
cybereason
2022
Ransomware
The True Cost to Business
A Global Study on Ransomware Business Impact

INTRODUCTION

CEO Insight

Ransomware continues to dominate the threat landscape in 2022. Organizations are under siege from a wide variety of threats, but ransomware offers threat actors a unique combination of very low risk with very high reward—which is why the volume of ransomware attacks nearly doubled from the previous year, and the total cost of ransomware was estimated to exceed $20 billion.

Ransomware began as little more than a new type of malware exploit with a different payload—generating revenue by extorting payment from victims—but it has evolved into a complex business model. The malware is just one element of the much larger ransomware operation—or RansomOp—that make today's attacks far more sophisticated and insidious.

Cybercrime gangs like Darkside, the group behind the Colonial Pipeline attack, REvil, the group behind the JBS attack, and the Conti ransomware group, whose attacks on multiple government bodies led President Rodrigo Chaves of Costa Rica to declare a national emergency, have developed ransomware-as-a-service models that mirror legitimate businesses, complete with customer service, human resources, and a network of suppliers and partners.

Ransomware is also more sinister because of the increasingly blurred lines between cybercrime gangs and nation-state adversaries who influence the objectives of ransomware attacks while also making it more difficult to bring the threat actors to justice.

> Our mission is to enable Defenders to reverse the adversary advantage. To advance that goal and help organizations to make better decisions about their security posture, we need concrete insights into the business impact of these attacks.

LIOR DIV
CEO, CYBEREASON

I often refer to these groups as "state-ignored," where nation-state adversaries look the other way as long as the ransomware targets align with their strategic goals, or "state-controlled," where the threat actors are executing attacks on behalf of and at the direction of the nation-state. The US Cybersecurity and Infrastructure Security Agency (CISA) reported that 14 out of 16 critical infrastructure sectors have been targeted by ransomware attacks.

Organizations that are hit by a ransomware attack face a no-win situation. The only options are to either ignore the ransom demand, rebuild and restore compromised systems from backups, and pray that the threat actor doesn't leak or sell your organization's sensitive data, or pay the ransom to obtain the decryption key from the attackers.

While paying the ransom may seem like the easier choice, our research this year proves once again that it does not pay to pay. Organizations that paid a ransom were frequently unable to recover all of their data, and many were hit by additional ransomware attacks—often by the same threat actors.

Given the ongoing threat that these attacks pose to organizations, this second annual *Ransomware: The True Cost to Business* study examines how ransomware continues to impact the business, the outcomes organizations are reporting after having been the target of a ransomware attack, and the strategies companies large and small are implementing to better prepare for an attack.

Our mission is to enable Defenders to reverse the adversary advantage. To advance that goal and enable organizations to make better decisions about their security posture, we need concrete insights into the business impact of these attacks. This report reveals the true cost and impact of ransomware, and it underscores that organizations need to Defend Forward with more proactive approaches to cybersecurity.

The best defense against ransomware attacks is to ensure your data is not stolen or encrypted in the first place through effective prevention, detection and response. It is my hope that your organizations will find this report insightful and that it will serve to inform your organization's strategies to remain undefeated by ransomware.

Key Global Results

80%
of those who paid were victims of a second attack

73%
targeted by at least one ransomware attack

68%
who paid once were hit again in less than a month for a higher ransom

41%
paid to expedite recovery

28%
paid to avoid downtime that could result in injury or loss of life

49%
paid to avoid loss in revenue

37%
forced to lay off employees

86%
reported increase in security budgets to fight ransomware

35%
reported C-level resignations following the attack

33%
forced to temporarily suspend business

64%
ransomware came from third-party supply chain

54%
who paid still reported system issues or corrupted data after decryption

33%
increase in ransomware attacks over 2021 study

88%
believe they have the right talent to protect their organizations from ransomware

