RANSOMWARE IN FOCUS

NEW RESEARCH ON CISO PERCEPTIONS, PERSPECTIVES AND PLANS FOR WEATHERING THE STORM

2021

CISOs CONNECT

AimPoint Group

W2Communications

TABLE OF CONTENTS

SPONSORED BY

RANSOMWARE IN FOCUS

Introduction

While ransomware is not a new phenomenon, 2020 brought a significant acceleration of attacks capitalizing on the pandemic-forced shift to remote work, the proliferation of Initial Access Brokers and the ready availability of ransomware as a service. With all of the headlines and hype, we wanted to understand the true perspectives of those who shoulder the burden of responsibility for managing the impacts of ransomware on a business: Chief Information Security Officers (CISOs).

In August 2021, we conducted a study of these senior-level executives to assess their ransomware experiences, concerns, and priorities for protecting their organizations going forward. This report, reflecting input from over 250 CISOs, presents what we learned.

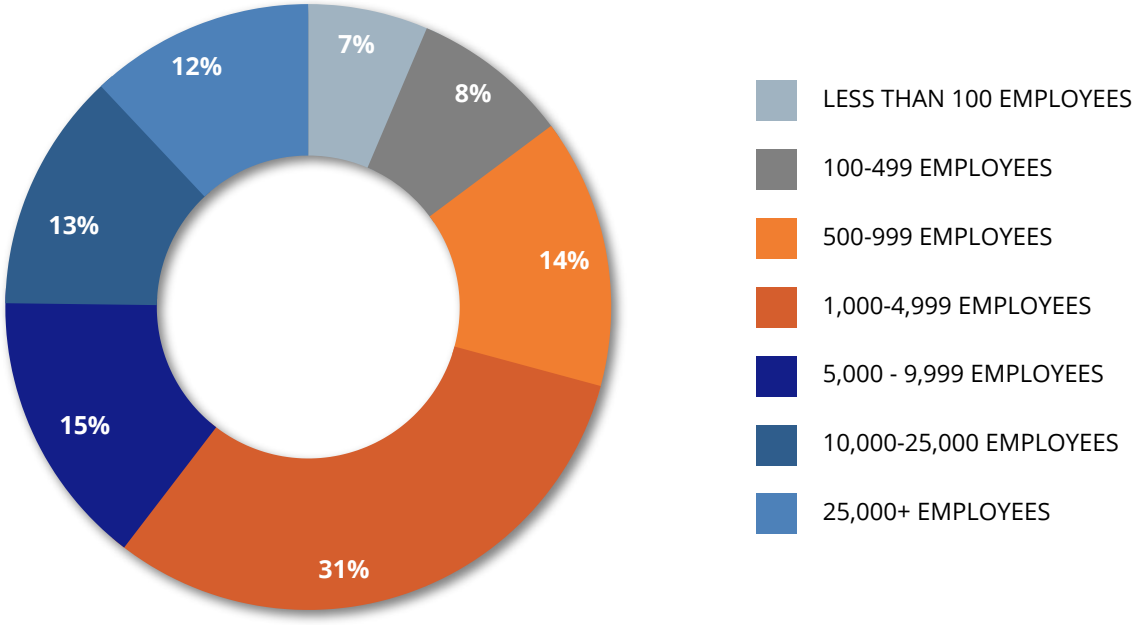
Methodology

This study utilized a quantitative survey that was designed with guidance from a Board of CISOs working at large, private sector organizations predominantly in the United States. Respondents were recruited through their direct relationships with CISOs Connect and from a well-screened panel. We received 250 survey completions from respondents identifying as CISOs or CISO-equivalents across a broad range of industry sectors. All responses were anonymous.

Additionally, we conducted in-depth discussions with members of our Board, a group particularly known for their strong technical and business acumen, to get their detailed perspectives on ransomware as a leading cyber threat. You will find insights and best practice recommendations from them throughout this report.

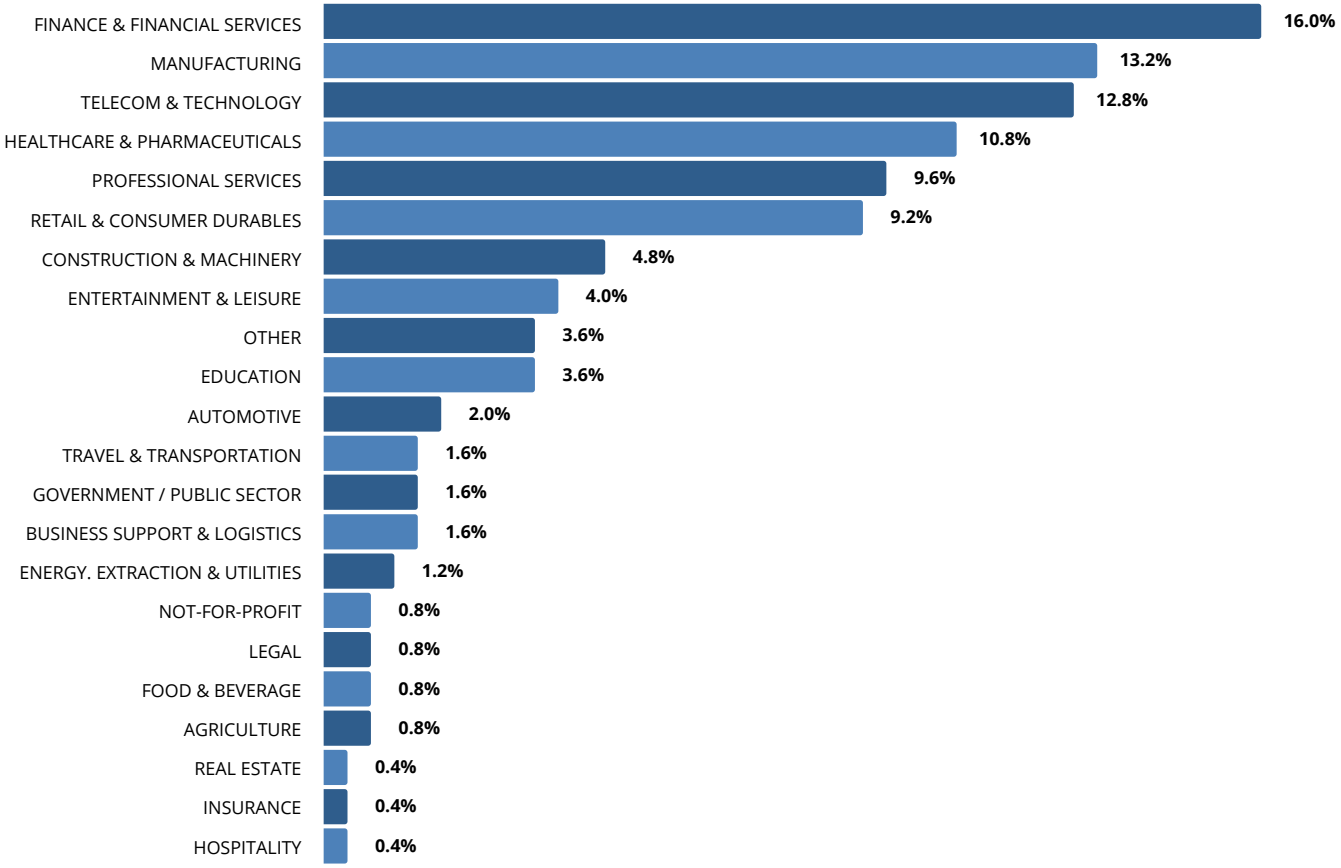
How many employees are in your organization worldwide?

