CORVUS

Corvus Risk Insights Index

Q4 2021 | Cyber & Technology E&O

Q4 2021 | Cyber & Technology E&O

Hello there! Welcome to the inaugural Corvus Risk Insights Index. In this series of reports, we — members of the Corvus flock including data scientists, claims managers, and cybersecurity pros — will be sharing unique data and analysis drawn from Corvus's work in modeling and managing risk. From Corvus's founding, our mission has been to **make the world a safer place** by mitigating or eliminating the impact of adverse events. Crucially, this mission goes beyond just the organizations we insure; we hope that the insights shared in these reports will have a broader impact by adding to the body of information used by risk managers, IT departments, security researchers, and service providers to hone their offerings and approaches to keeping organizations safe.

These reports will be driven by data gathered from our proprietary security scanning technology and our database of claims information, as well as numerous other first- and third-party data sources utilized by our data science team in the service of modeling and analyzing risk to improve Corvus underwriting and risk management.

This edition focuses on Cyber & Technology E&O risk:

1. **Industry Spotlight:** A deep dive on litigation risk for tech companies (Technology E&O risk)
2. **Data Science Spotlight:** Trends in the use of tools and technologies that impact cyber risk
3. **Ransomware Trends:** Mid-year check-in on trends in ransomware
4. **Vulnerability Report:** Review of key recent exploits & vulnerability discoveries

If there's one key takeaway from this edition, it's that a focus on the basics of security can reap instant rewards. As we discuss in the Data Science Spotlight, relatively simple measures, such as making use of the scanning and filtering features available from your existing email provider, can make a serious difference in reducing risk. Simply put: a big security budget and a dedicated in-house team are not prerequisites to making an impact. Encouragingly, we're seeing trends indicate that organizations are starting to discover these opportunities. These low-effort, high-impact measures are more easily discoverable now, too, thanks to expanded availability of IT scanning technologies. After all, security is visibility: you can only protect what you know about.

Section 1: Industry Spotlight

Amplified Cyber Risks for Tech

Cyber risk isn't just a concern for the end users of software and IT products. For technology providers, a cyberattack linked to their products or services can mean significant costs from defending lawsuits brought by customers who suffered outages or lost data as a result of the incident — on top of any first-party remediation and recovery efforts. In insurance, these kinds of risks are referred to as "Errors and Omissions" (E&O).

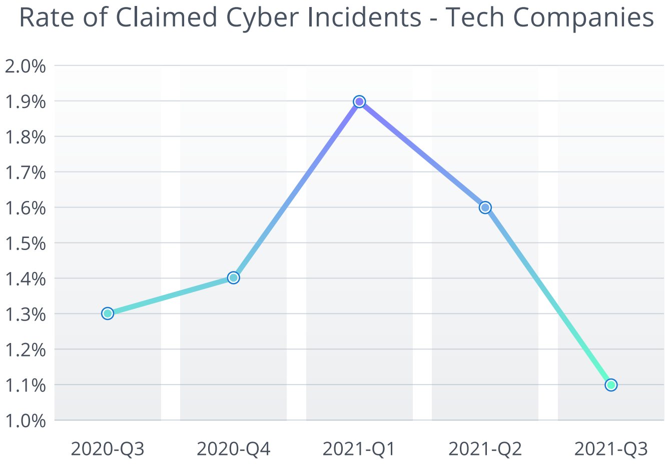
Attackers have realized that this added financial risk can turn into leverage. In July, a vulnerability in software provided by Kaseya led to the encryption of more than 50 managed service providers and in turn around 1500 customers of those MSPs. The ransom demand to Kaseya was rumored to be commensurately large, in the tens of millions.

While the worst case scenario is a ransomware attack that shuts down a customer's business entirely, more often an attack on a technology or services provider results in lost data, inability to access data, or the publication of sensitive data of the impacted technology or service provider and their customers. The customers who experience these issues may face financial or reputational harm and can litigate. These situations are more likely to avoid headlines, but still result in costs for the provider.