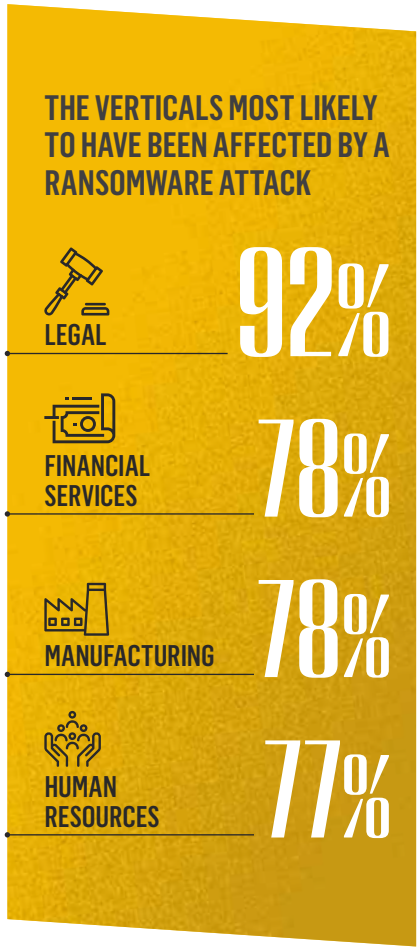
Ransomware Remains Pervasive

Ransomware continues to be a dominant concern for organizations. Despite significant action by the Biden Administration in the US, coordinated efforts by government and law enforcement agencies around the world, and an increased focus on ransomware, the volume of attacks nearly doubled in 2021.

Of the 1400+ cybersecurity professionals who participated in this second study, nearly three-quarters (73%) said their organization was targeted by at least one ransomware attack in the preceding 24 months, compared to just 55% of companies who had been targeted by at least one attack in our 2021 report, a staggering increase of 33% year over year.

73%

said their organization was **targeted by at least one ransomware attack in the preceding 24 months...** a staggering increase of 33% year over year.



Ransomware attacks can negatively impact an organization in many ways, with combined losses potentially reaching tens or even hundreds of millions of dollars. Last year's study revealed that the vast majority of organizations that had suffered a ransomware attack also experienced a significant business impact, whether revenue loss, reputational damage, unplanned workforce reductions, or in some cases business disruption..

Short-term impacts revealed in the report included disruption of critical business processes due to the inability to access critical systems and data, costs associated with incident response and other mitigation efforts, lost productivity, and the cost of the ransom payment itself if the organization chose to acquiesce to the extortion demand, among others.

Longer-term impacts included diminished revenue, damage to the organization's brand and reputation, the loss of key executives, employee layoffs, loss of customers and strategic partners, and the viability of the business altogether in some instances.

The results demonstrated some regional deviations, with organizations in Japan (95%), Italy (90%), and the UK (83%) among the most likely to have been targeted by a ransomware attack in the preceding two-year period, while organizations in the US (46%) and Germany (69%) were among the least likely to have been targeted.

While the majority of organizations participating in the study reported they were targeted by a ransomware attack, not all organizations experienced a negative business impact. Ransomware victims in the US fared the best (32%) and were least likely to have been negatively impacted. In comparison, organizations in Japan (69%), Italy (63%), and France (52%) were most likely to report an impact on their operations.

As well, there was some variance by industry vertical, with the Legal (92%), Manufacturing (78%), Financial Services (78%), and Human Resources (77%) sectors most likely to have been affected by a ransomware attack.

Ransomware is a lucrative business that will continue to be a threat. Attackers continue to find innovative ways to extort victims, so it is more crucial than ever for organizations to be able to defend against ransomware attacks.

Are Organizations Prepared?

Despite the ongoing cybersecurity talent shortage, the study revealed a significant increase in the number of respondents who believe their organizations have the right talent to defend against ransomware attacks: 88% this year vs. 60% last year, a nearly 50% increase year over year.

The other good news: nearly three-fourths of respondents indicated they believe their organization has the right contingency plans to manage a ransomware attack—a number that remained relatively unchanged year over year.

