CRA | Business Intelligence
A CyberRisk Alliance Resource

State of Ransomware: *Invest now or pay later*

February 2022

Sponsored by

Attivo NETWORKS

eSENTIRE

MENLO SECURITY

State of Ransomware: Invest now or pay later

FINDINGS FROM A JANUARY 2022 RESEARCH STUDY

BACKGROUND

It's the kind of note that grabs you by the shirt and doesn't let go: "All of your files are stolen and encrypted!"

The next thing you read is the extortion demand: pay up, or else.

Enterprise-level organizations were jolted by such messages in massive numbers in 2021. Shmuel Gihon, a threat intelligence researcher at Cyberint, recently wrote in SC Magazine that based on his research, the *US suffered by far the most significant number* of ransomware breaches with 1,352 "Big Game" attacks in the last year, followed by France with 146, Canada at 140 and the UK with 139.

While Gihon's analysis focused on big-game attacks that target enterprises with the deepest pockets, all organizations are at risk, whatever the industry or size.

Ransomware gangs are increasingly brazen. According to an analysis from blockchain research firm Chainalysis, the total value of ransomware paid in cryptocurrency was $600 million in 2020. It will likely surpass that number in 2021 when the final tally is done. "In fact, despite these numbers, anecdotal evidence, plus the fact that ransomware revenue in the first half of 2021 exceeded that of the first half of 2020, suggests to us that 2021 will eventually be revealed to have been an even bigger year for ransomware," the firm *wrote*.

Those scenarios mirror the results of a survey CyberRisk Alliance's Business Intelligence Unit conducted in January 2022. Many organizations continue to struggle ferociously with ransomware and

attackers have a clear edge today. Organizations continue to struggle at detection and response. But the news isn't all bad: Most respondents are taking additional steps that should prove helpful in their defense against ransomware in the years ahead.

"Our research confirms ransomware is still a big problem and cyber insurance is not the answer. Organizations will need to spend more to address ransomware in 2022, but it takes time to implement these solutions." **– Matt Alderman, EVP, CyberRisk Alliance**

RESEARCH METHODOLOGY

The data and insights in this report are based on an online survey conducted in January 2022 among 300 IT and cybersecurity decision-makers and influencers. All were in the United States except for 1% from Canada. Respondents represented organizations of all sizes and industries.

Organization size breakouts (sum is not 100% due to rounding):

- Small (1–99): **31%**
- Medium (100–999): **35%**
- Large (1,000–1,999): **28%**
- Enterprise (10,000 or more): **7%**

Industry breakouts:

- Manufacturing: **16%**
- High-tech/IT: **15%**
- Business or professional services: **15%**
- Retail or ecommerce: **12%**
- Financial services and insurance: **8%**
- Other (healthcare, education, transportation, government, non-profits, media, energy, and utilities): **34%**

Survey objectives were to gauge how well organizations were able to keep up with the latest ransomware trend. Research respondents were asked to provide their input about their ransomware experiences, how they are managing ransomware risks, as well as their overall resilience to ransomware events. Participants responded to structured survey questions and were encouraged to provide corresponding comments where applicable. The survey was conducted by the Business Intelligence Unit of CyberRisk Alliance.

EXECUTIVE SUMMARY

Ransomware attacks continue at a blistering pace because organizations remain vulnerable to the exploits bad actors use. Organizations are vulnerable at their endpoints. Staff can easily be tricked into clicking on links that provide attackers with a way in. Once there, they find it all too easy to move internally, either by identifying exploitable systems or by swiping user credentials. In many of the cases we surveyed, ransom was paid. And despite efforts to bolster defenses, many continue to struggle at detection and response.

Ransomware attackers are known to attack vulnerable systems opportunistically, and they are known to study target organizations to try and identify exploitable weaknesses. Sometimes they will send mass phishing attacks and then steal and encrypt the data of whomever is gullible enough to respond. Other times they will spear phish key people in an organization who they know have access to business-critical systems or valuable data.

The ransomware racket is complex. No longer is it just gangs who develop the malware and conduct the attacks and extortion. Today, it's a tiered business model where criminal interests develop and then sell or rent their services and malware to separate groups that want to conduct the attacks as is likely the case with the ransomware as a service group *DarkSide*, who conducted the infamous *Colonial Pipeline attack* in the spring of 2021.

