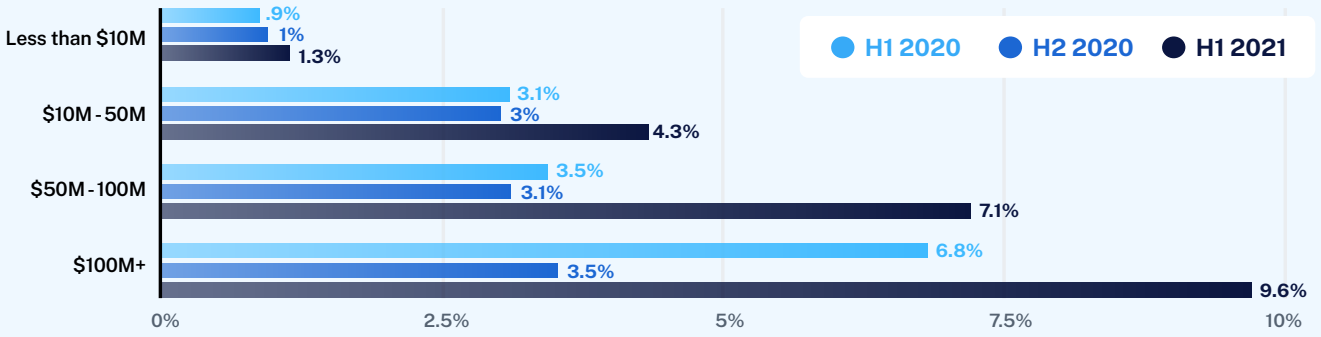
Market data is reported by US insurers to the National Association of Insurance Commissioners (NAIC). Market data for 2021 is not yet available.

Note: The figures you see here refer specifically to organizations that have decided to purchase cyber insurance. Unfortunately, many still don't. Our data only accounts for incidents where the organization filed a claim, and the losses were above the organization's deductible.

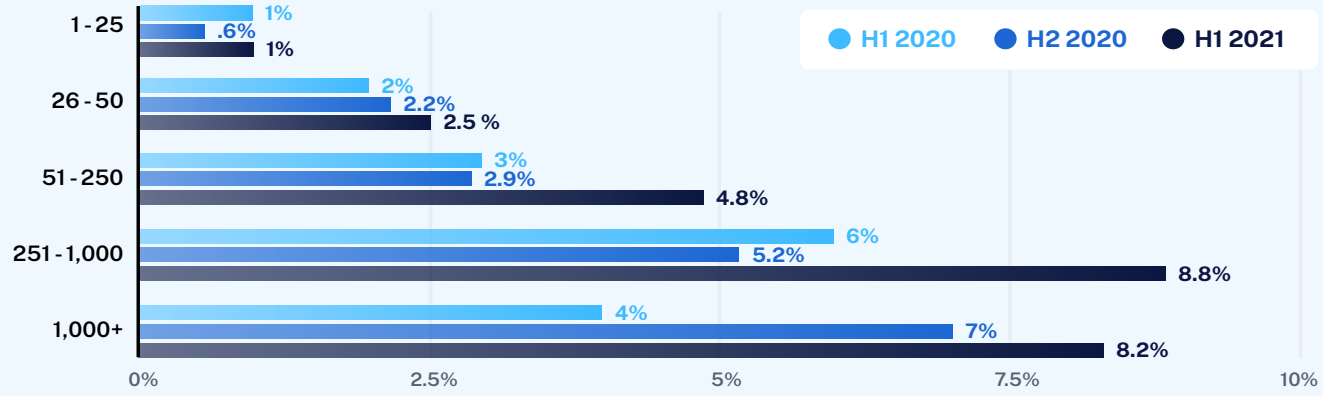
Historically, small and midsize businesses seemed to be off the radar of cyber criminals, but that has begun to change. While cyber incidents can be equally devastating to businesses of any size, we've seen a material uptick in claims targeting small and midsize businesses, with the frequency of claims increasing by 57% for organizations with 250 employees or less.

Coalition policyholders experience less than **one-third** the frequency of claims when compared to other carriers in the market.

Claims frequency by company size (revenue)



Claims frequency by company size (number of employees)

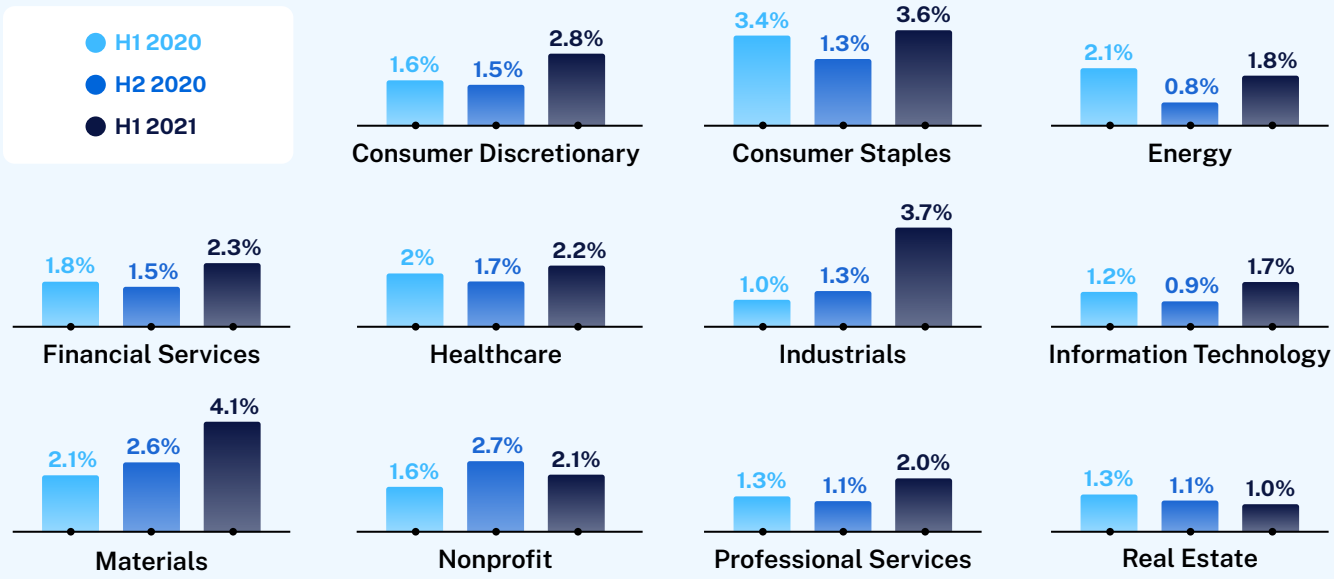


Cyber criminals are opportunistic, particularly when it comes to small businesses, and the technology and processes that organizations use are far more indicative of their risk than their industry. No company is too small to be an enticing financial opportunity for attackers. Still, some industries did experience notable increases in claims in the past year. From H1 2020 through H1 2021, we saw an increase in claims frequency of 30% for nonprofits, 46% for IT, and 53% for professional services. Industrial and manufacturing businesses experienced a notable surge, with industrials increasing 263% and materials increasing 99%.

In the last report, we stated that the frequency of attacks increased, and so did the severity of these events. Since that report, we actually saw the frequency of ransomware dip slightly in the second half of 2020, though there's been a resurgence in the first half of 2021. BEC has also made a steady climb over the last year (up 51%), and FTF has increased 28% compared to the previous year.

We will go more in-depth on ransomware and funds transfer fraud later in this report, but we'd be remiss if we didn't note that the ransom demands are skyrocketing, and more organizations are losing huge sums of money from these attacks. The average ransom demand made to our policyholders nearly tripled from the first half of 2020 to 2021, from $444,489 to $1,193,159. The average severity of

Claims frequency by industry

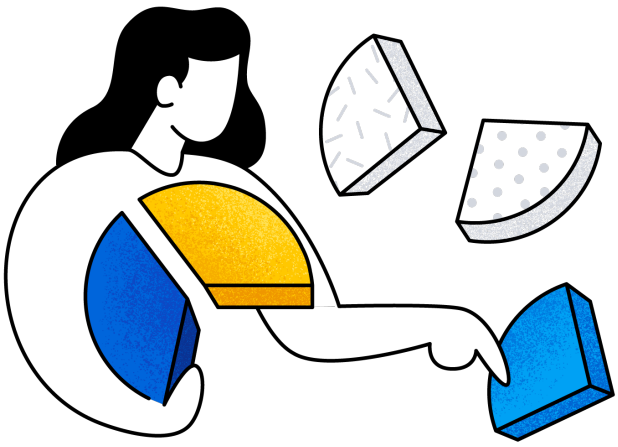


ransomware (meaning the average payout for each claim) has actually decreased slightly from the first half of 2020 to the first half of 2021. However, this is reflective of Coalition's efforts to negotiate ransoms on our policyholders' behalf and help them recover from data backups.