Respondents from the UK indicated a higher level of confidence in their people and policies at 94% and 77%, respectively. In comparison, participants in France expressed less confidence at 82% and 53%, and those in Singapore expressed the least confidence at 64% and 61%, respectively. By sector, Financial Services (95%) and Transportation (94%) had the highest confidence levels in their people, at 95% and 94%, respectively, while Education had the lowest confidence level in its people, at 71%, and in its processes, at 53%.

This is particularly concerning because colleges and school systems are frequent ransomware targets. Lincoln College, a 157-year-old historically black college in the US, announced that it is permanently closing down after being unable to access recruitment and fundraising systems for months following a December 2021 ransomware attack.

Ransomware and the Impact to the Business

While many respondents believe their business is prepared for a ransomware attack, their faith may be misguided. Our year-over-year data shows a significant disconnect and a false sense of confidence between how prepared respondents say they are vs. how prepared their organizations actually are to deal with a successful ransomware attack.

Of the organizations that reported losses from a ransomware attack, more than two-thirds (67%) said their combined **losses reached between $1 million and $10 million (USD),** while 4% estimated staggering losses **in the range of $25 million to $50 million.**

reported their organization was **forced to lay off employees** following the attack, an almost 30% increase over the 2021 report.

reported C-level resignations following a ransomware attack.

acknowledged they were forced to **temporarily suspend business operations,** a jump of 7 percentage points year over year.

Why Organizations Choose to Pay a Ransom

Of the organizations that paid one or more ransom demands following successful attacks, nearly half (49%) said their primary motivation for paying was to avoid any loss of revenue, while 41% cited the need to expedite recovery as the main driver for payment, both of which seemingly make sense from a business viability and continuity standpoint.

Some companies decided to pay the ransom because they weren't prepared for a ransomware attack. For example, 27% said they paid the ransom because they hadn't backed up their data. One-third (34%) indicated they were simply too short-staffed to attempt an effective response without the assistance of the attackers, both of which are preventable conditions for organizations that take the threat of ransomware seriously and are indicators that these organizations simply aren't prepared.

Top Motivations to Pay

49%
TO AVOID REVENUE LOSS

41%
TO EXPEDITE RECOVERY

27%
TO RECOVER DATA

34%
SHORT-STAFFED

28%
TO AVOID DOWNTIME THAT COULD RESULT IN INJURY OR LOSS OF LIFE

The decision to pay a ransom demand is not easy, especially for organizations with a critical infrastructure designation like those in the Healthcare sector. In cases where ransomware prevents access to crucial systems and data needed to provide care, the consequences could be dire the longer the attack persists. This urgency explains why nearly one-third of respondents (28%) said they paid the ransom demand because any delays in remediation could result in injury or loss of life.

This research demonstrates that paying the ransom doesn't guarantee a faster recovery from the attack, despite the claims attackers may make to entice organizations to pony up. In fact, of the organizations that reported having paid a ransom demand, only 42% said the payment resulted in restoration of all systems and data, a significant decrease from the 51% who said they fully recovered systems and data in the 2021 study. Furthermore, 54% said that system issues persisted or that some data was corrupted after decryption, up from 46% in 2021. This data strongly suggests that it still does not pay to pay.

Paradoxically, 78% of organizations that indicated they did not pay a ransom said they were able to fully restore systems and data without receiving the decryption key at all. Given the counterintuitive results here, one must ask why the outcomes would be better for organizations that did not pay a ransom. Were they simply better prepared to respond?

Paying the ransom DOESN'T GUARANTEE a faster recovery from the attack.

It Still Does Not Pay to Pay

One of the toughest decisions a business will ever make is whether to pay a ransom demand following a successful attack. While remediation expediency is certainly a primary consideration, organizations need to weigh a host of other factors as well, including:

- **Will the attackers honor their promise** to provide a decryption key and restore access to all systems and data?
- **What if the data gets corrupted** during the decryption process?
- **What if the attackers reside** in a country subject to sanctions where a ransom payment could be considered a criminal violation?
- **What if paying a ransom demand encourages** the threat actors to launch another ransomware attack against the organization?
- **Aside from delayed data and system recovery,** what are the other risks to the victim organization if the ransom demand is not met?