Figure 1.



Which best describes your organization's primary industry?

Figure 2.



Key Findings

1. **CISOs recognize ransomware as the #1 threat they face.** That is due to the multiple high-value impacts ransomware can impose: operational, financial, legal, reputational and more. Given the breadth of potential access points, preparing ransomware defenses involves everyone and everything in the organization - from users and endpoints to the data center and the cloud.

2. **Unfortunately, there is no relief in sight.** 69% of respondents consider it likely they'll be successfully hit at least once in the next year. With only 53% of them having been hit in the past year, this signals an expectation that the ransomware problem will get worse before it gets better.

3. **Mid-sized organizations are at the center of the ransomware crosshairs.** While 53% of respondents overall were successfully hit by ransomware in the past year, the rate is noticeably higher (reaching almost two thirds) for companies with between 1,000 and 9,999 employees. In addition, this same segment expects to be hit at a greater rate in the coming year: 80%, compared to a 69% average across all segments.

4. **Ransomware gains cyber its seat at the big table.** With so many high-profile attacks publicized over the last year, the ransomware threat is serving to highlight the importance of cybersecurity to the Board level like nothing else before it. For perhaps the first time, executive leadership and the Board are not seen as obstacles to CISOs pursuing the level of defenses they need to effectively protect against a specific threat.

5. **The ransom itself is not a top concern.** Paying is obviously controversial, as it isn't even a guaranteed short-term solution, and in the longer term it rewards threat actors while incentivising them to continue ransomware attacks. But the inclination to pay is understandable for several good reasons: business continuity or even survival, the cost-benefit of paying vs. recovering on your own, and growing concerns about data exposure. Regardless, CISOs' biggest cost worries come from recovery and restoration of business operations, which can be far more expensive than a currency payout. They're also very concerned about data exfiltration and the resulting risks to their business.

6. **Are businesses prepared to make a ransom payment?** Even if the actual payment amount is a lower concern, a payment may still have to be made. Input from our CISO Board strongly emphasizes that paying a ransom must be a pre-vetted business decision founded on thorough cost-benefit analysis and scenario modeling. CISOs know they're being targeted, yet very few indicate their organization has taken proactive steps like allocating a ransom budget, setting up a cryptocurrency account or retaining a third-party payment broker. While the inaction may indicate some level of organizational denial (it won't really happen to us!), it may also reflect the challenge of engaging active participation from other parts of the organization to build and vet the business case.

7. **The total cost of an attack can be steep.** There is a 1-in-5 chance that a successful hit will cost your organization more than $5M in total - that's out-of-pocket along with the significant costs of recovery. There's a 1-in-20 chance the total impact will be greater than $50M! You can increase your odds of minimizing cost impacts by maintaining a stringent backup regimen and a solid defense-in-depth strategy.

8. **Zero Trust is a key defense.** Network segmentation technology is #1 on the ransomware defense shopping list for the coming year. Commentary from across our CISO Board also stressed the importance of implementing and enforcing least privileged access control. It's clear that a Zero Trust approach is viewed as a leading way to help stem the tide of ransomware and the other cyber threats that are still very present in the ecosystem.

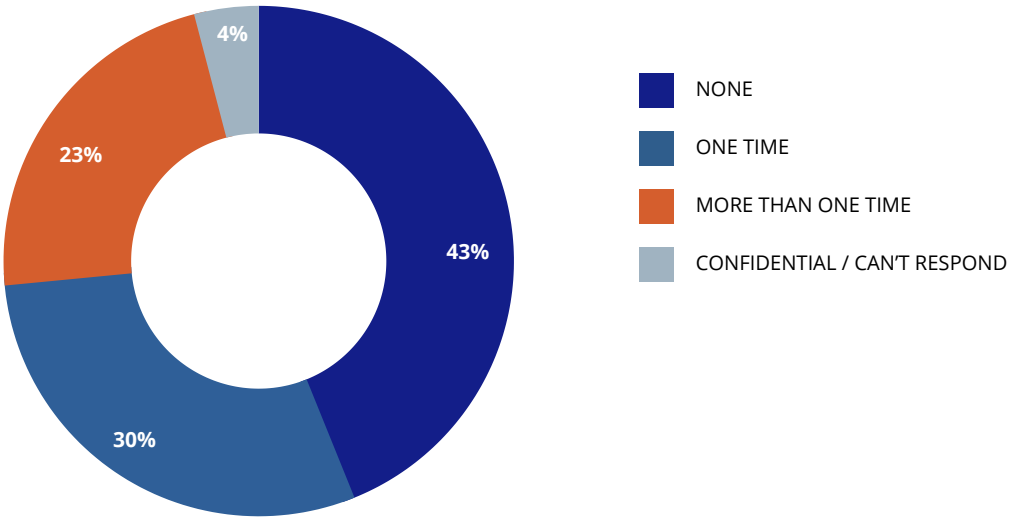
DETAILED FINDINGS

Impact and Response

We directly addressed a challenging question: in the last 12 months, have you been hit by a successful ransomware attack? ("Successful" meaning some number of computers were affected, and data was encrypted and/or threatened to be exposed.) While a small number of respondents declined to answer based on confidentiality concerns (even with survey anonymity), over half admitted that they had been hit once, with over a quarter being hit more than once.