Additionally, attackers will employ so-called "double extortion" attacks. Once the attackers get a hold of sensitive or valuable data in these attacks, they will exfiltrate that data before encrypting it and demanding the ransom. This provides the attackers with two additional avenues of exploitation. Should an organization refuse to pay the ransom, the criminals will threaten to release their data on the web. Additionally, the organization may think the attack is over if they pay the ransom and get the decryption key and recover their data. Unfortunately, often it's not. The attackers sometimes demand additional payments as they threaten to release the data a second time.

The only way organizations can win at this game is to harden their systems enough to avoid being successfully attacked in the first place.

Fortunately, organizations that actively defend their organizations can and do avoid such attacks altogether or can respond quickly and mitigate the damage.

Among the study's key findings:

- Forty-three percent of respondents suffered at least one ransomware attack during the past two years. Among them, 58% paid a ransom, 29% found their stolen data on the dark web, and 45% suffered financial losses.
- Thirty-seven percent said they lack an adequate security budget, while 31% believe they're powerless to prevent ransomware attacks because threat actors are too well-funded and sophisticated.
- Remote workers and cloud platforms/apps were the three most common attack vectors:
  - Remote worker endpoint (35%)
  - Cloud infrastructure/platform (35%)
  - Cloud app (SaaS): 32%
  - Trusted third-party (24%)
  - DNS (25%)
  - Software supply chain provider/vendor (24%)
- Exploitable vulnerabilities accounted for the most common initial infection point (63%), followed by privilege escalation (34%), credential exfiltration (32%), and averse mapped shares (25%).
- Respondents are most concerned about losing access to their organization's sensitive data (70%); stolen data being sold on the dark web (58%); and ransomware gangs gaining privileged access and/or controlling directory services (54%).
- Companies are not taking the threat lying down: 62% will increase ransomware protection spending in 2022.

ORGANIZATIONS FEAR THE WORST: LOSING THEIR DATA TO RANSOMWARE ATTACKERS

The concerns for ransomware continue to rise: 32% of respondents are moderately concerned while nearly half (49%) are very or extremely concerned.

A large majority (70%) worry most about losing access to their organization's vital/sensitive data, another 58% worry that their data will be sold on the dark web. Fifty-four percent are concerned that ransomware will gain privileged access or end up controlling directory services (e.g., Active Directory).

Other top concerns include regulatory penalties, attackers returning for more, legal issues from paying ransom, and attackers not honoring payoff agreements.

What are your top three concerns about ransomware attacks or threats to your organization? Select up to three choices.

*(e.g., Windows Active Directory)

REMOTE WORKERS AND CLOUD COMPUTING OPENING DOORS FOR ATTACKERS

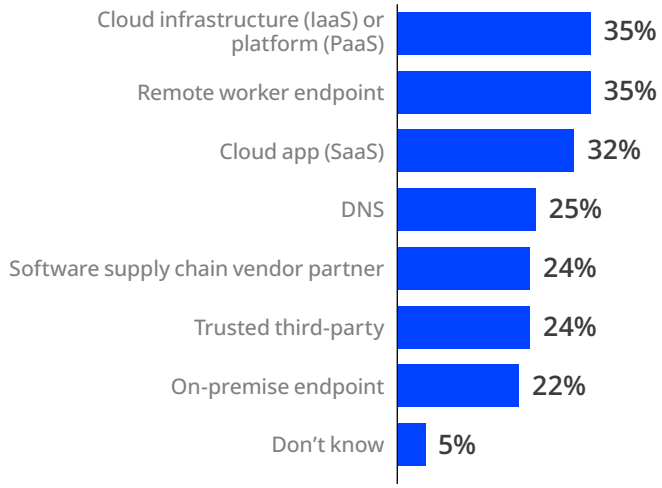
The good news is that 54% of organizations did not experience a ransomware attack in the past two years (2020 and 2021).

However, some organizations suffered quite a bit, with many experiencing multiple ransomware attacks in the past year.