Frequency of Cyber Claims for Tech Companies

Cyber claims occur at a slightly lower rate for tech providers as compared to other industries. In Q1 '21 we saw the highest rate of cyber claims for tech companies in over a year, matching the rate of overall cyber claims for all types of organizations. That spike is attributed to the Microsoft Exchange vulnerabilities exploited by Hafnium and other threat actors in March 2021.

Despite lower frequency, ransomware attacks against a tech company can be costly as they tend to result in downstream impact to their customers. Customers may experience an inability to use the tech, or worse, may have their own data held within the tech compromised. For the companies that are providing technology services, a focus on resilience, in addition to prevention, is particularly critical. Knowing how to respond effectively if an attack does occur can mean the difference between containing issues to a small group of customers and a full catastrophe.

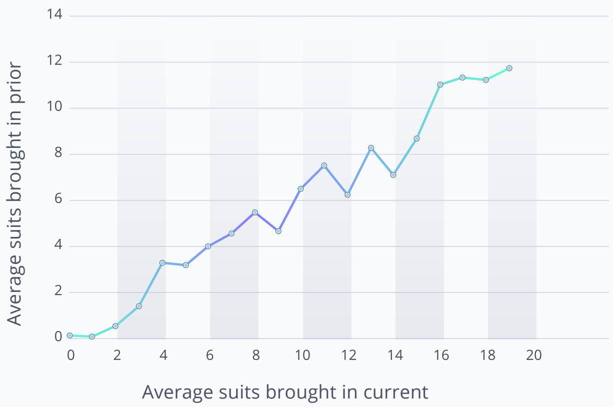


Claims from the cyber liability coverage within Corvus Technology E&O policies as a percentage of policies in force per quarter

Litigation Risk Factors

The litigation risk that comes after the crisis phase of a cyberattack (or any sort of incident that causes an outage) is where tech companies can see greater severity in claims. Our model of litigation risk focuses primarily on the past litigation activity of customers of a tech company (this is a strong predictor of future litigation — see right). But even without digging into a specific organization's litigation history, we do see some notable differentiation across industry and size.

Past Year Litigation vs. Current Year Litigation



Customer Size

Experienced Tech E&O underwriters won't find this shocking — an important factor in litigiousness is the size of the plaintiff. Above a certain size, organizations will have a general counsel on staff, and may have a legal department; large companies often have substantial legal departments and a firm on retainer. Unsurprisingly, then, the risk of getting sued by a customer multiplies the bigger that customer gets, looking at employee count as a proxy for size. When we examined companies that sued their technology providers, we found that a company with 250 or more employees is 216% more likely to sue their tech vendor than a company with 10 or fewer employees, and twice as likely as a company with 11-50 employees.

Likelihood of filing suit against a vendor, by employee

24%	**43%**	**59%**	**76%**
1-10	11-50	51-250	250+

Customer Industry

In the same analysis of companies that sued their technology providers, we also found substantial differences based on industry. Industries like Transportation and Public Administration sit right around the average rate of litigiousness we see across the entire database. Health Care entities are the least likely to sue, but the difference is only around 16% less than average. We see more differential on the high side, with media companies (publishers, TV networks, etc.) and metals manufacturers each nearly 50% more likely to sue than average. Insurers are around 23% more likely.

Likelihood of filing suit against a vendor, by industry

Health Care	**-16.2%**
Educational Services	**-15.4%**
Construction	**-7.19%**
Transportation & Warehousing	**+0.1%**
Public Administration	**+0.2%**
Retail Trade	**+15.5%**
Finance & Insurance	**+23.1%**
Manufacturing (metals)	**+45.4%**
Information (media)	**+47.5%**

Defendant Risk

Looking at the other side of the equation — the defendants, or the technology providers who may get sued by their customers — the analysis also yields some interesting findings at the cross section of industry and company size. Here similar trends follow, with larger companies presenting larger risk. But some classes, such as video game makers, defy the industry size trend by showing similar risk up and down the spectrum of size, often lower than it's assumed by underwriters. Other industries can provide insight when looking at both dimensions. For instance, hardware/ semiconductors is generally considered to be a high-hazard risk class, and while that's true of large businesses in the industry, small hardware makers appear less risky when viewed through this lens.