FTF losses have also surged, with the average claims severity increasing nearly threefold from H1 2020 to H1 2021. And the average funds transfer loss before clawing back funds in H1 2021? A painful $326,264. Given the shift to remote work during the pandemic, many organizations moved most of their operations online, forcing all communication to happen via email with little to no face-time or guard rails in place.

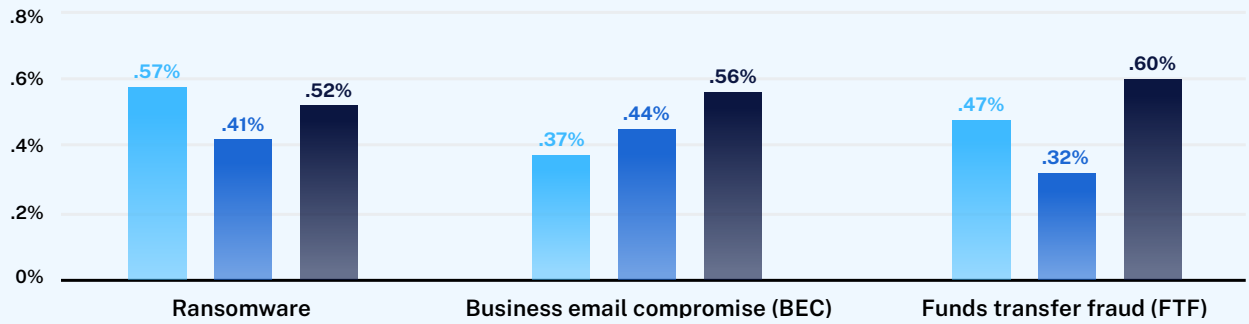
This means email security protocols were often overlooked, opening the door for more sophisticated social engineering scams and more excuses to divert large money transfers. Imagine the subject line: "Due to COVID-19, we are changing our payment procedures."

Despite the evolution in cyber crime over the past year, the coverages that paid out are consistent with prior years, with Breach Response, Cyber Extortion, and Fund Transfer Fraud topping the list. However, as cyber criminals have become more creative and begun targeting an even broader swath of organizations, we've called upon our full range of coverages to protect our policyholders. These include the less common yet critical Bodily Injury and Property Damage and Cryptojacking coverages.

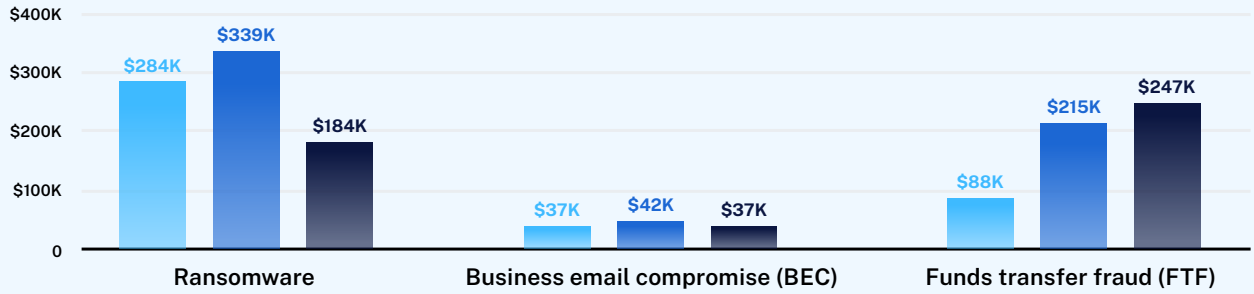


KEY: H1 2020 H2 2020 H1 2021

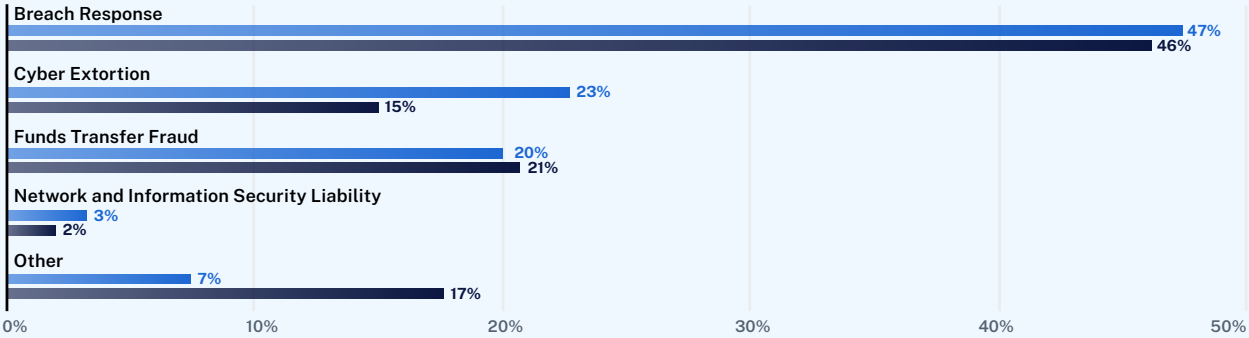
Claims frequency by category



Average claim severity by category



Claims reported by insuring agreement triggered



Monetizing cyber crime:

How criminals have turned hacking into a lucrative business

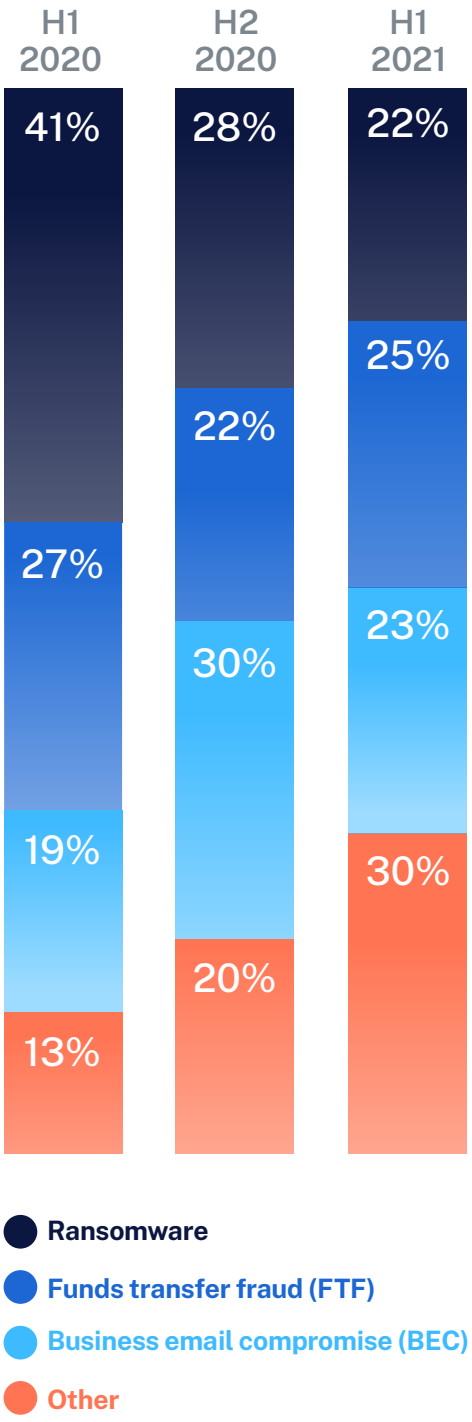
The business model of cyber crime has shifted significantly over the past few years. Hackers have transitioned from selling stolen data and credit card information online to something much more effective and lucrative — stealing funds directly through FTF and ransomware.