Nearly
80% of those who paid were hit a second time
and close to half the time by the same attackers.

WHY IT STILL DOESN'T PAY TO PAY

68%
were hit a second time within a month a month and with a higher ransom demand

6 out of 10
weren't able to recover their data

This decision is particularly difficult for any organization to make in the heat of incident response. There are no clear-cut best practices to follow that work for every organization in every circumstance. Every ransomware attack scenario needs to be evaluated on a case-by-case basis because each infiltration, attack group, victim organization, jeopardized data set, and impacted third-party situation is unique, and there are numerous factors that need to be considered when determining whether or not to make a payment.

That said, this research found that it clearly does not pay to pay. Of the organizations that chose to pay a ransom demand, the vast majority (nearly 80%) indicated they were victims of at least one subsequent ransomware attack. Of those who were hit a second time with ransomware, nearly half (48%) indicated the attack was perpetrated by the same attackers, which remained unchanged from the 2021 study.

Two-thirds (68%) who paid a ransom and were hit again reported that the second attack came less than a month after the first and that the threat actors demanded an even higher ransom amount the second time around. Of the organizations that paid a ransom following the first attack, nearly half (44%) also paid the second ransom demand, and nearly one in ten (9%) said they paid a ransom demand three times or more.

Let those statistics sink in: nearly 8-out-of-10 companies that paid a ransom were hit by a second ransomware attack—almost half of which were perpetrated by the same threat actors. Adding insult to injury, more than two-thirds of those subsequent attacks demanded a higher ransom than the initial attack, and nearly 6-out-of-10 organizations were unable to recover all of their systems and data even after paying the ransom.

Our research found that certain industry segments are virtually guaranteed to be hit a second time after paying a ransom demand. Companies in the Legal (100%), Human Resources (100%), Engineering (91%), and Manufacturing (85%) sectors were most likely to have suffered a second attack after having paid a ransom. Larger organizations with more than 1,500 employees were also preferred targets for repeated attacks (88%).

The big takeaway from both this year's study and the last is that it really does not make sense to pay a ransom demand unless there is the risk of losses that go beyond monetary costs, such as when human life is at risk. Overall, the cost of preventing a ransomware attack from being successful is lower than the combined cost of paying the ransom and all the associated costs of recovery when responding to a successful ransomware attack–possibly multiple times by the same threat actor.

Overall, the cost of preventing a ransomware attack from being successful
is lower than the combined cost of paying the ransom
and all the associated costs of recovery and all the associated costs of recovery when responding to a successful ransomware attack–possibly multiple times by the same threat actor.

Most Dangerous Ransomware Attack Vectors

Ransomware attacks involve a variety of infection vectors, but ransomware actors traditionally prefer some methods over others. In a 2020 study, researchers found that unsecured Microsoft Remote Desktop Protocol (RDP) connections were leveraged in over half of all ransomware attacks. This was followed by phishing emails at approximately a quarter of all ransomware infections and the exploitation of software vulnerabilities at 12%.

A proprietary protocol developed by Microsoft, RDP enables users to connect to other computers over a network connection remotely. This protocol necessitates that both computers involved in the connection run RDP software.

As noted by ZDNet, some digital crime groups specialize in scanning the web for these exposed ports. When they find them, they carry out brute-force attacks to gain access. They can then sell that access on Dark Web marketplaces, giving attackers like ransomware groups an opportunity to establish a foothold in an organization's network.

Then there are the attacks that leverage exploits of known and unknown vulnerabilities. Let's revisit the phishing scenario discussed above, in which an attack email has an embedded link that redirects a target to a website serving up an exploit kit. A phishing email might be the initial attack vector in this case, but it's not the ransomware payload delivery method.

In this case, the exploit kit functions as the delivery vector. It evaluates things like the target's web browser, operating system, and/or other software running on the device for vulnerabilities. If it detects a supported vulnerability, the exploit kit activates to install ransomware on the victim's machine.