How many times was your organization hit by a successful ransomware attack in the last 12 months?

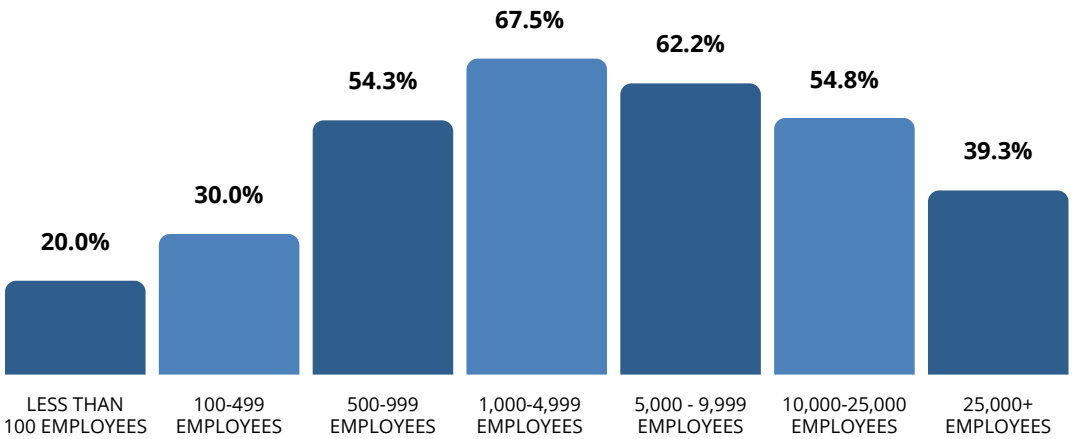
Figure 3.



Mid-sized organizations experienced the greatest number of successful ransomware hits, with those in the 1,000-4,999 employee range faring the worst (67.5%) followed by those with 5,000-9,999 employees (62.2%). This may reflect security challenges for companies that are on a good growth trajectory but not big enough to have the greater resources and stronger defenses that large enterprises often enjoy.

Successful ransomware attacks, by size of organization

Figure 4.

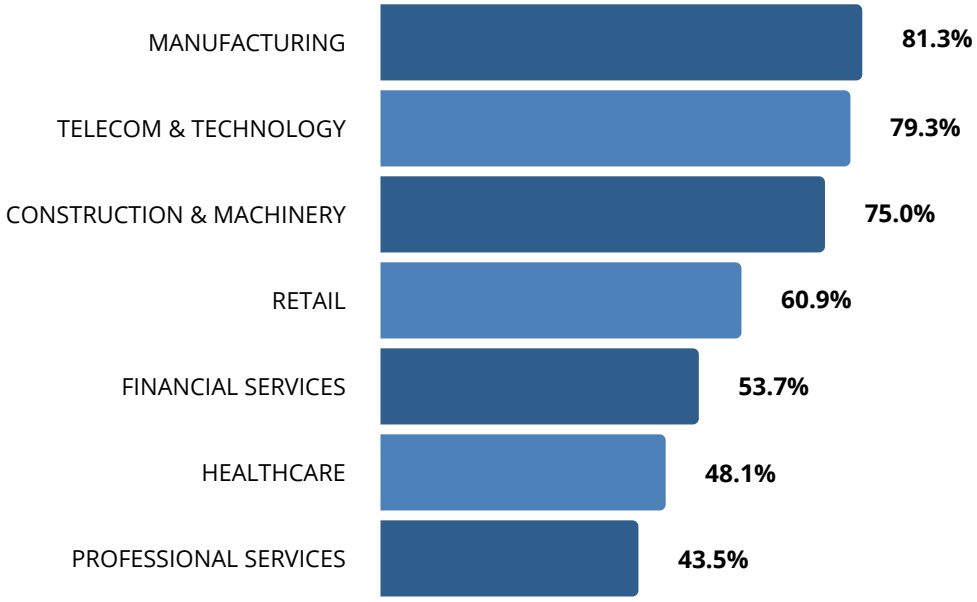


Certain industries experienced a greater level of successful attacks than others. Companies in the manufacturing sector (which has historically under-invested in cybersecurity) led the way, with an 81% successful hit rate for our sample. Those in the sector encompassing telecommunications, technology, internet and electronics followed closely behind, with a nearly 80% hit rate. As these two sectors in particular have highly complex supply chains, there may be some connection to the numerous successful hits and the common vulnerabilities found within supply chains that make member networks fruitful access points for reaching the ultimate target organization.

Retail came in somewhat lower, but at a still high 61%. Financial services experienced just over 50%, with healthcare following closely at 48%. That latter statistic is perhaps a bit surprising given the critical nature of the healthcare industry and its legacy of under-spending on cybersecurity, which would seem to make healthcare organizations a greater than average target.

Successful ransomware attacks, by industry

Figure 5.