Data theft remains a critical risk that can result in all kinds of headaches and expenses, including regulatory fines, penalties, reputational harm, and customer notifications and monitoring, just to name a few. However, ransom payments and funds transfer fraud have quickly become the preferred tactics for criminals. Not only do they result in much larger payouts, but they also provide far easier and faster ways to monetize cyber crime.

The next few sections are a deep dive into the two most common (and consequential) claims our policyholders experience: ransomware and funds transfer fraud.

Ransomware and funds transfer fraud account for 50% of all known losses.

Percentage of reported claims by category



Ransomware

Towards the end of 2019, the industry saw an increase in the frequency and severity of cyber claims. This put pressure on carriers moving into 2020, coupled with increased regulation at all levels of government. Last year the industry saw the first real signs of a hardening cyber insurance market, resulting in increased underwriting scrutiny and increased premiums. The main culprit? Ransomware attacks.

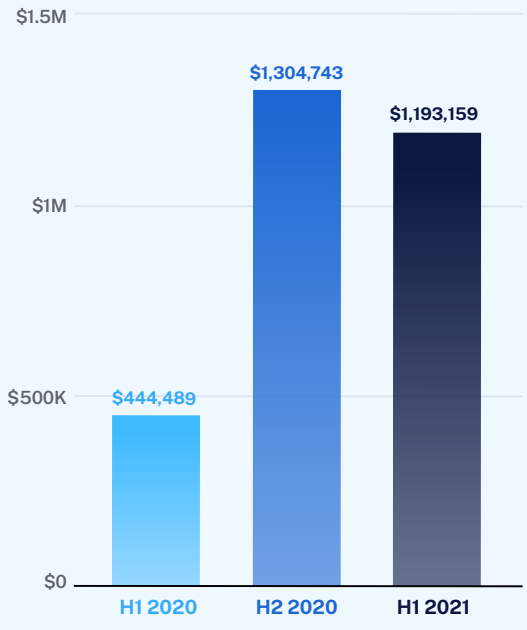
While social engineering and funds transfer fraud threats are still very much present, ransomware reshaped the industry. Hackers are using automation to target insecure businesses more broadly, increasing the amount of the ransom they hope to collect, and unleashing sophisticated malware variants with more complex attack techniques.

Ransomware is not just a type of malware; it is a criminal business model in which the perpetrator seeks to benefit by taking hostage a victim's data, infrastructure, economic output, intellectual property, or even privacy. It is extortion in its purest form, and it won't go away as long as attackers keep finding new ways to take an organization's assets hostage. We've even seen the appearance of Ransomware as a Service (RaaS), a business model used by ransomware developers in which they lease malware variants out to bad actors. RaaS gives everyone, even those without technical expertise, the power to launch powerful ransomware attacks. A RaaS kit may include 24/7 support, bundled offers, user reviews, and forums like legitimate SaaS companies.

We've seen a sharp increase in ransom demands over the past year. This increase in demands is related to the change in systems necessary for companies to go remote, which has permitted easier and longer access. Additionally, longer access has allowed hackers to research an organization's operational patterns, financial information, and insurance coverage to better understand what a company can "afford" and the value of the information encrypted.

This has pushed ransom demands higher. Unfortunately, with the complexity of ransom events, and the failure of companies to have backups, ransoms have increased along with the business interruption and time to recover. Our average ransom demand for the second half of 2020 was $1,304,743 and leveled to $1,193,159 in the first half of 2021. That isn't a small price to pay for any company, and it's a nearly 170% increase in just one year. We have also seen costs grow for remediation.

Average ransom demand made to Coalition policyholders



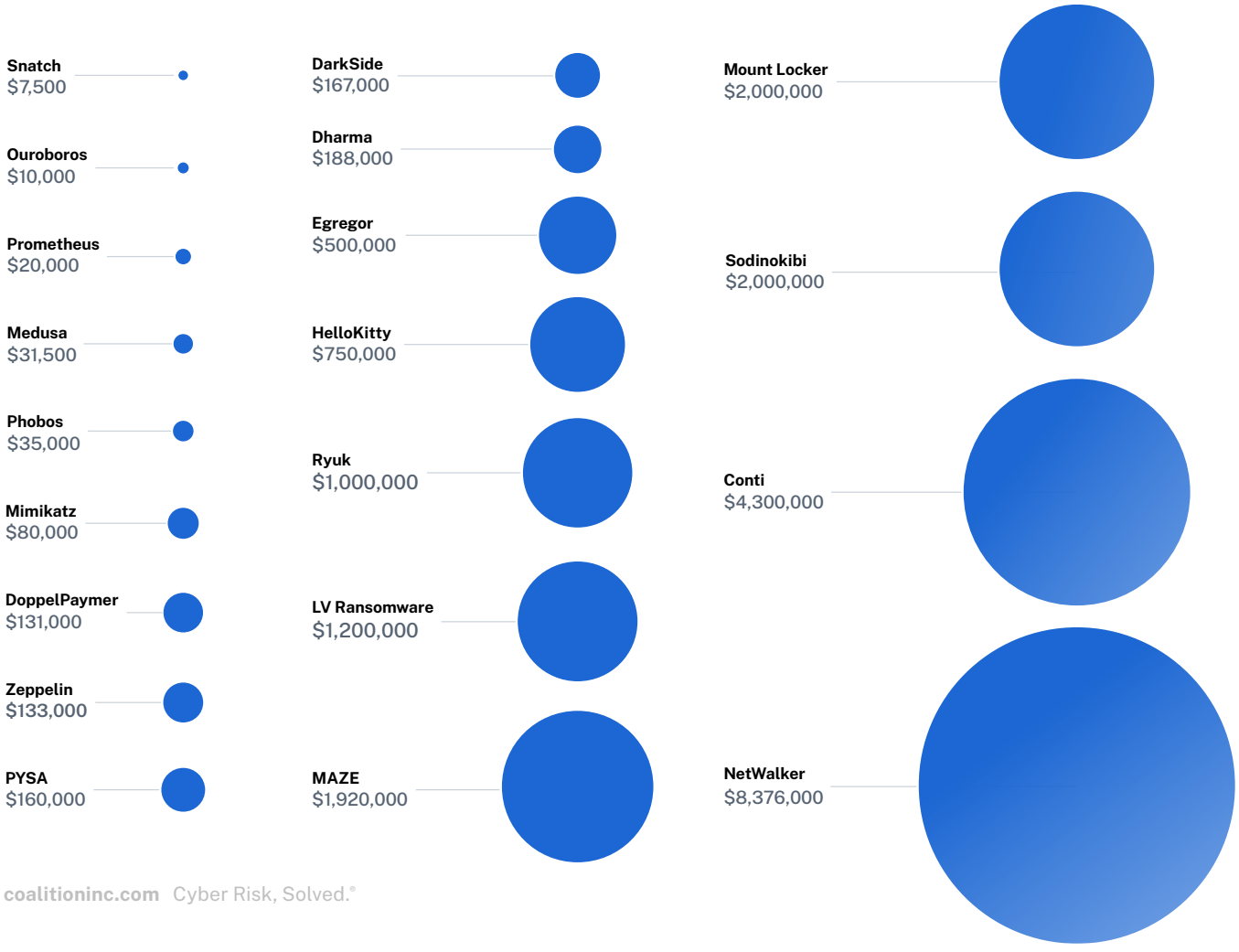
In addition to the increase of ransom demands, we have also observed an explosion of new ransomware variants that are even more invasive and dangerous. We've witnessed the addition of PYSA, Mimikatz, Medusa, Snatch, Egregor, Conti, Mount Locker, and HelloKitty.

Ransomware attacks often result in significant interruptions to ongoing business activities. The process to recover and restore business operations, even when system backups are readily available, can be complex and time-intensive. What's unfortunate is that small and midsize businesses are impacted more often than larger organizations — and they are the least able to defend themselves and bounce back quickly. According to Coveware, 70% of ransomware attacks impact organizations with fewer than 1,000 employees, which may be more vulnerable to attacks.

How to combat ransomware

Email security like spam filtering and user training is critically important, as ransomware can be installed when users open a suspicious attachment or visit a malicious website. A robust cybersecurity program is also crucial to ensure technical vulnerabilities like old, unpatched software or insecure remote access tools are unavailable for attackers to exploit. Finally, before ransomware strikes, you should implement a robust backup strategy that includes frequent backups and offline storage, allowing you to rebuild systems without paying the ransom.