Respondents cited the ransomware groups Tycoon (28%), Maze (26%), and Qakbot (22%) as the top groups responsible for these attacks.

How did attackers get in? It has a lot to do with current work and cloud computing trends. Thirty-five percent of respondents report that ransomware attacks exploited remote workers. Among the various other vectors were cloud infrastructure and platform services (35%), and cloud applications (32%). Other methods, such as DNS, software supply chain, third-party partners, and on-premise endpoints were also mentioned.

Which of the following were the initial infection vector(s) used to infiltrate your organization's network/system in these attacks/infections? Select all that apply.

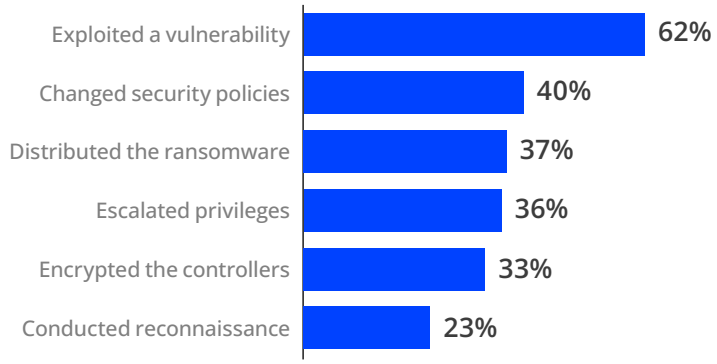


Once inside, how did attackers get deeper into the organization? Sixty-three percent of respondents reported that attackers exploited a vulnerability on another system and moved laterally. Other exploits included privilege escalation (34%), credential exfiltration (32%), and traverse mapped shares (25%).

Virtually all (95%) attacks involved Windows Active Directory with nearly one in four reporting this method as responsible for at least 50% of their attacks.

The majority of Windows Active Directory exploits stemmed from an exploitation of vulnerability (62%), although various other methods, including changed security policies and escalated privileges were also used.

Which of the following methods were used to exploit Windows Active Directory in these attacks/infections? Select all that apply.

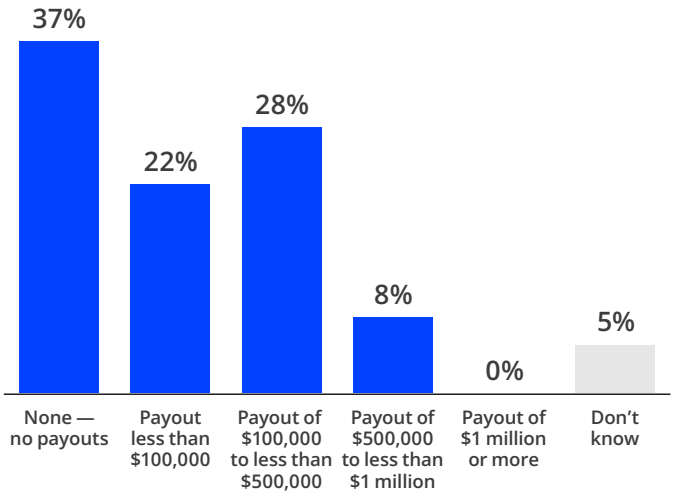


RANSOM PAYOUTS: A NECESSARY EVIL FOR SOME

"It would be nice not to pay them, but realistically sometimes you have to in order to protect your information," was the position of many respondents in providing their opinion about whether organizations should pay the ransom when attackers take their data hostage. In reality, 45% of respondents said they made a ransom payout for a single key and 30% made multiple payouts for double/multiple encryption keys. One-third said they were extortion victims who were faced with paying ransom to get their stolen data back.