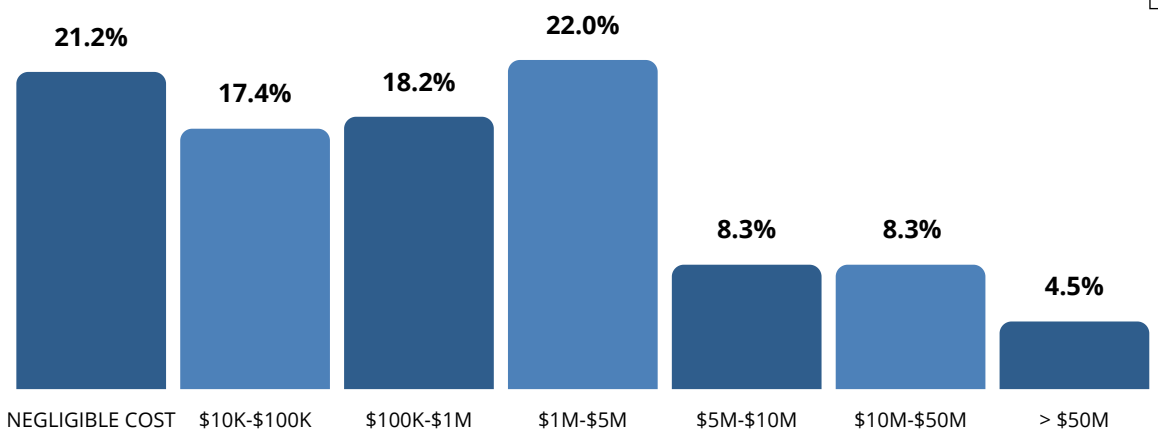


For those that were successfully hit, the financial impacts were not trivial. While close to four out of ten were able to get away with relatively minor cumulative costs, just over two out of ten suffered considerably in this regard, accumulating a financial impact of more than $5M. Nearly one in twenty fell into the unenviable position of losing more than $50M.

> "If you were hit with ransomware right now, do you know how you could recover from it? How often are you doing backups - every four hours? every eight hours? daily? weekly? monthly? This is where the business needs to be involved in determining how long can you go without some systems before there is an impact. Then you have to scope and design your systems so you can recover within that window or put a price tag on what exceeding that window is going to cost. It's about doing the due diligence, making sure you've got everything in place to recover from it gracefully."
>
> CISO and VP of IT, Large Retail Enterprise

Total cost of ransomware attacks

Figure 6.



Respondents reported that the percentage of their cumulative losses representing hard costs of paying a ransom versus the costs of response and recovery came out at close to even. However, the weightiness of those impacts is not of equal concern to our CISOs, as we will cover in a bit.

Expectations for the Next Twelve Months

When asked if they expect their organization to be successfully hit by ransomware in the next twelve months, there is a notable shift in the pessimistic direction. Only 23% of our respondents said that it is somewhat unlikely, and only 7% are fully confident in their defenses, saying it is not likely at all. That is an interesting juxtaposition to the 43% who reported not having been successfully hit in the prior twelve months.

A full 69% consider it somewhat or very likely that they will be successfully hit at least once. Since 53% reported having been hit in the past year, this signals an expectation that the ransomware problem is going to get worse before it gets better.

In a bit of a silver lining, only 12% of respondents consider it very likely that they will be successfully hit multiple times, when nearly twice as many (23.8%) were actually

"Ransomware is the biggest threat now. It has a financial risk component, an operational risk component, a compliance and legal risk component, and it has a reputational risk component, because even if you have recovered, the attacker still has data he can threaten you with."

Angel Redoble, CISO, PLDT Group

"Ransomware has got to be right at the top of the threat list. The other threats haven't gone away, but ransomware is extending it."

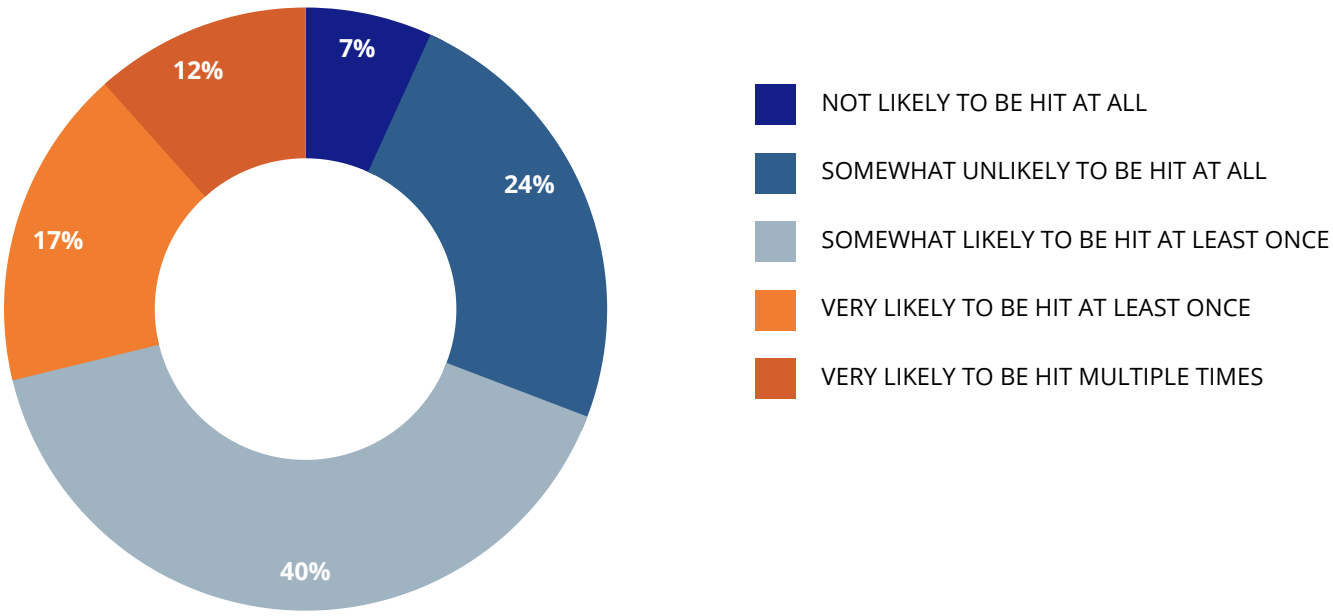
David Levine, VP Corporate & Information Security, CSO, Ricoh USA, Inc.

hit multiple times in the past year. That may suggest a small but growing feeling of confidence in CISOs that they are getting prevention around this problem at least somewhat figured out. Or, based on so many high-profile attacks, they may have been granted more budget to implement defensive programs (we discuss that farther on). That perspective is reinforced by responses to later questions in this study that indicate where CISOs feel they are "already in good shape" with regard to certain defensive technologies and practices (see Figures 22 and 23). We will need to see how that bears out in coming months.