Average ransom demand made to Coalition policyholders by variant



Case Study:

HelloKitty

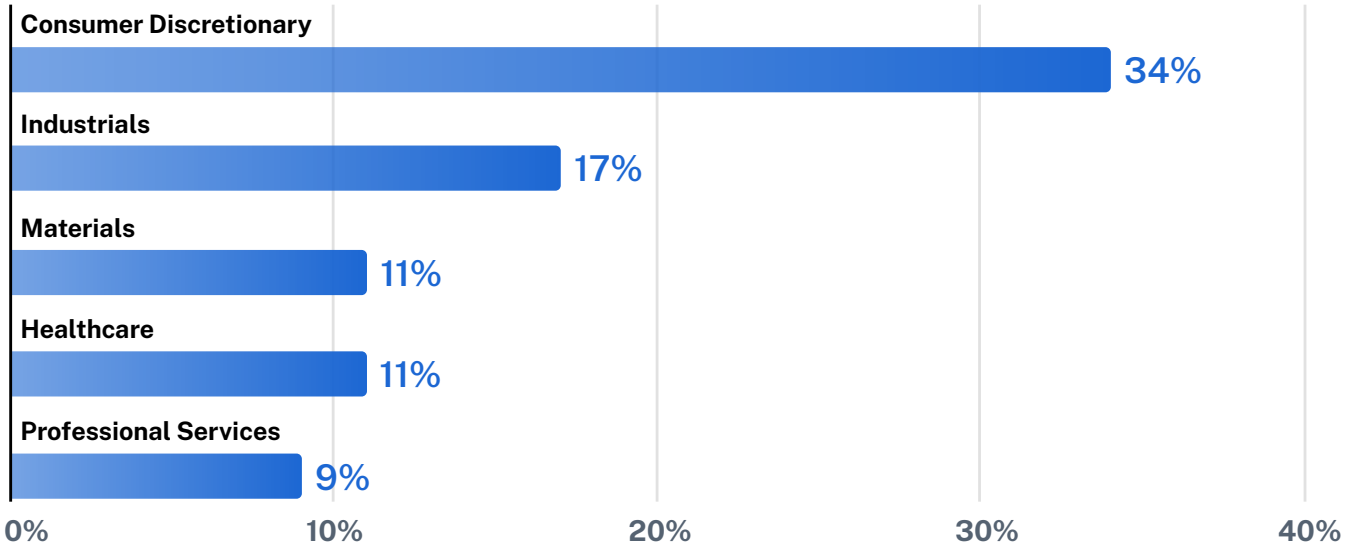
INDUSTRY: HEALTHCARE

REVENUE: $3.3M

EMPLOYEES: 51-250

After more than 30 years in business a medical practice management company started their day like any other only to realize they couldn't access any of their computer systems. The company's IT staff discovered that nearly all of their files had been encrypted, including their backups. Shortly after the discovery of the incident they contacted our claims team who, together with our dedicated digital forensics and incident response team, Coalition Incident Response (CIR), got to work to help the company recover. CIR quickly determined that the company had been infected with HelloKitty malware, a dangerous new ransomware variant that is known to exfiltrate the data of its victims prior to encrypting it. With their backups fully encrypted, and absent any other options to restore their operations, the company made the difficult decision to pay the ransom in order to restore their operations. Fortunately, CIR was able to negotiate the ransom demand down by nearly 75% from $750,000 to $200,000, and proceeded to help the company restore all of their data. The costs to respond to the incident, to recover lost data, and to pay the extortion, together with the lost income resulting from the incident, were covered by the company's cyber insurance policy with Coalition.

Ransomware claims by industry — H1 2021



Funds transfer fraud

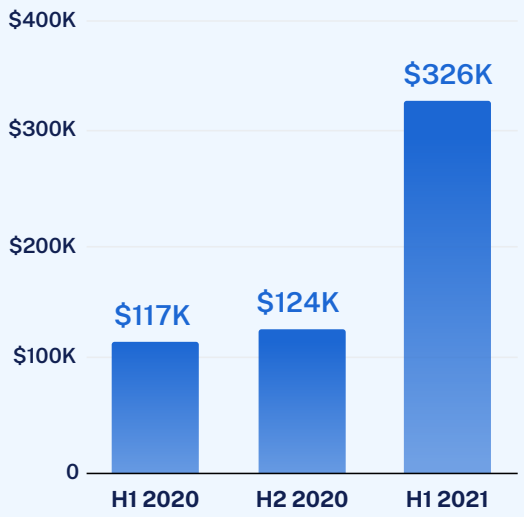
Funds transfer fraud is among the easiest ways to monetize cyber crime. Unlike ransomware, which requires more sophisticated attack techniques and specialized malware, FTF is most often perpetrated through phishing and email compromise followed by social engineering. Once a criminal has access to a mailbox they are able to manipulate contacts connected to that mailbox to modify payment instructions or otherwise make fraudulent payments. Some FTF incidents don't involve a security failure at all — criminals will send spoofed emails, doctored invoices, and even make phone calls that appear to be legitimate enough to convince a victim to wire funds.

The average funds transfer fraud loss (prior to recoveries) increased 179% from H1 2020 to H1 2021, from $116,842 to $326,264.

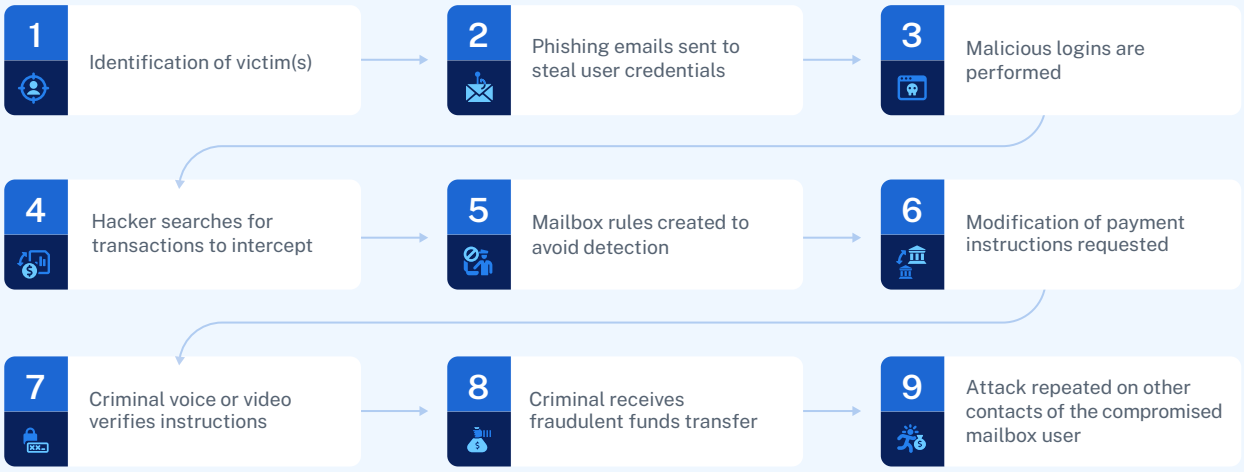
Funds transfer fraud losses can be significant, but you can recover losses in many cases if you move quickly. We recommend our policyholders take the following actions to maximize the chances of recovery:

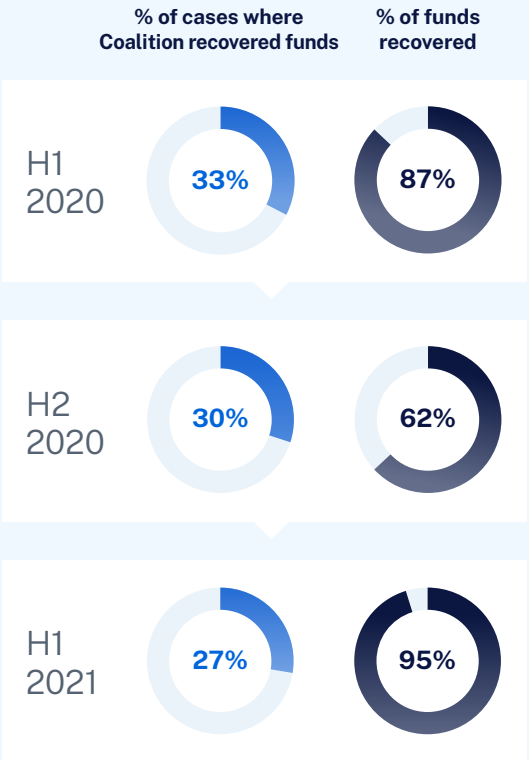
1. Notify Coalition's claims team of the loss as soon as possible, and ideally within 72 hours of the transfer. Coalition's security & incident response team will spring into action.
2. Immediately notify your bank of the fraudulent transfer, and request a clawback of the funds. This may require an interbank agreement between your bank and the receiving bank.
3. File a report with the FBI at IC3.gov.
4. File a report with your local police department.
5. Be the squeaky wheel and repeatedly inquire with your bank and the receiving bank on the status of the recovery.