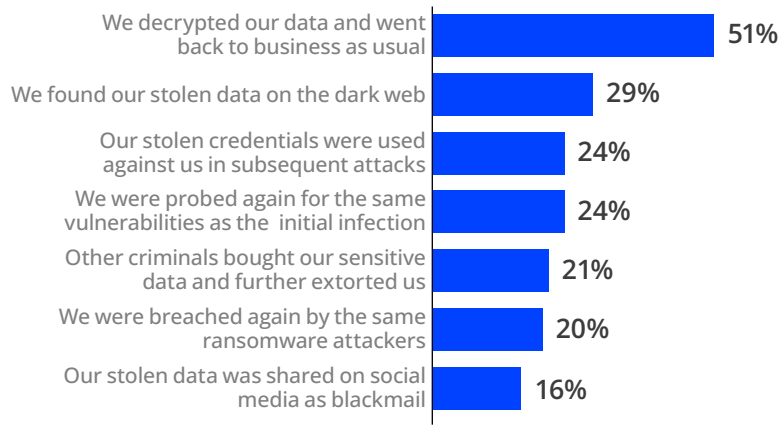
Those payouts proved costly for nearly two-thirds (63%) of respondents whose organizations they said paid a ransom — typically ranging from $100,000 to $1 million.

In total, what were your organization's ransomware payouts for these attacks/infections?



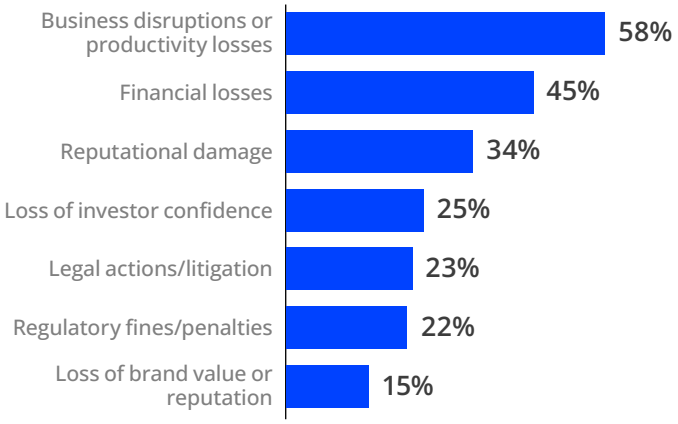
For those that paid to free their data held hostage, nearly half said after their data was decrypted they went back to business as usual. For organizations less fortunate, they found their stolen data on the dark web (29%), while many said their stolen credentials were either used against them in subsequent attacks or they were probed again for the same vulnerabilities.

Which of the following occurred as a result of your organization paying the ransom for these attacks/infections? Select all that apply.



The impacts of ransomware attacks varied. While business disruptions and productivity losses were the most typical results of an attack, reported by 58% of respondents, 45% said their organization also experienced financial losses. Other serious impacts included reputational damage, legal ramifications, and regulatory fines.

Which of the following were the impacts to your organization as a result of these attacks/infections? Select all that apply.



Of course, with so many successful ransomware attacks and many organizations ill-prepared to recover their data, the issue as to whether or not to pay a ransom remains heated.

The tradeoffs are apparent: Pay the ransom, and an organization may get its data back, but this also funds criminality and increases the odds that they, and others, will be victims again. Those with absolutist stances may not be taking in everything their organization must deliberate on into consideration. If a business pays a $500,000 ransom to avoid a multi-million dollar loss of business, don't they owe it to shareholders to do so? If a hospital's critical systems are encrypted, and a $100,000 ransom will get patients the care they need more quickly, isn't paying the more ethical thing to do?

"It depends on how much they want compared to the potential loss. I think this may be different for everyone."

– CISO, Healthcare

While it's best not to be compromised, the current state of security, technology, and software security, presents challenges in winning the war against ransomware.

Law enforcement gets the difficulty. Herb Stapleton, deputy assistant director at the FBI's Cyber Division, spoke to the WSJ last spring and reiterated the FBI position that victims shouldn't pay the ransom. "We know the payment of ransoms does fuel further criminal activity. That money is reinvested in the business models these illegal organizations have set up. In addition to lining their own pockets, it's used to make them better and faster at the work they do," Stapleton said.

"That being said, we understand that some victims are making a choice between shutting down operations and paying ransom. And so, while our advice remains that victims should not pay the ransom, we also want to clear up any misconception there may be that if you do decide to pay the ransom, that you shouldn't work with the FBI," he continued.