> "The reason ransomware has this much notoriety is because it has that instant gratification for the intruder. Pull the switch, and all hell breaks loose. Unfortunately, this is going to keep getting worse, because there's more and more emphasis by the hacking community to come up with more harsh ways of creating malware payloads.
>
> CISO, Large Healthcare Enterprise

Expected ransomware attacks in the next 12 months

Figure 7.



When we look at the breakout by organization size, expectations mirror past experience, as those having between 1,000-4,999 employees and 5,000-9,999 employees—the group that experienced the highest hit rates in the last twelve months—have the highest expectations for being hit again. The smallest and the largest organizations have the greatest confidence and lowest expectations for being hit.

While it is understandable that very large organizations are confident in their defenses, it is likely that the smallest organizations feel the least vulnerable because presumably they are not on attackers' radar. That is not necessarily sound logic, given the accelerated supply chain attacks most industries are experiencing. As a member of our CISO Board put it, you need to look where you are in the supply chain of the company that is the real target.

"Businesses under a certain revenue or market share are not going to make that big of a news article. The impact is there, but it's at a smaller scale. It's not that they're not being targeted, they're just not getting known, even when the attack causes their business to be permanently shutdown."

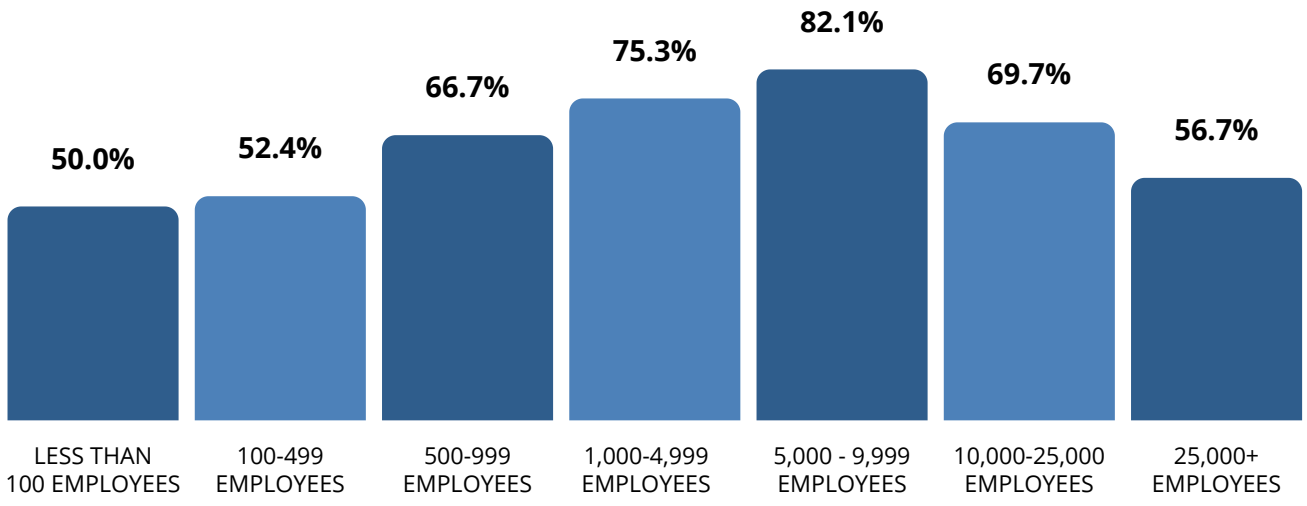
CISO, Large Healthcare Organization

"You might not be as newsworthy as some of the bigger organizations, but you're deluding yourself that you're not a target. Go on to the dark web and do some searches, you'll find your information, and you'll realize the scope of this problem is not relegated to any one industry, company or size."

Dave Ruedger, CISO, Invitae

Expect to be hit at least once in next 12 months, by size

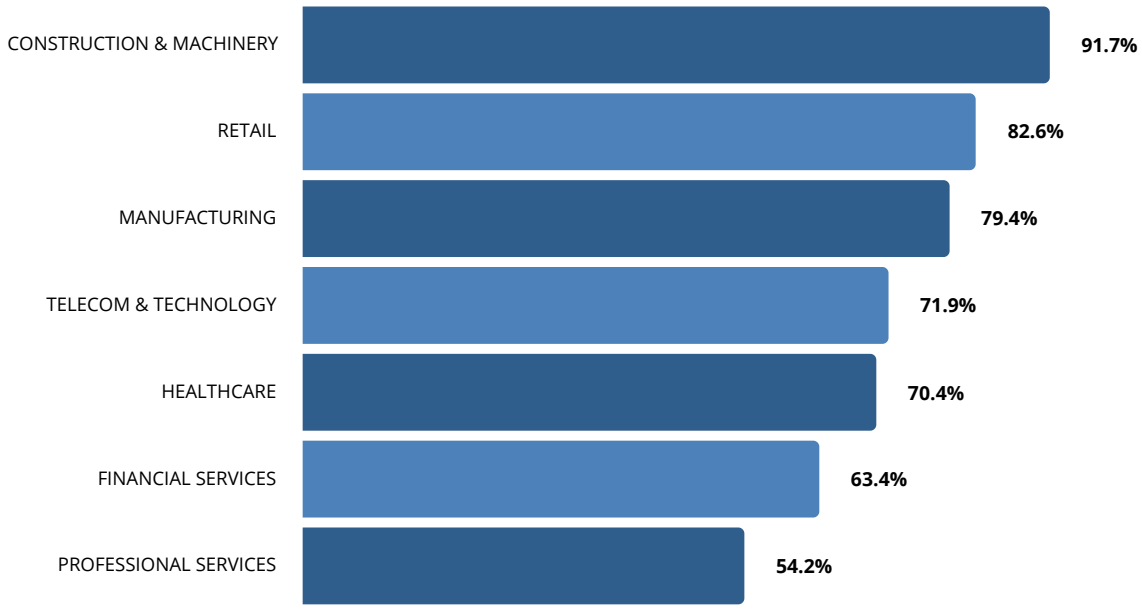
Figure 8.



Expectations to be hit by industry sector show that retail and healthcare, in particular, are expecting things to get worse. Only 60% of retail respondents were successfully hit in the last year, but that number jumps to 82.6% for expectations to be hit in the next year. Healthcare jumps from 48% actually hit to 70.4% expecting to be hit.