Average funds transfer fraud loss (prior to recoveries)



Typical process for a funds transfer fraud event





While the frequency of FTF cases increased 28% from 1H 2020 to 1H 2021, in the cases where Coalition's Claims and Incident Response teams have managed to claw back funds, we've recovered 95% in H1 2021. This is an increase from 87% in the first half of 2020.

How to combat FTF

Defined procedures for handling new requests and change in payment requests are the primary defense. These procedures should include calling the requesting party on a known good number seeking to confirm the request. Never use the contact information provided in an email requesting a change. Verification procedures like defined two-party approval for transfers or required reviews for payment detail changes help combat the issue. If an FTF does occur, quick action is essential — the sooner an incident is reported to Coalition, the more likely we can help by canceling transactions or clawing back funds before the attackers can withdraw them.

Case Study:

Exploiting COVID-19

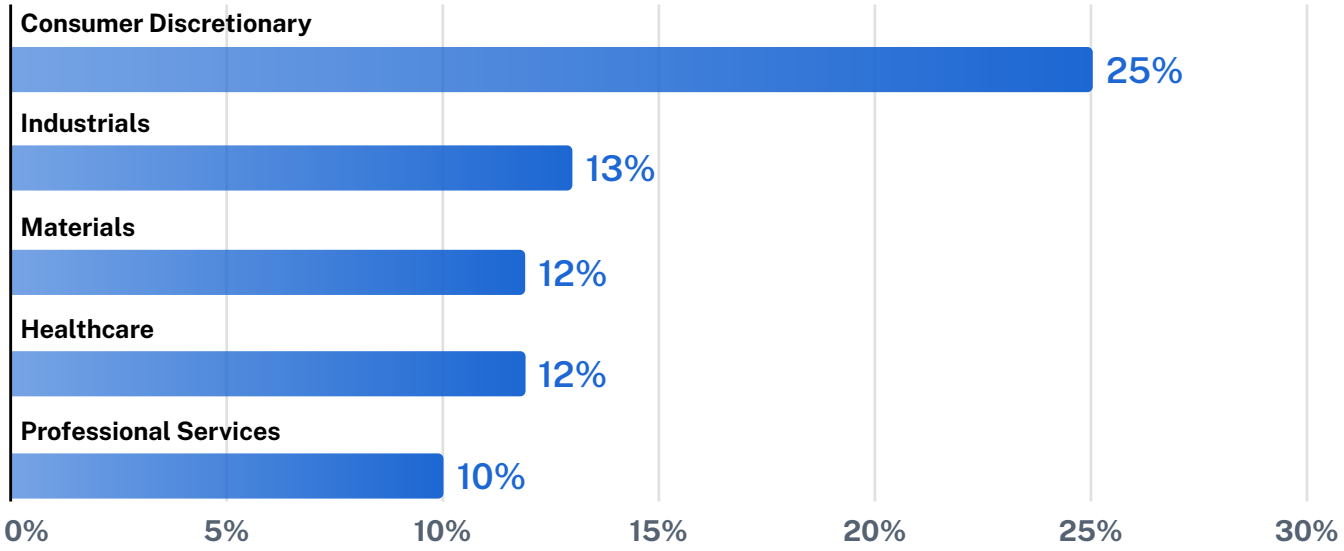
INDUSTRY: EDUCATION

REVENUE: $16M

EMPLOYEES: 1-25

The criminal sat in the email inbox of a nonprofit's Finance Director for over four months, just waiting and watching. How did they get access? They did their research, found the person who handled the money, sent a phishing email, and stole her credentials. The attacker spoofed the nonprofit's legitimate domain, set up email rules to divert replies, and sent compromised attachments. They sent an email to six people facilitating two very large fund transfers of roughly $620,000 each — totaling nearly $1.3 million. The subject line was 'Change banking service,' citing COVID-19 as the reason. Sometime later, the organization realized employees were being asked to purchase gift cards over email, which was highly suspicious. After doing some digging, they realized they'd been hacked, and the large payments they recently made went to a fraudulent bank account. They acted quickly, called us immediately, and made no changes to their environment. We discovered 82 malicious logins into her account worldwide, including South Africa, Lagos, and Nigeria. Coalition's Claims team sprung into action, working with law enforcement to file a report and stop the funds from being transferred. Due to our swift response, we managed to claw back all of the money except $500.

Business email compromise claims by industry — H2 2021



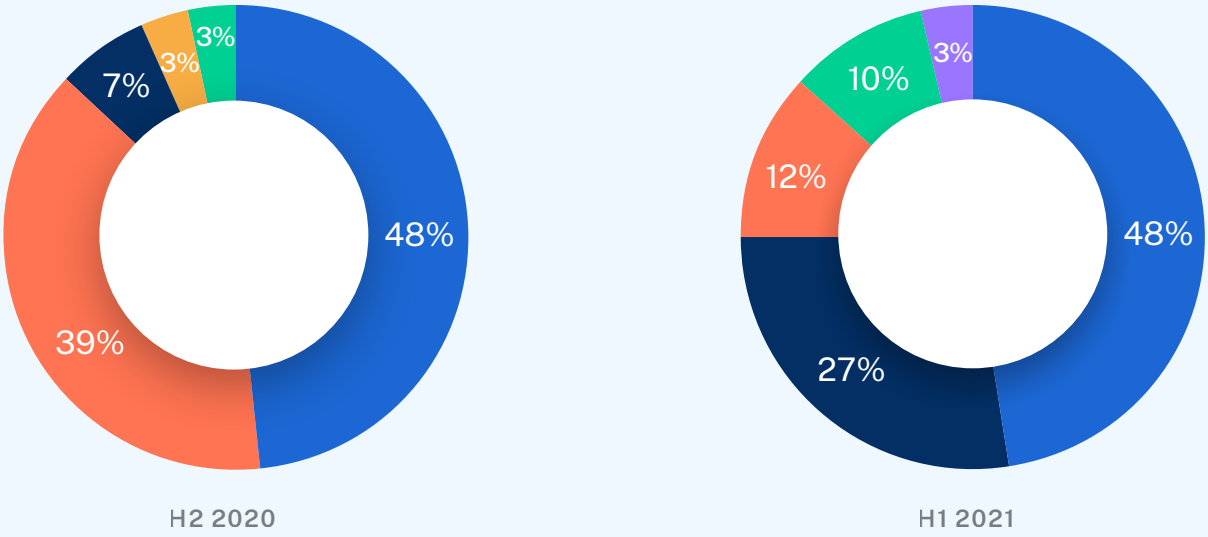
Executing cyber crime

Attack tactics and techniques

While ransomware and funds transfer fraud are the main ways criminals immediately monetize cyber crime, they use a wide array of attack techniques and tactics to gain access to systems in the first place. These tactics enable criminals to install malware to execute ransomware attacks or maliciously redirect funds.