Section 2: Data Science Spotlight

Security Measures and IT: Post-COVID Trends

Trends in the use of certain types of software or IT services tend to move gradually in the aggregate. ("Transitioning to the cloud" has remained a stalwart conference topic for over a decade.) Something cataclysmic, like a pandemic or an unprecedented trend in attacks, is what it takes to make a noticeable difference in the short term. Last year saw both.

While we know COVID-19 caused rapid shifts in technology usage upon remote work's rise, we wanted to see what trends endured a year later. We looked at two major IT security measures through data gathered by our proprietary security scan, with time frames in early 2020 and mid-2021.

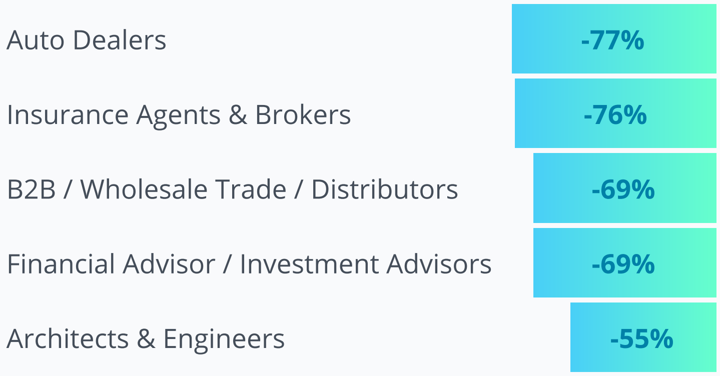
(The Decline of) Remote Desktop Protocol

With businesses already reeling from the pandemic, the first half of 2020 saw a crescendo of attacks linked to remote desktop protocol (RDP). RDP is a legacy method of providing remote access to computers or servers that is vulnerable to credential compromise because it is visible and accessible on the internet. Newer, safer ways of providing remote access now exist, which avoid having a Windows system exposed to the internet, but RDP has been slow to be replaced.

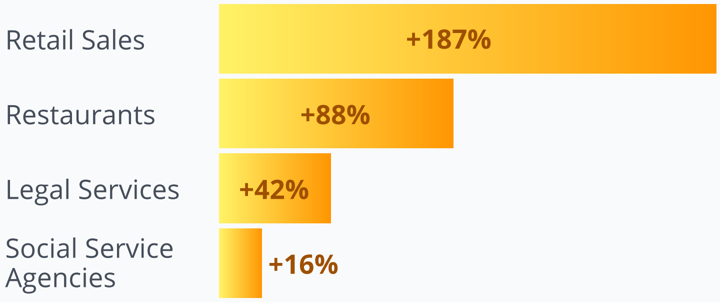
Our analysis shows that, thanks to the efforts of many security practitioners (and to scanning software that enables quick assessments of vast IT systems), the **overall presence of accessible RDP dropped by nearly 50% within a year**. Looking at individual industries, typically between 2% and 10% of organizations in a given industry had RDP accessible to the internet pre-pandemic; that range has shrunk down to 0-4%.

There was some variation in how much change certain industries experienced. Auto dealers and Insurance Agents and Brokers saw declines of around 75%. While the majority of industries (80%) saw a decline, a few, including retailers and restaurants, actually bucked the trend and saw increases in accessible RDP, likely because of how rare remote work was for these industries before COVID-19. (When looking to quickly stand up a brand new type of IT service, RDP would be a fast and easy option.)

Decrease in Accessible RDP (Select Industries)



Increase in Accessible RDP (All Industries)



Overall reductions in RDP exposure across industries were likely due to a successful awareness campaign by security practitioners and cyber insurers. Among Corvus policyholders, for example, the rate of RDP presence is consistently zero or near zero thanks to alerting technology implemented last year that notifies current and prospective policyholders about the presence of RDP. In fact, in the six months following implementation of the feature, the rate of ransomware claims among new Corvus policyholders dropped by 65%. Learn more

(A Boom in) Email Security Tools

Email phishing has continued to be the most popular method for threat actors to launch a variety of cyber crimes against businesses and organizations, from wire fraud to ransomware. Thankfully, the move to cloud/SaaS products hasn't left email security behind, and today there are a variety of tools that can make email communication safer while avoiding a costly hardware installation.