Expect to be hit at least once in next 12 months, by industry

Figure 9.



CISOs Concerns about Ransomware Impacts

When asked about which ransomware impacts they are most concerned, exposure of sensitive data topped the list with a 4.11 weighted response average (WAVG). That is not surprising given that data is the lifeblood of every modern organization, and its exposure can cause all manner of harm. This finding also indicates that CISOs understand the increasing threat of "double-barrel" demands for payment plus extortion, and accept it as the new reality.

> "What you should do is just skew towards making everything disposable. Don't keep data where it doesn't belong, and make sure that everything that is important has a backup and is recoverable. That's the best possible approach."
>
> Dave Ruedger, CISO, Invitae

Beyond that top issue, the responses for other impacts show that all of them cause significant concern. In fact, the spread between the highest and lowest concern is only a half point. Clearly, CISOs have a lot to worry about. Still, some issues are higher priority than others.

Concerns about the hard cost of recovering and restoring operations after a successful ransomware attack (3.99 WAVG) are about equal to the loss of revenue from operational disruption (3.98 WAVG). This finding demonstrates that ransomware is truly a business problem, and CISOs understand and feel the pressure of that impact. As a sort of mixed blessing and curse, at least the ransomware threat is serving to elevate the importance of cybersecurity to the Board level like nothing we've seen before.

Damage to brand reputation follows (3.94 WAVG), although it is slightly less critical than the top three concerns. That is perhaps because reputation can be recovered over time, as consumers and customers grow desensitized to the headlines about the cyber-attack of the week and the feeling of inevitability takes over.

"In the past CISOs used to talk about the one big breach for the year, but now it's a question of how many companies were breached in the last 24 hours? And, frequently, they don't garner much attention unless it's particularly bad or unique."

David Levine, VP Corporate & Information Security, CSO, Ricoh USA, Inc.

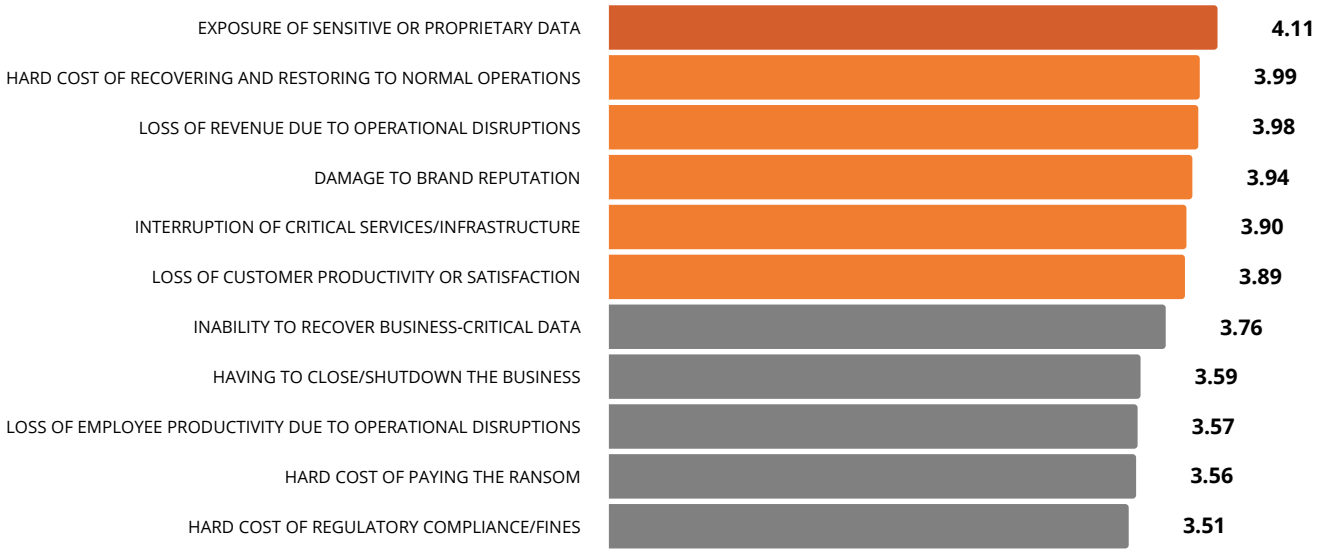
Interestingly, the least worrisome impacts include the loss of employee productivity from operational disruption (3.57 WAVG) – possibly because people can be pretty good at finding workarounds to get their jobs done. Productivity loss ranks about equal to concern about the actual hard cost of a ransom payment (3.56 WAVG). Threat actors are wisening up to the reality of setting their demands to a level that organizations will actually pay, either because the amount is low enough or because it's aligned with an organization's insurance benefit.

The issue of least of concern was regulatory fines. While CISOs don't want their Boards to be upset at such transgressions, the amounts of actual fines may suit a checkbox mentality. The impact relative to data exposure and cost of recovery is just not as significant.

What does all of this mean? We offer the mercurial but truly valid answer of 'it depends.' For instance, if your organization provides critical services (think healthcare, or fuel and power distribution), then getting systems back online ASAP is the priority, while hard costs and other issues are secondary. If your organization is smaller or less well-established, then the threat of having to shutter your entire business because of a crippling ransomware attack is a make-or-break issue. The bottom line is that breach impact is complex, and every facet must be considered and factored into business continuity planning according to each organization's risk tolerance.

How concerned are you about the following potential impacts from a ransomware attack? (1 = low concern, 5 = high concern)

Figure 10.



To Pay or Not to Pay?

For those who were successfully hit, more were inclined to pay the ransom than not. Slightly more than 65% paid, but to varying returns on their investment.

Indeed, for those that paid the ransom, doing so only led to a full recovery of data slightly more than half the time (55%). For the remaining 45% of cases, the result was less than ideal. For just over a third (34%), partial data recovery was the outcome (we were even told of a company that got their data back in one very big flat file), while 11% suffered the unfortunate fate of getting nothing back in exchange for paying the ransom.