Evolution of Ransomware Attacks to RansomOps

Ransomware attacks have evolved dramatically over the last few years, from a small cottage industry conducting essentially nuisance attacks like phishing and drive-by exploits to a highly complex business model known for its efficiency, specialization, innovation, and technical sophistication.

While broad, random attacks are still prevalent, ransomware purveyors are moving away from high-volume attacks with low ransom demands in favor of more focused, custom attacks aimed at organizations selected for their ability and likelihood to pay multi-million-dollar ransom demands. It is becoming increasingly common for ransomware attacks to involve complex attack sequences in low-and-slow campaigns designed to infiltrate as much of the targeted network as possible versus infecting a single machine with the ransomware payload.

It is becoming increasingly common for ransomware attacks to involve **complex attack sequences in low-and-slow campaigns** designed to infiltrate as much of the targeted network as possible versus infecting a single machine with the ransomware payload.

Of the organizations that suffered a ransomware attack in the last 24 months:

reported that the attackers were in their networks for **up to six months** before being detected.

21% said it was **seven to twelve months** of dwell time.

said attackers were in their networks **for a year.**

The silver lining: there are potentially weeks or even months' of detectable activity that could allow organizations to disrupt an attack before it results in serious impact, provided they have the right tools in place to detect the RansomOps attack sequence early versus later in the kill chain at payload delivery.

These more complex ransomware operations, or *RansomOps*, involve highly targeted, complex attack sequences conducted by sophisticated threat actors. Cybereason recently published a report titled *RansomOps: Inside Complex Ransomware Operations and the Ransomware Economy* that examines the growing threat from elaborate ransomware operations and the burgeoning Ransomware Economy and provides prescriptive guidance for organizations.

A joint report issued by the US, Australia, and the UK in early February 2022 and published by CISA specifically noted the increasing complexity observed in ransomware operations, stating, "ransomware tactics and techniques continued to evolve in 2021, which demonstrates ransomware threat actors' growing technological sophistication and an increased ransomware threat to organizations globally."

Unlike early iterations of ransomware attacks that relied on "spray-and-pray" tactics to infect large numbers of victims while seeking relatively small ransom demands, RansomOps attacks are much more intricate and akin to the stealthy operations conducted by nation-state threat actors.

RansomOps also involve a great deal of reconnaissance on the targets, which are carefully chosen for their ability to pay substantial ransom demands and high likelihood to pay, given they may be in an industry with the potential for significant ripple effects should their operations be disrupted, such as with Healthcare and other critical infrastructure organizations.

With a RansomOps campaign, the actual ransomware payload that encrypts data happens essentially at the tail-end of the attack. Of the organizations that suffered a ransomware attack in the last 24 months, 63% reported that the attackers were in their networks for up to six months before being detected, 21% said it was seven to twelve months of dwell time, and 16% said attackers were in their networks for a year or more before security teams became aware of the network compromise.

The silver lining: there are potentially weeks or even months' of detectable activity that could allow organizations to disrupt an attack before it results in serious impact, provided they have the right tools in place to detect the RansomOps attack sequence early versus later in the kill chain at payload delivery (more on mitigation strategies below).

Supply Chain Attacks on the Rise

The shift to more complex RansomOps attacks has also led to a rise in supply chain attacks. A supply chain attack enables attackers to focus on compromising just one organization, which then allows them to compromise the entire customer base. The attack against managed IT services provider Kaseya in 2021 that led to further attacks on their customers is a prime example of a supply chain attack.

How serious is the supply chain threat? In May 2022, CISA, the NSA, FBI, and an international coalition of cyber authorities issued a joint advisory warning of an increased risk of supply chain attacks designed to compromise Managed Services Providers (MSPs) and their customers.