These cloud-based tools, which scan and filter incoming messages to anyone in the organization, are updated frequently to keep up with the latest phishing tactics, and are relatively easy to implement. Some email service providers even have scanning and filtering tools built into their product suites; these are often the easiest to enable, but may be less expansive in functionality than standalone services.

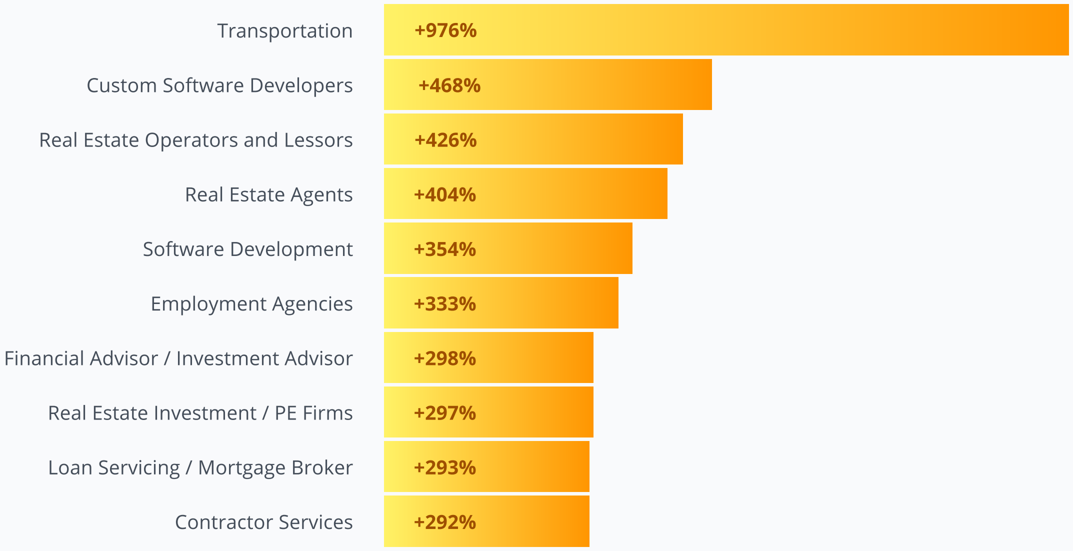
Looking at adoption of top-tier email providers (in terms of security features) and the use of add-on security software, we can see some clear trends.

This is another case where the pre-pandemic picture has shifted significantly: we saw **a 2.5x (158%) lift in the usage of email security tools** in aggregate.

In fact, many of the industries we studied saw an even larger 3-4x increase in use of email security tools, and not a single industry was flat or down on this measure. The industry with the lowest growth figure, K-12 schools, still notched measurable growth at 23%. Other highlights include two real estate categories that each had major jumps (albeit from low bases) of over 5x. Most impressively, the transportation category had nearly 1000% growth, from a low base of just 1.5% of its organizations using email security software pre-pandemic, to 16% a year later.

Still, after all that growth in adoption, the post-pandemic average across all industries is just **16.8%**. The use of these tools should be more widespread, but the trend is encouraging.

Top 10 industries showing an increase in email security provider usage



Note: for this analysis we excluded scans performed for existing policyholders since the risk mitigation services Corvus provides can lead to substantial changes in security measures that would skew our view of broader trends. All of the results studied were taken from scans performed at the point of quoting, for organizations that may or may not have later become Corvus policyholders. The data collected for the pre/post time frame is the three months leading into March 2020 ("pre-pandemic" for the U.S.) and March-May 2021.

Email Tools - Impact to Claims

In the previous section we covered the trend in the use of email security tools. But just how much of an impact do these tools have? Do they really move the needle?