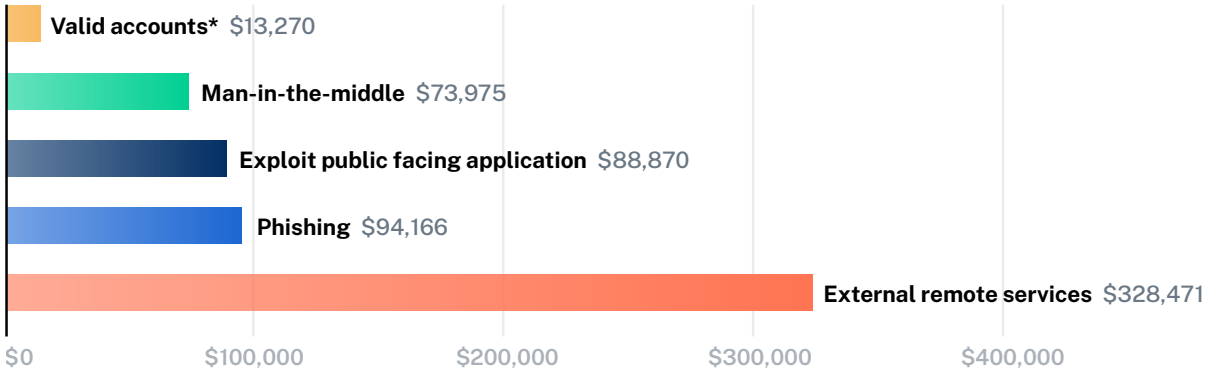
Social engineering leading to business email compromise, insecure remote access exposed directly to the internet, and third-party vendors targeted in supply chain attacks all lead to potentially catastrophic cyber events. Here is how criminals executed cyber crime in the past year.

Percentage of reported claims by attack technique

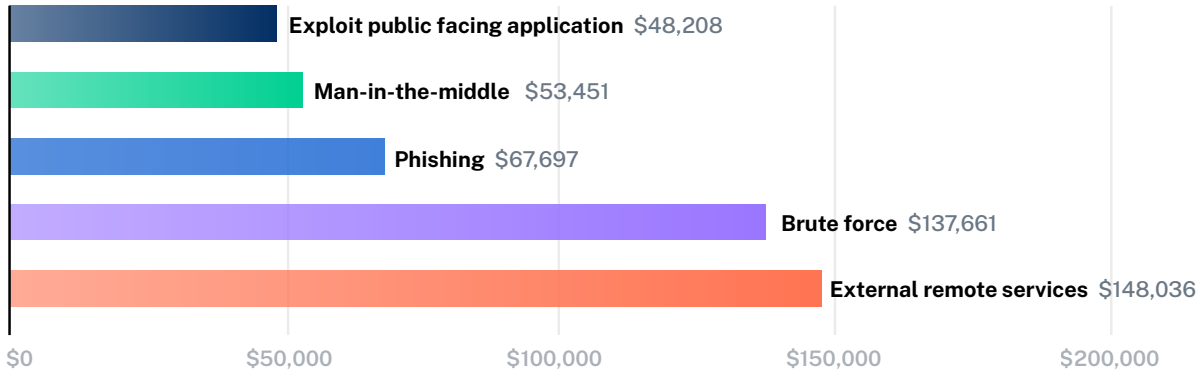


Note: attack vector data is not known in all cases. These charts reflect attack vectors for reported claims where the attack vector was known. Vectors are categorized according to the MITRE ATT&CK taxonomy of adversary tactics and techniques.
** Valid accounts is an attack technique whereby a criminal gains unauthorized access to a legitimate account.*

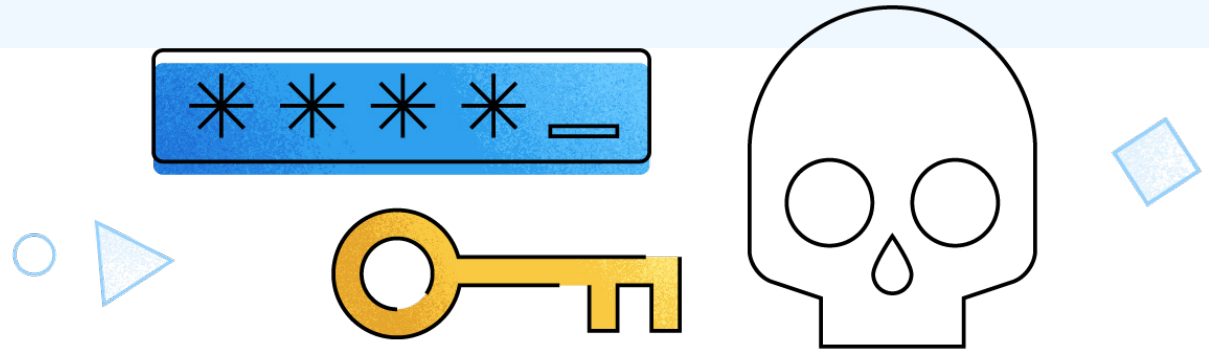
H2 2020 average claim severity by attack technique



H1 2021 average claim severity by attack technique



* *Valid accounts is an attack technique whereby a criminal gains unauthorized access to a legitimate account.*

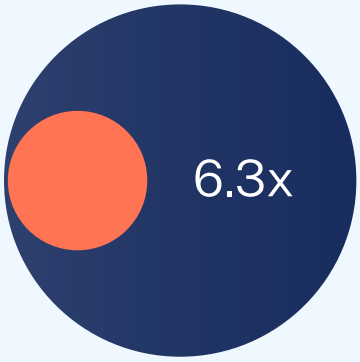


Business email compromise (BEC)

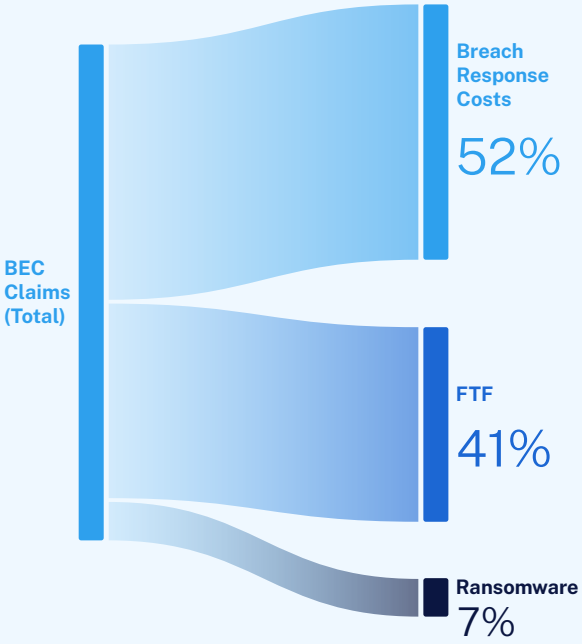
Any business that uses email (i.e., all of them) is susceptible to business email compromise (BEC). Once an attacker gets access to your email it's game over. Business email is a treasure trove of sensitive information that criminals use to pretend to be people in your company, redirect money, and deploy ransomware.

In our last claims report, we noted that your email provider matters when it comes to your organization's security. In H1 2021, Microsoft 365 email users were 6.3x as likely to have a claim as Google Workspace users — nearly double what we reported in H1 2020.

Relative likelihood of a claim by email provider — H1 2021



Email phishing was the initial vector of attack for 48% of reported claims where this data was available.



The evolution of BEC claims

Business email compromise can also lead to a wide array of losses for organizations — everything from ransomware to funds transfer fraud to data breaches. In almost every case, digital forensics work is required to understand the scope of the damage.

In 2020:

- **52%** of BEC claims did not extend beyond the breach of data in the mailbox, resulting in only breach response and forensics costs.
- **41%** evolved into an FTF incident resulting in the direct loss of funds.
- **7%** evolved into a ransomware event resulting in business interruption, cyber extortion, and/or digital asset recovery costs.

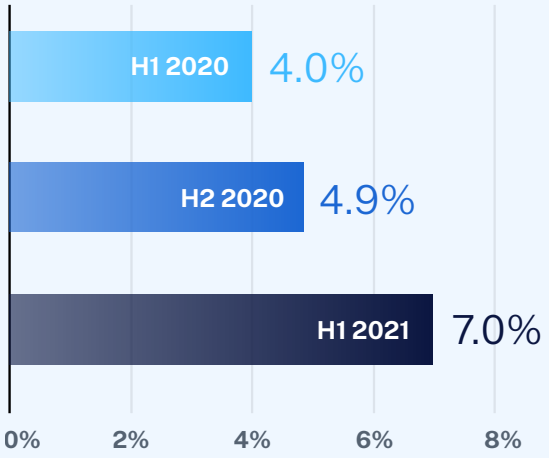
Insecure remote access

In the second half of 2020, we experienced more claims due to poorly managed remote access. The percentage of policyholders who experienced a claim due to insecure remote access increased from 29% to 39%. The severity of these attacks also increased by 103%. While remote access is useful and at times necessary, it needs to be handled with extreme caution.