"Supply chain vulnerabilities are amongst the most significant cyber threats facing organisations today," said Lisa Fong, Director of New Zealand's National Cyber Security Centre. "As organisations strengthen their own cyber security, their exposure to cyber threats in their supply chain increasingly becomes their weakest point. Organisations need to ensure they are implementing effective controls to mitigate the risk of cyber security vulnerabilities being introduced to their systems via technology suppliers such as managed service providers. They also need to be prepared to effectively respond when issues arise."

In this study, most organizations (64%) that suffered a successful ransomware attack in the last 24 months indicated the primary infection vector was a third-party supply chain compromise. Small to medium-sized organizations were more likely to be compromised via supply chain attacks, while larger organizations were more apt to be infected by direct attacks on their environments.

64%

that suffered a successful ransomware attack in the last **24 months** indicated the primary infection vector was a third-party supply chain compromise.

Data Exfiltration and Double Extortion

Organizations have adapted to the rising threat of ransomware attacks with improved data backup practices, so they can simply restore their data if necessary. Cybercriminals have responded by introducing additional incentives for organizations to pay the ransom. While lateral movement through the targeted network is a primary goal for RansomOps threat actors to maximize both the impact on the targeted organizations and the potential ransom payout, these more complex operations often also seek to exfiltrate sensitive data from the victim before detonating the encryption payload so they can leverage it to force a ransom payment through double extortion techniques.

With double extortion, the ransomware encrypts the victim's data and demands payment in exchange for a decryptor within the ransom note, as expected. However, the threat actor can also apply additional pressure to victims who would not usually pay a ransom by threatening to leak or sell the exfiltrated data. With double extortion, the options for organizations become more limited.

According to reports, only one ransomware gang was using the tactic in 2019, but by the end of Q1 2021, researchers observed ransomware attacks that included threats to publish exfiltrated data if a ransom demand was not paid had increased to 77% of all ransomware attacks.

Data Types Targeted for Double Extortion

The growth in double extortion raises an important question: what types of data do ransomware attackers tend to target for exfiltration to leverage for double extortion? It usually depends on the affected organization, but there are some common data categories that ransomware actors typically pursue:

- **Protected Health Information (PHI):** This includes medical records, diagnosis details, and patient medical insurance data. Attackers target this data category because they know that Healthcare organizations need anytime access to medical information to render patient care on a timely basis. Hence, they changed their tactics during the COVID-19 pandemic to include exfiltration of this kind of data.
- **Personally Identifiable Information (PII):** Which includes birth dates, physical addresses, email addresses, Social Security numbers (SSNs), and so on. Ransomware actors can monetize the information and sell it on the Dark Web as part of a complete identity profile. Buyers can then use that information to conduct different types of identity theft or fraud.
- **Account Credentials:** Consisting primarily of usernames and passwords, account credentials are essential to ransomware actors. Attackers need those details to infect as much of a target's network as possible.
- **Intellectual Property (IP):** Intellectual property includes new product releases and/or details that are integral to a victim's line of business or details on their customer base. As with the theft of sensitive personal details, ransomware actors can monetize a victim's intellectual property on the Dark Web or hand it over to a state sponsor. A competing organization can then purchase the information on the black market and use it to undermine the victim's business objectives. Alternatively, a competing state government can use it to advance their interests at the expense of the victim's host country.

In our study, of the organizations that suffered a ransomware incident in the last two years, 54% indicated the attackers attempted to or actually exfiltrated sensitive customer data, 34% went after PII, 30% targeted intellectual property (IP), and 27% went after PHI.

Top Data Types Targeted for Double Extortion

27%
PHI

34%
PII

54%
SENSITIVE CUSTOMER DATA

30%
IP

Ransomware's Impact on Security Budgets

The steady increase in the volume, complexity, and severity of ransomware attacks is driving increases in security budgets, with 86% of respondents indicating an increase in their security budgets to defend against ransomware attacks. Overall, two-thirds (66%) of respondents stated their security programs increased significantly-between 11% and 50%.