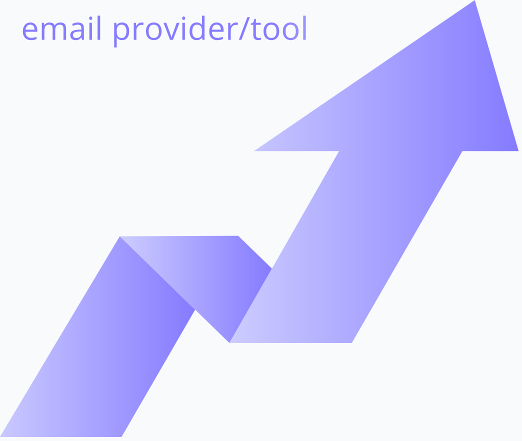
Seeking an answer to this question, our data science team analyzed the rates of phishing incidents among policyholders based on the email provider or email security tool the organization uses. For a simple comparison, looking at policyholders using an email security service or tool with a below-average rating (meaning a larger number of incidents) we see a substantial **45% increase in the likelihood of a phishing claim**, and a more than 2x increase in likelihood of any cyber claim, when compared to the group using above-average tools.

Below, we're showing the email security providers and tools with lowest rate of incidents among the 20 most popular with Corvus policyholders. Bear in mind, this is observational data. Many tools/providers *can* be used effectively to improve phishing safety, but may have customers who aren't aware of, or choose not to activate, all of the features available.

2x

likelihood of cyber claim

using a below-average email provider/tool



Top Email Tools & Providers

among 20 most-used by Corvus policyholders

Top Email or Managed Service Providers

- Network Solutions
- Google Mail
- GoDaddy Email

Top Email Security Tools

- N-Able
- Proofpoint
- Mailprotector

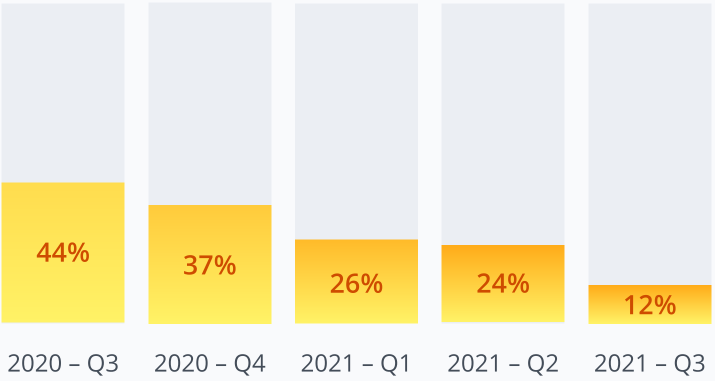
Ransomware Trends

Ransomware has become the defining force in cyber risk. That's beyond dispute. But it's not, as it's sometimes made to seem, moving inexorably in the wrong direction. As we'll show, it's not all "up and to the right." There's variation over time in how successful cybercriminals are at their endeavors, and even some cause for optimism.

How often are ransom demands met?

The ratio of ransoms demanded to ransoms paid is declining steadily. Despite efforts by criminals to double extort victims (see page 10) or find other ways to increase leverage, organizations have generally become better prepared to handle ransomware. Improvements to system backups are the major factor, enabling victims to stand up to criminals with confidence. More robust backup strategies include both better-protected internal backups as well as offsite backups that act as a failsafe.