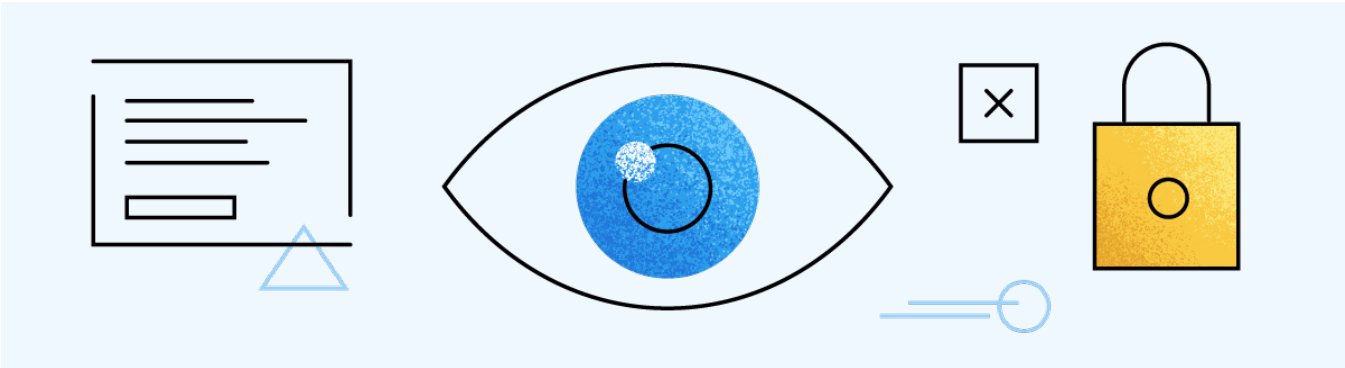
Remote desktop protocol (RDP) is a popular remote access solution used very often in Microsoft Windows environments. RDP enables a familiar experience for users — remote access to the well-known Windows desktop from anywhere. It's a powerful tool that can be very useful for remote collaboration and productivity. We saw a substantial uptick in the usage of RDP during the pandemic, which unfortunately opened up a world of fresh risk and vulnerability. Coalition scans for RDP, and we won't insure organizations until they close it due to its high level of risk.

RDP is subject to a variety of attacks, including the ability for RDP connections to be intercepted and the ability to get a remote computer to execute unauthorized programs. In addition, since the computer running RDP is inside your network, attackers get internal access to more resources, contributing to the increase we've seen in remote access attacks.

Percentage of insurance applicants with insecure remote access enabled



The percentage of businesses that had insecure remote access enabled when they applied for insurance nearly doubled from H1 2020 to H1 2021.



Third-party vendors and supply chain attacks

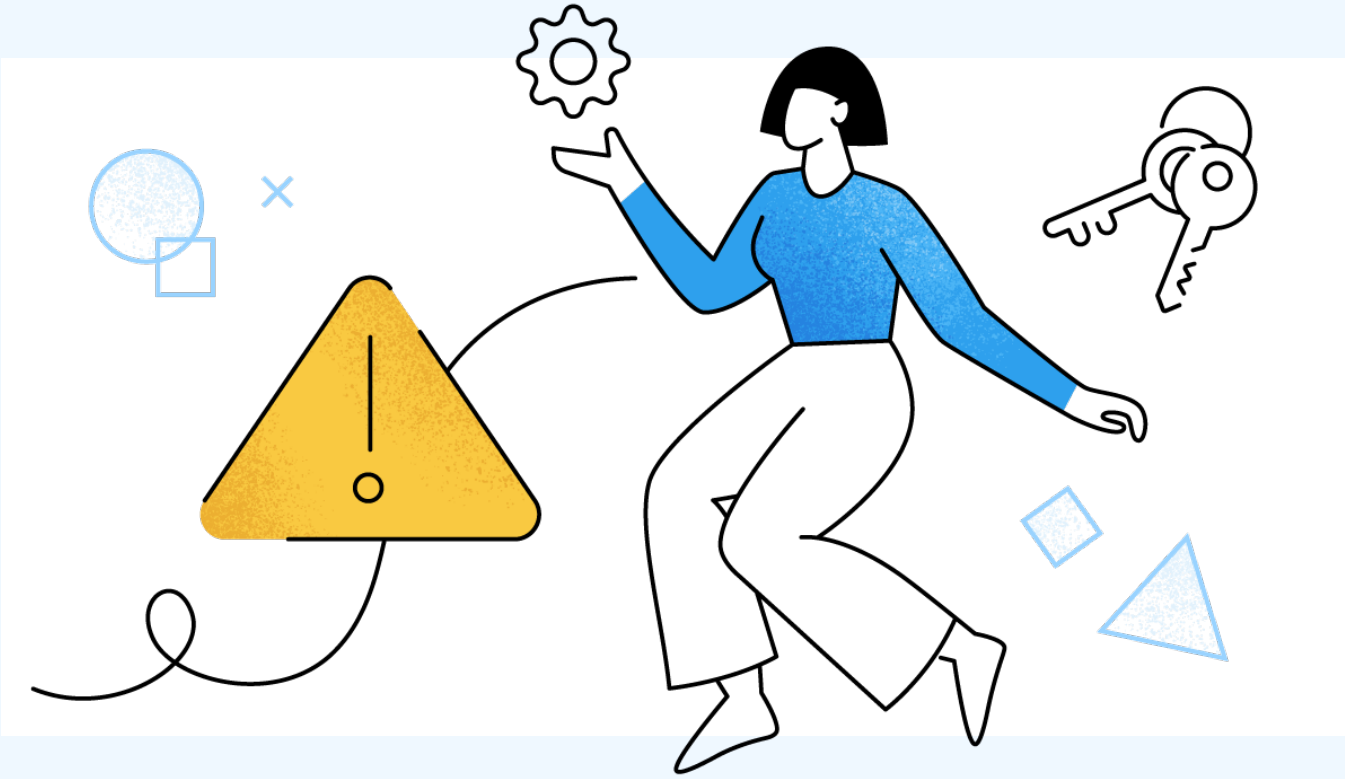
What was once referred to as individual vendor cyber risk has morphed into something much more complex, known as digital supply chain risk. Why supply chain? As organizations undergo digital transformations, they tend to purchase more cloud services, and these cloud services rely on vendors. And, more than likely, those vendors rely on other vendors.

If the thought of this makes you feel uneasy, your instincts are correct. By relying on these cloud services and their vendor partners, you are opening yourself up to more risk — risk you can't control. You've essentially exposed your business to a less secure environment you don't own that could impact your network in the case of an external incident.

What's the difference between BEC and supply chain risk?

BEC is a one-to-one exploitation of processes and uses email to gain unauthorized access to one individual email inbox. On the other hand, supply chain attacks are wide-scale events targeting the underlying software, which might happen to involve email but can also target a wide range of business systems.

Supply chain risk management (also referred to as vendor risk management or VRM) is the process of ensuring that the use of service providers and IT suppliers does not create an unacceptable potential for business disruption or a negative impact on business performance. And this concept of supply chain risk (and effective management) is more relevant than ever before.