The average increase in security budgets across all participants in the study was 20%, demonstrating that ransomware is among the leading drivers for security spending across organizations of all sizes and industry verticals. So, where are organizations investing the extra budget to reduce the risk posed by ransomware attacks? This study reveals that budget allocations for cyber insurance policies were the top line item for increased spending.

of respondents indicated their organizations have a cyber insurance policy in place, up from 75% in the 2021 report. Of those with cyber insurance, **84% indicated their policies include coverage** specifically for ransomware attacks, up from just 54% in last year's report.

Since it was introduced to the market, cyber insurance adoption has been rapid and widespread, with 93% of respondents indicating their organizations have a cyber insurance policy in place, up from 75% in the 2021 report. Of those with cyber insurance, 84% indicated their policies include coverage specifically for ransomware attacks, up from just 54% in last year's report.

Generally, the larger the organization, the less likely they were to have cyber insurance for ransomware attacks. In fact, the larger the company, the less likely they were to have any cyber insurance at all, with 9% of companies with 1,500 or more employees reporting no cyber insurance protection.

The other budget winners in the effort to counter ransomware attacks were hiring additional security talent at 51% and additional security awareness training for employees at 50%. Organizations in Germany and Japan were most likely to invest more funds into hiring at 61% and 60%, respectively, while organizations in the UAE (40%) and Singapore (41%) were the least likely to spend the additional budget on new hires.

Surprisingly, the addition of new security technologies like NGAV, Endpoint Protection, and Endpoint Detection and Response solutions was a priority for 47% of organizations. It is interesting to note that investment in new technologies designed to prevent or disrupt ransomware attacks was only the fourth most common choice for where to allocate additional security budget.

This may be due to the fact that most of the organizations participating in the study have already made significant investments in prevention, detection and response solutions, but given the level of increased investment in cyber insurance, one might conclude that these organizations are not necessarily confident that they have the right solutions in place to adequately defend against ransomware attacks.

While cyber insurance can be an effective tool for transferring some of the risk of a ransomware attack, it doesn't mitigate all of it or provide any meaningful defense. Even if a cyber insurance policy covers a ransom demand, it may not cover a number of other financial consequences, such as lost revenue, cost of remediation, higher insurance premiums, regulatory fines, legal fees, and the like.

What's more, cyber insurance will not protect an organization from being among the 8-out-of-10 that are hit with a second ransomware attack—and it is doubtful that cyber insurance would cover back-to-back ransom payments within a month.

Defending Against Ransomware and RansomOps Attacks

Once an organization has been compromised with ransomware, no clear-cut "best option" is available. If the ransom is not paid, business may grind to a halt for days or weeks as data is manually restored from backups—assuming the organization has backups.

If a ransomware attack includes data exfiltration for double extortion, not paying the ransom also means accepting the risk that sensitive data and intellectual property may be exposed publicly—and the legal and regulatory consequences that can stem from such exposure. Again, the financial, legal, regulatory, and reputational impact of a ransomware attack—including lost business and productivity and the cost of recovery efforts—can often exceed the ransom demand.

The alternative is to pay the ransom, but that comes with issues and risks as well. As noted earlier, many organizations that pay the ransom are able to regain access to their data but find that some or all of it has been corrupted. The decryption tool provided by ransomware attackers is often buggy or slow, forcing companies to restore from their backups even after paying the ransom. There is also no guarantee that your data won't still be sold online after paying the ransom.

The best option for defending against ransomware is to be proactive and prevent an attack at the outset, to detect and disrupt an attack in progress as early as possible, and to be prepared to respond to a successful attack swiftly.