Percentage of Ransoms Paid

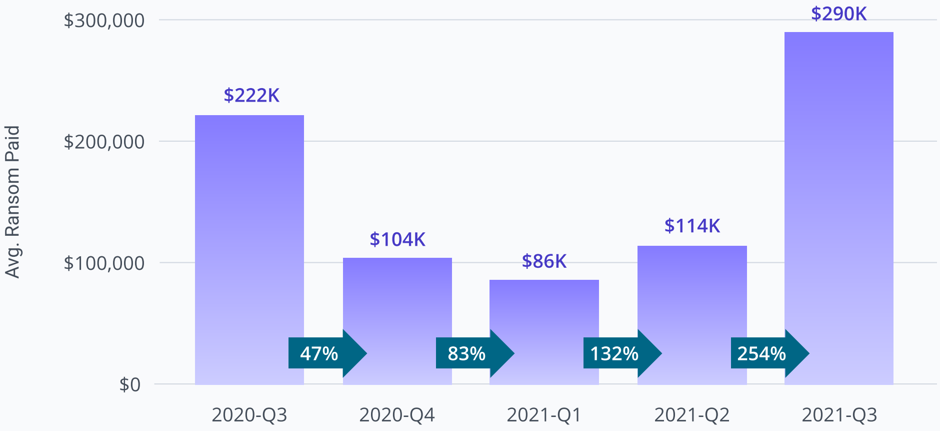


How much ransom is being paid?

The first half of 2021 saw lower quarterly averages for ransoms paid as compared with 2020, but Q3 saw a more than 2x rise Q/Q. The average of $290k for the quarter marks a return to $200k+ averages not seen for a year (see chart below). This rise in ransom costs is tempered by the reduction in the success rate of attacks noted above, and reduction in overall attack frequency (see next page).

When including the spike in ransom amounts in Q3, this year's overall average to date matches that of 2020s exactly, at $142,637 (2021) vs. $142,368 (2020).

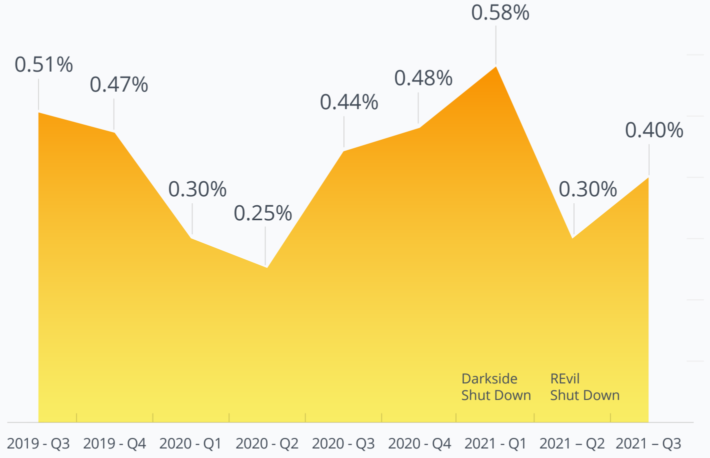
Average Ransom Paid by Quarter



Ransomware Incident Frequency

The frequency of ransomware tells a different story than the average costs. We saw a steady rise in frequency from Q2 2020 through Q1 2021, but frequency of ransomware dropped by 50% in Q2 and that rate has sustained through Q3. This dropoff is likely linked to the shutdown of two prolific ransomware groups, Darkside and REvil, in May and July 2021.