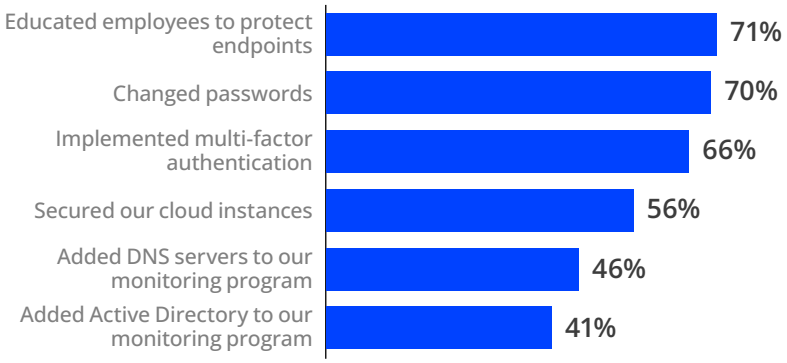
" It really depends on the individual circumstances, but every time one is paid, it emboldens these thieves to strike again and again."

– IT Director, Financial Services

LEARNING FROM THEIR MISTAKES: WILL THAT BE ENOUGH?

Remediation activities following a ransomware event vary for organizations. The most common are hardening their systems against future attacks (81%), investigating root causes (72%), and re-scanning for vulnerabilities (70%). Educating employees, changing passwords, and implementing multi-factor authentication were among the top methods used to harden organizations' systems to prevent future attacks.

Which of the following steps has your organization taken in hardening its systems to prevent future ransomware attacks? Select all that apply.



Respondents cited a number of methods to respond and recover from attacks. Among the top approaches were secure backups (78%) and implementing ransomware protection applications or services (61%). Others include swift incident response, cyber insurance, a resiliency plan, and a few turned to a professional ransom negotiator.

"We have backups of all critical information and can get back up and running in a matter of days, but not hours. We also take extreme security measures to make sure a ransomware attack does not happen."

– Chief Technology Officer, Healthcare

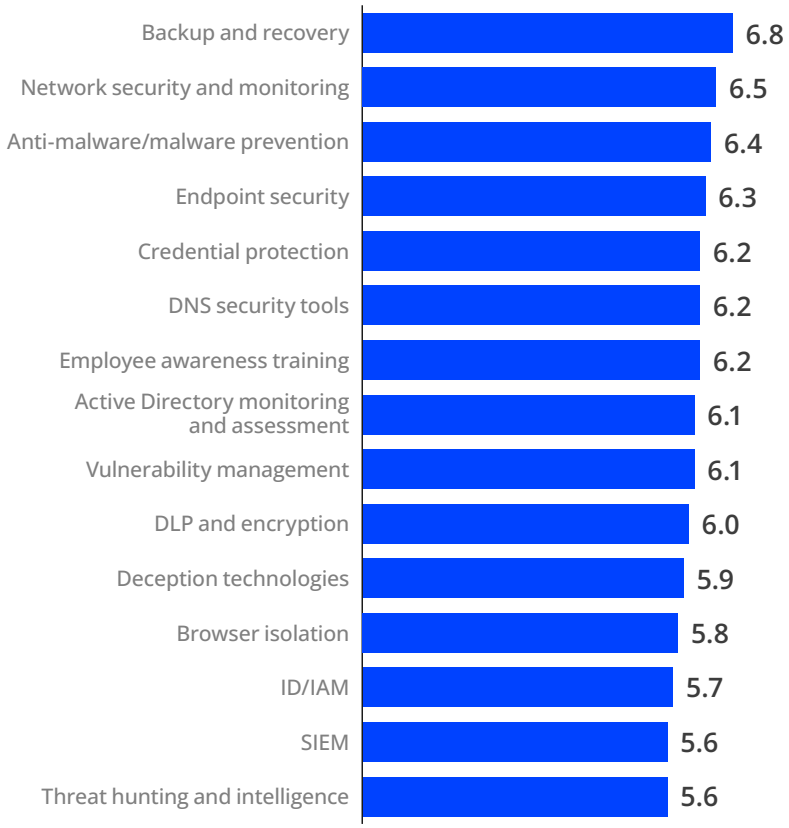
Despite a troubling history with ransomware, many respondents (56%) say they are confident in their organization's ability to successfully respond to ransomware attacks in the coming year. Respondents described various reforms and protections that justified their confidence: tighter controls, continuous monitoring, frequent file backups, regular rapid response plan testing, employee training, and cybersecurity insurance, among others. For some respondents however, the all-too familiar sentiment — "I really don't think my organization is large/important enough to be a target of an attack" — was their main defense. For those less optimistic about their ability to fight off ransomware attacks, their fears that criminals are coming up with "more and more ways to steal their data" and modern attacks cause "greater harm to their organization's business than previously" describe the sense of foreboding that many security teams have.