Case Study:

Microsoft Exchange vulnerabilities

INDUSTRY: HEALTHCARE

REVENUE: $3.3M

EMPLOYEES: 51-250

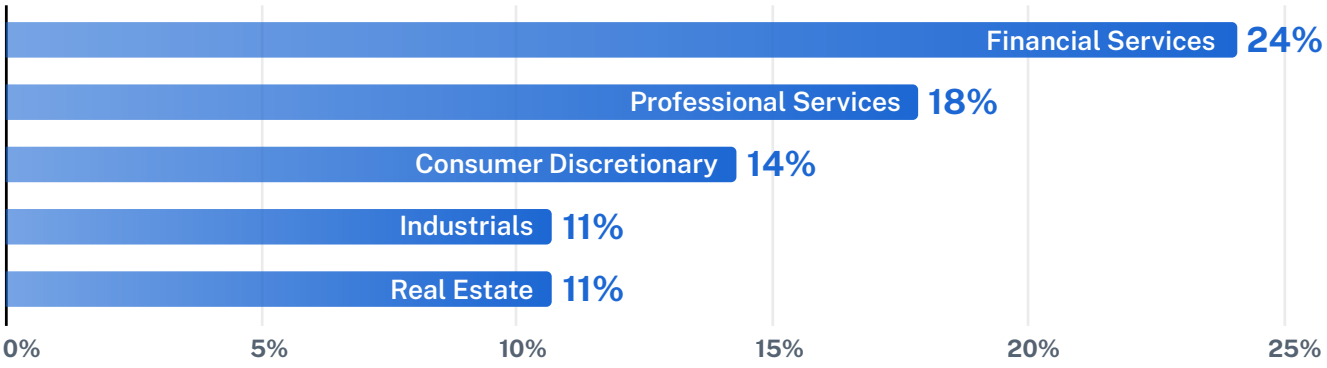
On March 3, 2021, Microsoft announced it had detected multiple exploits being used to attack on-premises versions of Microsoft Exchange Server in limited and targeted attacks. The exploits utilized a zero-day attack against four separate vulnerabilities in Exchange Server, which were disclosed on March 2, 2021.

Exploiting these four vulnerabilities together lets threat actors take control of an on-premise Exchange server and access email accounts or install malware, which could be used for other, long-term attack activities.

Microsoft Threat Intelligence Center (MSTIC) observed attacks carried out by Hafnium, a group assessed to be state-sponsored and operating out of China, primarily targeting US-based organizations running on-premises Exchange servers.

Supply chain attacks are becoming more common. Roughly 1,000 Coalition policyholders were exposed to the Microsoft Exchange vulnerability. Our in-house forensics team acted quickly, and we were able to notify and remediate the vulnerability for 98% of our impacted policyholders within a week of the disclosure. Unfortunately, not all were so lucky, and the remaining 2% of our customers experienced a claim. This incident accounted for 13% of H1 2021 claims. Fortunately for them, they have insurance! These incidents highlight the need for an insurance partner that understands and can help mitigate risk quickly during a crisis.

Business email compromise claims by industry — H2 2021



Looking ahead:

Cyber crime in 2021 and beyond

At Coalition we have unique insight into the cyber threat landscape and its impact on our policyholders. We expect the market will continue to evolve and our claims, incident response, and insurance teams share the following predictions for the remainder of 2021.

Ransomware will remain the single biggest threat for all organizations

Ransomware remains the most lucrative cyber criminal activity, and the widespread use of poorly secured remote access protocols and tools on the internet will continue to leave organizations open to ransomware attacks. As a result, we expect ransomware frequency to increase moderately. Conversely, we expect that ransomware severity will flatten as there is little leverage left to be gained beyond that which criminals already have after taking an organization's operations hostage.

The cyber insurance market will continue to harden throughout the year

It will be harder to qualify for cyber insurance, and the implementation of many common cybersecurity controls will increasingly be required as a condition of coverage. We predict that many insurance carriers will also begin to require companies to address identified vulnerabilities during the policy period or risk losing some (or all) coverage. Price increases, coinsurance, and sublimits on critical coverages are already happening, and will continue throughout 2021.

Supply chain attacks will be more common

Criminals will increase their targeting of software and service providers that other organizations rely upon. Supply chain attacks allow criminals to victimize a large number of organizations at once, rather than just one. As organizations increase their reliance on cloud software and service providers, they open themselves up to more risk—risk they will struggle to control.

Government regulation and scrutiny will increase

Following the Colonial Pipeline attack in May 2021 and other attacks on critical infrastructure, we expect to see considerably more policy focus on cybersecurity incidents. New York's Department of Financial Services formally released a cybersecurity framework, and President Biden recently signed an executive order to improve national cybersecurity. Not only do we expect to see more regulation, we expect to see more public frameworks from government institutions around the world, and new laws that will require far greater disclosure of cybersecurity incidents. However, these efforts may not have a material effect on the frequency or severity of claims unless they are accompanied by a serious effort to deter criminals themselves.

Criminal attacks will follow nation-state attacks

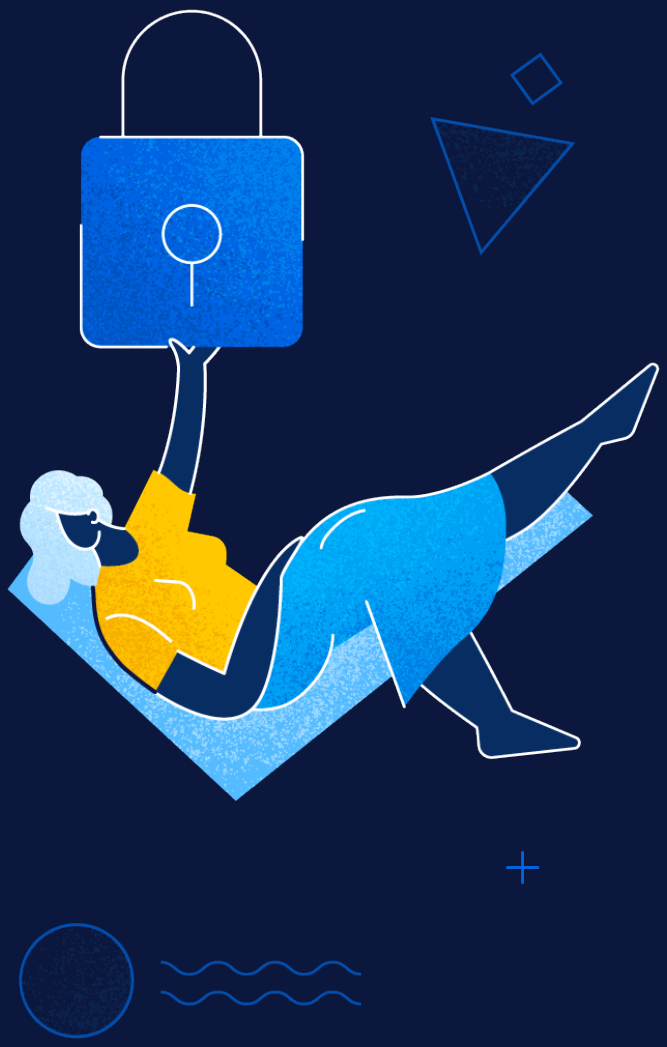
Several high-profile attacks over the past year, including against Mimecast, SolarWinds, and Microsoft Exchange, were believed to be instigated by nation-state actors. While these attacks are typically motivated by espionage rather than financial gain, the exploits used often eventually make their way into criminal hands, as occurred with the Microsoft Exchange vulnerabilities disclosed earlier this year. We expect this trend to continue.

Most cyber attacks will continue to be easily avoidable

Despite frequent claims by compromised companies that they've fallen victim to highly sophisticated attacks, most cyber attacks will remain anything but sophisticated. We predict that phishing, exploitation of remote network access points, exploitation of unpatched software with known vulnerabilities, and weak credentials will continue to be the main causes of cyber incidents. Basic controls to secure email, enable multi-factor authentication, and frequently patch software will remain the most effective controls for the foreseeable future.

Why Coalition

The past year has shown that cyber risk is increasingly impacting organizations of all sizes, yet many organizations remain unprepared. As cyber attacks increase in frequency and severity, it's more important than ever that companies take the time to understand their cyber risk and have the defenses in place to recover.



The insurance industry is uniquely positioned to fight cyber crime. Insurers have one thing in common that others (including cybersecurity companies) do not: a direct financial incentive to protect insured clients and prevent financial loss. Coalition was founded with the mission to solve cyber risk, and our technology-driven approach to underwriting, risk management, and incident response *works*. We proactively help our policyholders avoid potentially business-ending cyber incidents, and help them recover financially and operationally should the worst happen.

Regardless of whether you become a Coalition customer, we encourage you to understand your risk, implement controls to protect your organization from being a target, and procure cyber insurance. 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