Returning to the aggregate results, a third of respondents didn't pay but were able to recover their data anyway, presumably through a strong backup regimen. Unfortunately, two percent didn't pay, and lost it all.

> "I'd hate to be in the firefight and have to make that decision on the fly. Hopefully, you've made that business decision prior to when you need it. Attackers know more about your company than you think. They know how much every hour and every day of interruption costs, and they right-size the ransom to where they get paid. If it's going to cost us $12 million to restore services, and they're only asking for $1M, how do you look to your shareholders and those who have a financial interest in your company and say we chose to go the $12 million route instead of the $1 million route? "
>
> CISO and VP of IT, Large Retail Enterprise

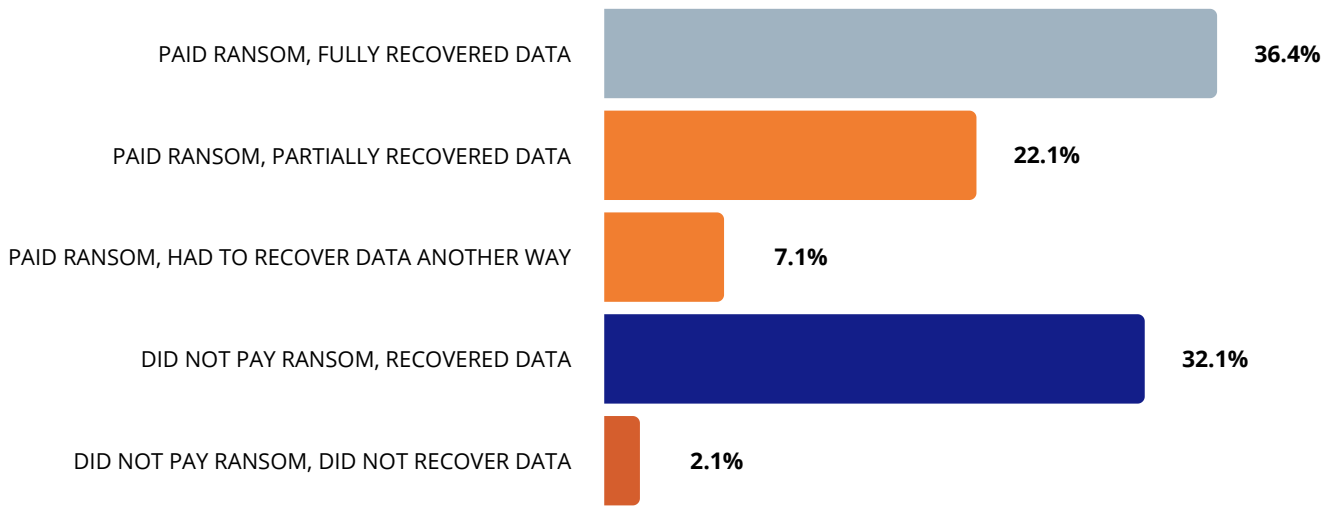
This begs the question: should one pay in a ransom situation? Even partial data recovery has some value. While paying reinforces the problem and fuels the ransomware epidemic, it's understandable that at least some organizations will pay given the serious potential impacts of not paying. We noted earlier that threat actors have taken to right-sizing ransom demands to palatable amounts or to align with insurance coverage. Because many companies now carry ransomware insurance (we discuss that a bit later), there may be a sense that the insurance provider will own the payment burden – although the premiums are getting steep. But also, the growing trend of attackers threatening to expose sensitive data is likely convincing more companies that paying could be in their best interest.

"There are a number of legal issues associated with paying ransom. Know the rules for whether or not it is possible to pay a ransom in a way that is compliant with federal laws on money laundering. You're transferring money to someone, and you don't know who they are, where they are, and what they're going to do with it. You run the risk of engaging in a financial transaction with a prohibited nation. Then, other regulations require use of a money transfer agent that's federal and state licensed. Coinbase is not. You're also required to report financial funds transfers that are more than a certain dollar amount. Is cryptocurrency a funds transfer? How are you going to treat this for tax purposes? Will the cost of paying the ransom be covered by insurance? Will the costs of NOT paying be covered by insurance? You don't want to pay this out of your pocket."

Mark Rasch, Cybersecurity Legal Expert

Response and outcome to ransomware attack

Figure 11.



"Some of it is security awareness training, some of it is additional endpoint controls. Now you start to build the argument of defense-in-depth. We know we're going to remove a majority of our risk by having multi-factor authentication. Then we get better endpoint protections, and we've reduced that risk even further. Then we add in data protection controls, and now we're down to a risk level that is fairly well managed at any given point in time."