Guidance to Defend Against Ransomware

- FOLLOW SECURITY HYGIENE BEST PRACTICES
- CONDUCT PERIODIC TABLE-TOP EXERCISES
- ENSURE KEY STAKEHOLDERS CAN BE REACHED
- DEPLOY ENDPOINT AND EXTENDED DETECTION AND RESPONSE
- LOCK DOWN CRITICAL ACCOUNTS FOR WEEKEND AND HOLIDAY PERIODS
- ENSURE CLEAR ISOLATION PRACTICES
- EVALUATE MANAGED SECURITY SERVICES PROVIDER OPTIONS
- IMPLEMENT MULTI-LAYER PREVENTION CAPABILITIES

- **Follow Security Hygiene Best Practices:** This includes timely patch management and ensuring operating systems and other software are regularly updated, offsite data backups, implementing a security awareness program for employees, and deploying best-in-class security solutions on the network.
- **Implement Multi-Layer Prevention Capabilities:** Prevention solutions like NGAV should be standard on all enterprise endpoints across the network to thwart ransomware attacks leveraging both known TTPs as well as custom malware.
- **Deploy Endpoint and Extended Detection and Response (EDR and XDR):** Point solutions for detecting malicious activity like a RansomOps attack across the environment provides the visibility required to end ransomware attacks before data exfiltration occurs or the ransomware payload can be delivered.
- **Ensure Key Stakeholders Can Be Reached:** Responders should be available at any time of day as critical mitigation efforts can be delayed during weekend/holiday periods. Having clear on-call duty assignments for off-hours security incidents is crucial.
- **Conduct Periodic Table-Top Exercises:** These cross-functional drills should include key decision-makers from Legal, Human Resources, IT Support, and other departments all the way up to the executive team for smooth incident response.
- **Ensure Clear Isolation Practices:** This can stop further ingress into the network or the spread of ransomware to other devices or systems. Teams should be proficient at disconnecting a host, locking down a compromised account, blocking a malicious domain, etc. Testing these procedures with scheduled or unscheduled drills at least once every quarter is recommended to ensure all personnel and procedures perform as expected.
- **Evaluate Managed Security Services Provider Options:** If your security organization has staffing or skills shortages, establish pre-agreed response procedures with your MSPs so they can take immediate action following an agreed-upon plan.
- **Lock Down Critical Accounts for Weekend and Holiday Periods:** The usual path attackers take in propagating ransomware across a network is to escalate privileges to domain-level admin and then deploy the ransomware. Those highest privilege accounts, in many cases, are rarely required to be in use during the weekend or holiday breaks. Teams should create highly-secured, emergency-only accounts in the Active Directory that are only used when other operational accounts are temporarily disabled as a precaution or inaccessible during a ransomware attack. Also, take similar precautions with VPN access in limiting its availability during the weekend depending on business needs. For more information on Weekend and Holiday ransomware threats, refer to our other 2021 study, Organizations at Risk: Ransomware Attackers Don't Take Holidays.

SURVEY METHODOLOGY

The survey was conducted by Censuswide in April 2022 on behalf of Cybereason. A total of 1,456 cybersecurity professionals from organizations with 700 or more employees took part in the survey—with participants from the United States (24%), United Kingdom (17%), Germany (10%), France (10%), Japan (10%), Italy, (7%), South Africa (7%), United Arab Emirates (7%), and Singapore (7%). The survey sample includes responses from a variety of industry segments. Technology has the highest representation in the survey at 37%, followed by Manufacturing (14%), and Finance (10%). The rest of the survey participants came from Education, Healthcare, Legal, Transportation, or other industries. There is a range of different size companies represented. Smaller organizations with 700-999 employees make up just over half (52%) of the survey participants. Companies with 1000 to 1,499 employees comprise one-third (33%), with organizations larger than 1,500 employees making up the remaining 15%.

cybereason

ABOUT CYBEREASON

Cybereason is the XDR company, partnering with Defenders to end attacks at the endpoint, in the cloud, and across the entire enterprise ecosystem. Only the AI-driven Cybereason Defense Platform provides predictive prevention, detection and response that is undefeated against modern ransomware and advanced attack techniques. The Cybereason MalOp™ instantly delivers context-rich attack intelligence across every affected device, user, and system with unparalleled speed and accuracy. Cybereason turns threat data into actionable decisions at the speed of business. Cybereason is a privately held international company headquartered in Boston with customers in more than 40 countries.

Learn more at **www.cybereason.com**