"We have the best protection right now, but if a hacker wants to get in, they probably will."

– Controller, Manufacturing

In measuring respondents' overall satisfaction (on a scale of 1 to 7) with their organization's ability to protect against ransomware, respondents were most satisfied with their backup and recovery capabilities scoring an overall average of 6.8, followed by network and security monitoring at 6.5. The lowest satisfaction levels (5.6) were with SIEM and threat hunting/intelligence capabilities.

How satisfied are you/your organization with your organization's current ability to protect against ransomware using each of the following? Rate each on a scale of 1 to 7 where 1 is "Not at all satisfied" and 7 is "Extremely satisfied."



"We've worked hard to make our systems more resilient to malicious actors, provided significant investment in training and take proactive approaches to scanning, discovering and neutralizing threats."

– Director of IT, Healthcare

THE MANY HURDLES IN FIGHTING RANSOMWARE

Organizations face a variety of challenges in combating ransomware: ranging from inadequate budgets to ineffective internal processes, controls, and technology. Additionally, the growing sophistication and funding levels of ransomware attackers present a formidable challenge according to 31% of all respondents.

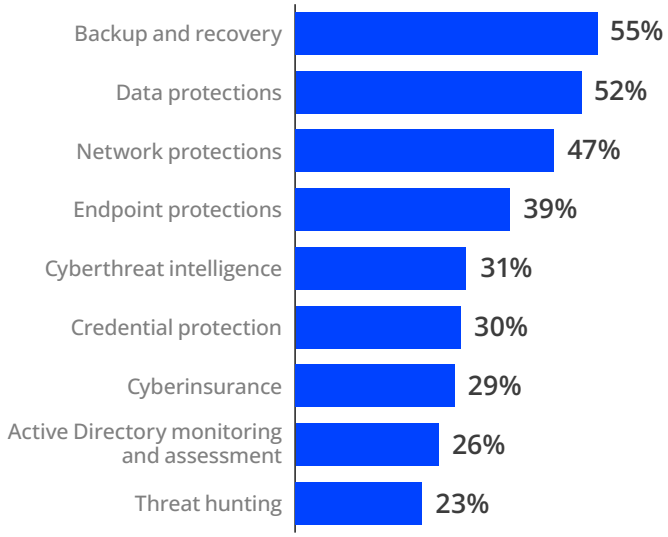
While there are plenty of hurdles for ransomware victims, there are a lot less for attackers. In February, authorities in the United States, Australia, the United Kingdom *issued a joint alert* that warned increased critical infrastructure ransomware attacks would likely continue in the year ahead. "Ransomware tactics and techniques continued to evolve in 2021, which demonstrates ransomware threat actors' growing technological sophistication and an increased ransomware threat to organizations globally," the advisory stated. And it's not just the 16 critical infrastructure industries that will be targeted, as our survey shows: it's everyone.

BUDGET FOR DEFENSE... AND POSSIBLY RANSOM

In the year ahead, most organizations (62%) plan to increase their ransomware protection spending while 31% don't plan to change their budget.

Most of this spending will be targeted to backup and recovery, data protections, and network protections. Twenty-nine percent also indicate they plan to invest in cyberinsurance to cover the cost of ransomware attacks, which is likely far less expensive than the cost of ransom payments.

In which of the following areas does your organization plan to invest in 2022 to protect itself from ransomware attacks? Select all that apply.