Ransomware Claims, Quarterly Rate

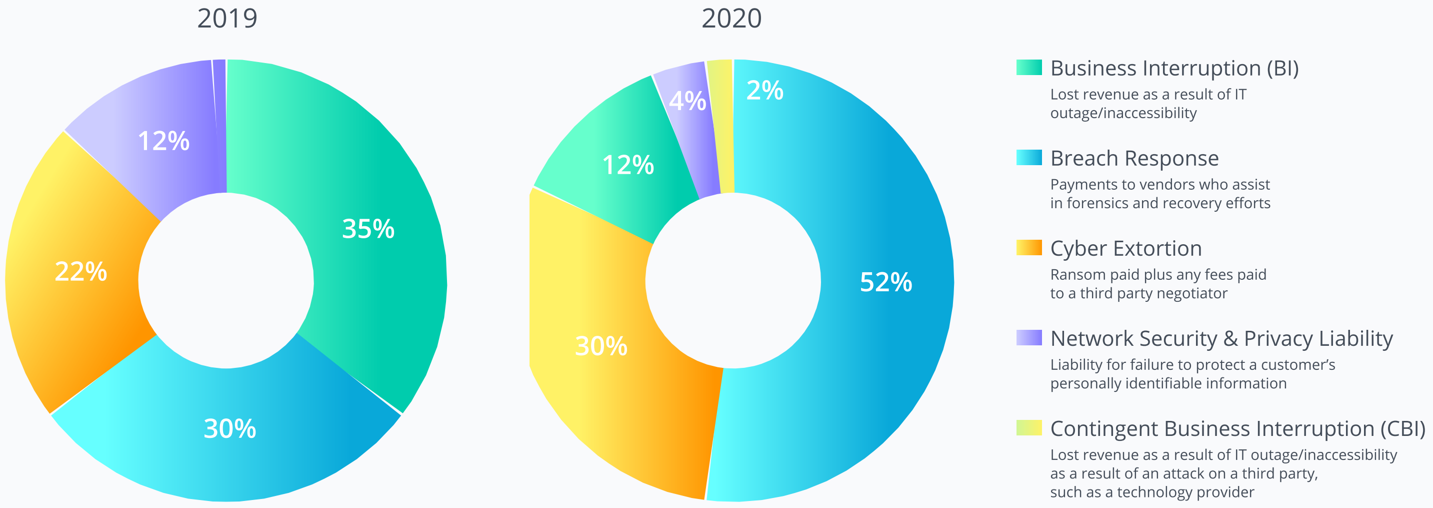


Anatomy of a Ransomware Claim

There has been a significant shift over the past three years in where the true cost of ransomware recovery lies. The cost of the ransom payment itself is rising as a share of the overall cost. It's a similar story for breach response costs — the costs of the vendors who assist in forensics and recovery efforts, for instance — increasing from 30% to 52%.

Meanwhile, business interruption (BI) costs have shrunk as a percentage. This is mostly due to improved preparedness and resiliency on the part of organizations, allowing for breach response professionals to handle ransomware situations efficiently and get companies back online faster.

Ransomware Claim Cost Centers
(Percentage of Total Claim Costs, Year)



Because Business Interruption costs have a long reporting lag, we aren't able to show interim 2021 figures without risking a misrepresentation of the data. We'll provide an update in our Q1 2022 report.

Double Extortion

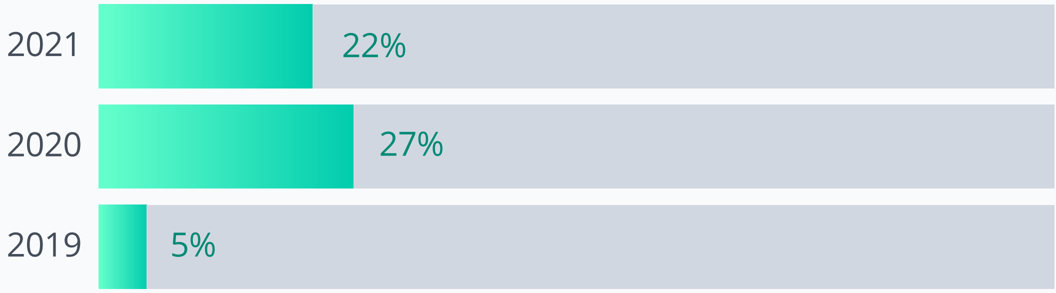
Data exfiltration, meaning the theft of data from a victim's IT system, is a tactic used by cybercriminals to "double extort" and increase leverage. One use case for the tactic is that if a victim is prepared to withstand encryption of their system (likely thanks to a good backup strategy) the criminals need a different reason to prompt a payment. By stealing sensitive data and threatening to expose it — which could leave the victim with regulatory fines, reputational damage, and more — the criminals may succeed in getting their demands met.

Another case would be for criminals to go back to the well. There have been cases reported where a victim has paid a ransom to unencrypt their system but, having revealed themselves to be a willing party, then receive a second ransom demand. The criminals will try to prove that they are in the possession of sensitive data and threaten to expose it unless they get the second payment.

Exfiltration is down slightly this year so far, from 27% of all ransomware incidents in 2020 to 22% this year to date. Prior to 2020 it was rare.