While there's no easy way to defend against ransomware, there are things enterprises can do to protect their systems and data better:

- **Security awareness training.** While not perfect, and users will likely continue to click on links they shouldn't, the first line of defense is teaching users to be aware of the risk of malicious links and attachments. The fewer malicious links staff click upon, the fewer attacks the security team will have to respond to. With phishing being a common initial attack vector, ensure email anti-spam and anti-malware defenses are as robust as possible.
- **Asset management.** The security team can't protect systems they don't know exist, so gaining an accurate listing of systems, cloud services, endpoints, and more in the network will help teams understand what systems need protecting and keeping up to date. Pay special attention to how credentials and access are managed, system configurations, network shares, and ensure all software is kept up to date.
- **Keep systems up to date and safely configured.** Be sure to implement an effective vulnerability and configuration management program. Have systems scanned for outdated software, misconfigurations, excess access rights, and more. And when these things are identified, be sure to remediate the situation quickly.
- **Data management.** Knowing where critical data resides is the first step to protecting it from being encrypted by criminals. Not only can data be better protected, but it can also be securely backed up in case of a ransomware attack and then readily restored.
- **Multifactor authentication.** Ransomware attacks typically involve stolen login credentials, either for the initial compromise, moving laterally within the organization, or perhaps both. Two-factor authentication can go a long way to cutting these attacks short.
- **Trust no one.** Because attackers use stolen credentials to gain access to systems within an organization, adopting a zero trust architecture is crucial to limit account access until users can prove they're who they claim to be.
- **Begin segmenting your networks.** Network segmentation is another strategy that helps to reduce risk. Once an attacker is on the network, they move to other systems. If the network is wide open and can access any system from the point they gained entry, an enterprise could be in trouble. Segmenting networks makes it much more challenging to wander from system to system throughout the organization at will.

- **Incident response.** If there's been a breach, and it's a safe bet that every organization will be breached, the organization needs to be able to identify that it's been breached and have a plan in place to mitigate the damage as much as possible. This means having a team in place. They develop playbooks for different attacks and situations and practice their response.

CONCLUSION

Ransomware attacks are on the rise — both in numbers and the size of payouts. Considering the substantial costs to enterprises in potential business disruption, loss of access to data, regulatory fines, and damage to reputation, enterprises must do everything they can to defend themselves against these attacks better. This isn't even considering the substantial risk of loss of life when such attacks hit critical infrastructure and services, such as hospitals and energy.

The work required for enterprises to get where they need to be is considerable, from improving endpoint security to threat intelligence.

There is a lot of work to do. Yet, organizations seem to be taking the steps they need to get to the level of security required.

The challenge is the bad actors don't stand still, either. They are continually improving their strategies and tactics.

That, coupled with the reality that business technology systems continue to grow in complexity, we likely have a test of wills between attacker and defender for some time.

ABOUT CYBERRISK ALLIANCE

CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community, and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers, and practitioners. CRA's brands include SC Media, Security Weekly, InfoSec World, Cybersecurity Collaboration Forum, our research unit CRA Business Intelligence, the peer-to-peer CISO membership network, Cybersecurity Collaborative, and now, Identiverse, ChannelE2E and MSSP Alert. More information is available at *http://cyberriskalliance.com/*.

ABOUT ATTIVO NETWORKS

Attivo Networks, the leader in identity detection and response, delivers a superior defense for preventing privilege escalation and lateral movement threat activity. Customers worldwide rely on the ThreatDefend® Platform for unprecedented visibility to risks, attack surface reduction, and attack detection. The portfolio provides patented innovative defenses at critical points of attack, including at endpoints, in Active Directory, and cloud environments. Attivo has 150+ awards for technology innovation and leadership. *www.attivonetworks.com*.

ABOUT eSENTIRE

eSentire, Inc. is the Authority in Managed Detection and Response, protecting the critical data and applications of 1200+ organizations in 75+ countries, representing 35 industries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts, Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit *www.esentire.com* and follow *@eSentire*.

ABOUT MENLO SECURITY

Menlo Security enables organizations to outsmart threats, completely eliminating attacks and fully protecting productivity with a one-of-a-kind, isolation-powered cloud security platform. It's the only solution to deliver on the promise of cloud security—by providing the most secure zero-trust approach to preventing malicious attacks; by making security invisible to end users while they work online; and by removing the operational burden for security teams. Now organizations can offer a safe online experience, empowering users to work without worry while they keep the business moving forward. For more information, visit *www.menlosecurity.com*.