Despite the recent decline, we aren't expecting to see an extended decline in the tactic. Ransomware as a Service is shifting from an attack-based model to an access-based model. That is, criminal groups are not so focused on software that will enable the encryption of systems and make demands, but simply to guarantee access to a victim's system to then let the perpetrators decide how to act. In this context, it's likely that data theft will continue to occur, with or without the attendant ransom demands.

Percentage of Ransomware Claims Including Exfiltration



Section 4: Vulnerability Report

Key Vulnerability Review

March

Microsoft Exchange Server Vulnerability

Microsoft issued an alert on its blog concerning attack activity from a China-based threat actor it calls Hafnium. The U.S. Cybersecurity and Infrastructure Security Agency issued an emergency directive for government agencies to follow the steps it outlined, using information from the agency's activity alert on the matter. Learn more

April

Microsoft Exchange Server Vulnerability

Microsoft released patches for four new vulnerabilities relating to Microsoft Exchange Server software. Note that while this is the same type of software involved in zero-day vulnerabilities announced in early March, those announced in April were new and separate. Learn more

Pulse Connect Secure Vulnerability

Threat actors exploited four vulnerabilities in Pulse Connect Secure products, widely used for virtual private network (VPN) remote access. Learn more

May

Exim Mail Server 21Nails Vulnerability

The Qualys Research Team announced that it had discovered multiple critical vulnerabilities in the Exim mail transfer agent (MTA). These could allow for remote command execution attacks against those mail servers. Learn more

July

Kaseya VSA Alert

The REvil ransomware group attacked software provider Kaseya, creating downstream risk for customers of the company. Learn more

PrintNightmare Vulnerability

Microsoft issued an urgent out-of-band security patch to fix a critical vulnerability, CVE-2021-34527, in the Windows Print Spooler service that impacts all Windows Operating Systems. Learn more

August

Microsoft Exchange ProxyShell Vulnerability

CISA issued an urgent security update regarding ProxyShell vulnerabilities. Threat actors are leveraging the vulnerabilities to bypass access control and elevate privileges on the Exchange PowerShell backend, allowing for unauthenticated, remote code execution. Learn more

Microsoft Azure Cosmos DB Vulnerability

Security researchers announced a vulnerability, ChaosDB, that was associated with the cloud-based Microsoft Azure Cosmos Database (Cosmos DB). Learn more

September

Microsoft MSHTML Vulnerability

Microsoft Security Response Center (MSRC) reported on a security vulnerability, CVE-2021-40444, in the MSHTML engine. Learn more

VMware vCenter Server Vulnerability

VMware issued an advisory that a vulnerability CVE-2021-22005 in their vCenter Servers was being actively exploited. Learn more

Looking Ahead

Thanks for reading the inaugural Risk Insights Index! If you stuck around this long, we hope that means you found it interesting (and not that you're just looking for where to send hate mail). Either way, please send your thoughts to insights@corvusinsurance.com. In future editions, we promise to bring more unique findings and trend reports from Corvus focusing on, but not limited to, cyber risk. Look out for our next Index in late Q1 2022, where we'll look back at cyber trends in 2021 as a whole, including a deeper dive into how cyberattacks happen.

Report Contributors

Lori Bailey
Chief Insurance Officer

Jason Rebholz
Chief Information Security Officer

Lauren Winchester
Vice President, Risk + Response

Chris Hedenberg
Director, Data Science

CORVUS

About Corvus

Corvus is reimagining commercial insurance for a digital world by making insurance smarter, companies safer, and brokers more successful.

Corvus empowers brokers and policyholders with actionable insights to mitigate complex risks and reduce losses through the CrowBar digital platform, smart insurance products, and premier risk management services. Corvus is the world's largest specialty commercial InsurTech company.

Founded in 2017 by a team of veteran entrepreneurs from the insurance and technology industries, Corvus is backed by Insight Partners, Bain Capital Ventures, .406 Ventures, Hudson Structured Capital Management, Aquiline Technology Growth, FinTLV, Telstra Ventures, Obvious Ventures, and MTech Capital. The company is headquartered in Boston, Massachusetts, and has offices across the U.S.