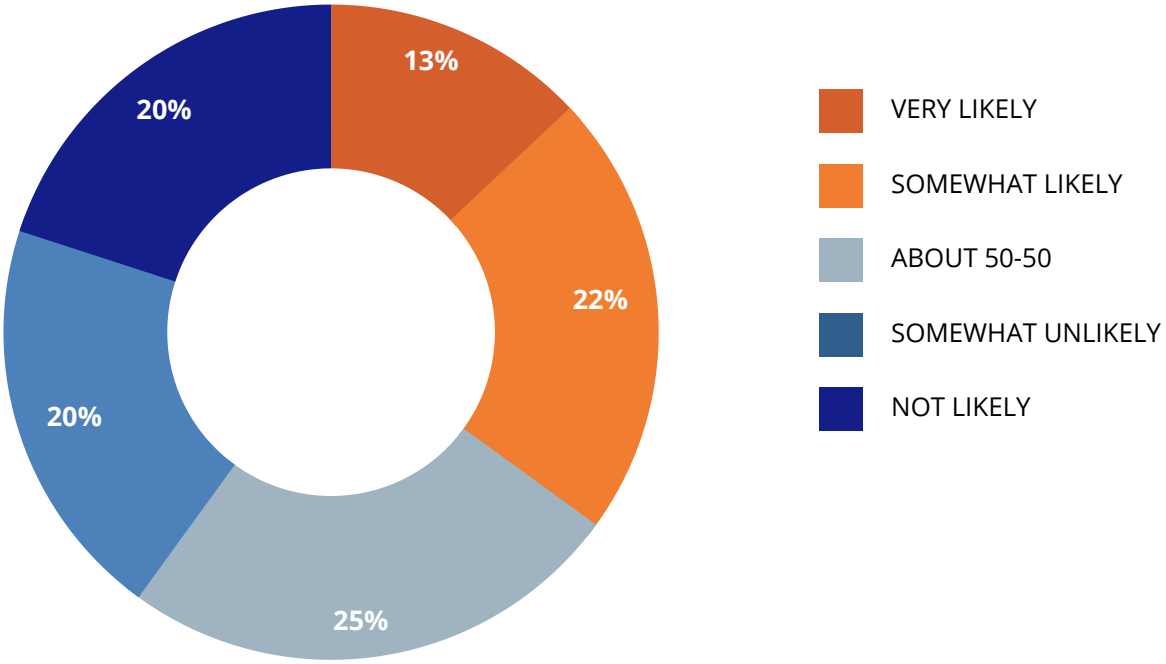
Dave Ruedger, CISO, Invitae

Current and Planned Mitigation Efforts

Given the suboptimal future outlook, we asked respondents about the likelihood that their organization would pay a ransom if successfully attacked in the next twelve months. Two thirds of respondents fall into a middle group (somewhat likely/50-50/somewhat unlikely) that reflects the 'it depends' reality we previously discussed. Only 13% say it's very likely they will pay, and 20% say they won't. This suggests a balancing of forces, with a greater inclination to pay as a result of payment being an informed business decision offset by the headway organizations are making in improving their prevention and mitigation capabilities.

If hit by a successful ransomware attack in the next 12 months, how likely is your organization to pay the ransom?

Figure 12.



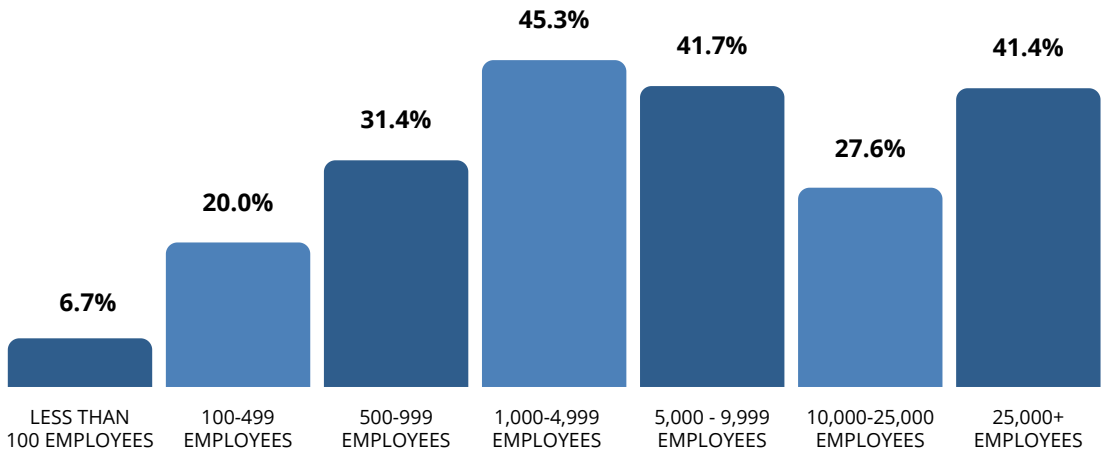
Unsurprisingly, the smallest organizations are least inclined to pay. They have the fewest resources, although arguably the most to lose as a total, unrecoverable lock-up of their data could put them out of business. Midsized organizations, again those most hit successfully in the past, are most inclined to pay.

"You need to have a plan and build readiness into your infrastructure: cyber resilience, cyber readiness, ransomware readiness, which is engaging with a company that can help you negotiate and pay the ransom, also a forensics company that can help you figure out what happened, and data backup and restoration. Do that right away."

Mark Rasch, Cybersecurity Legal Expert

More inclined to pay ransom than not, by size of organization

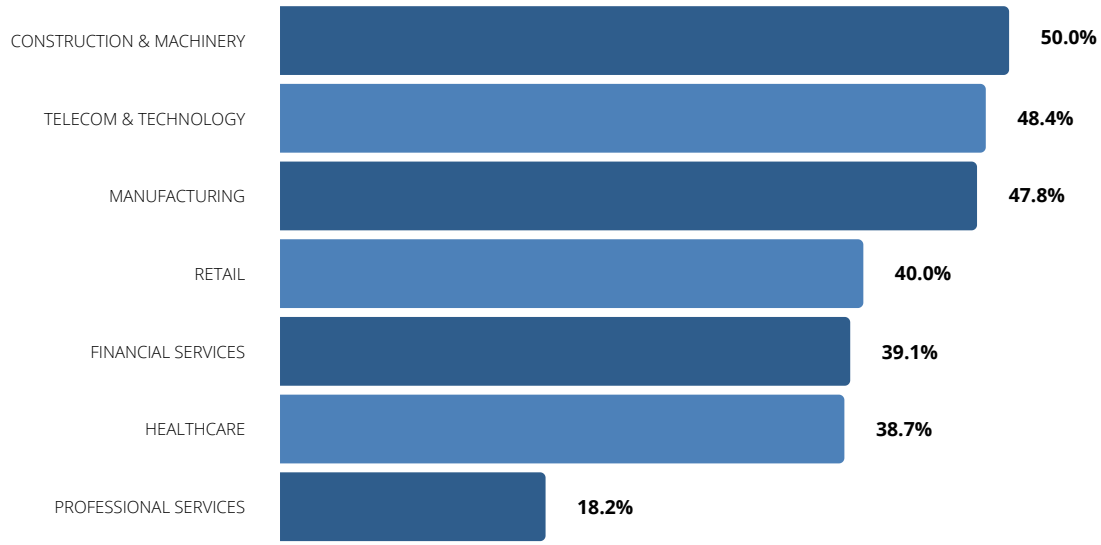
Figure 13.



With the notable exception of professional services, all of our other top respondent industry sectors rated above the 35.6% average for being 'more inclined to pay than not' (i.e., the sum of "very likely" and "somewhat likely" from Figure 12).

More inclined to pay ransom than not, by industry

Figure 14.

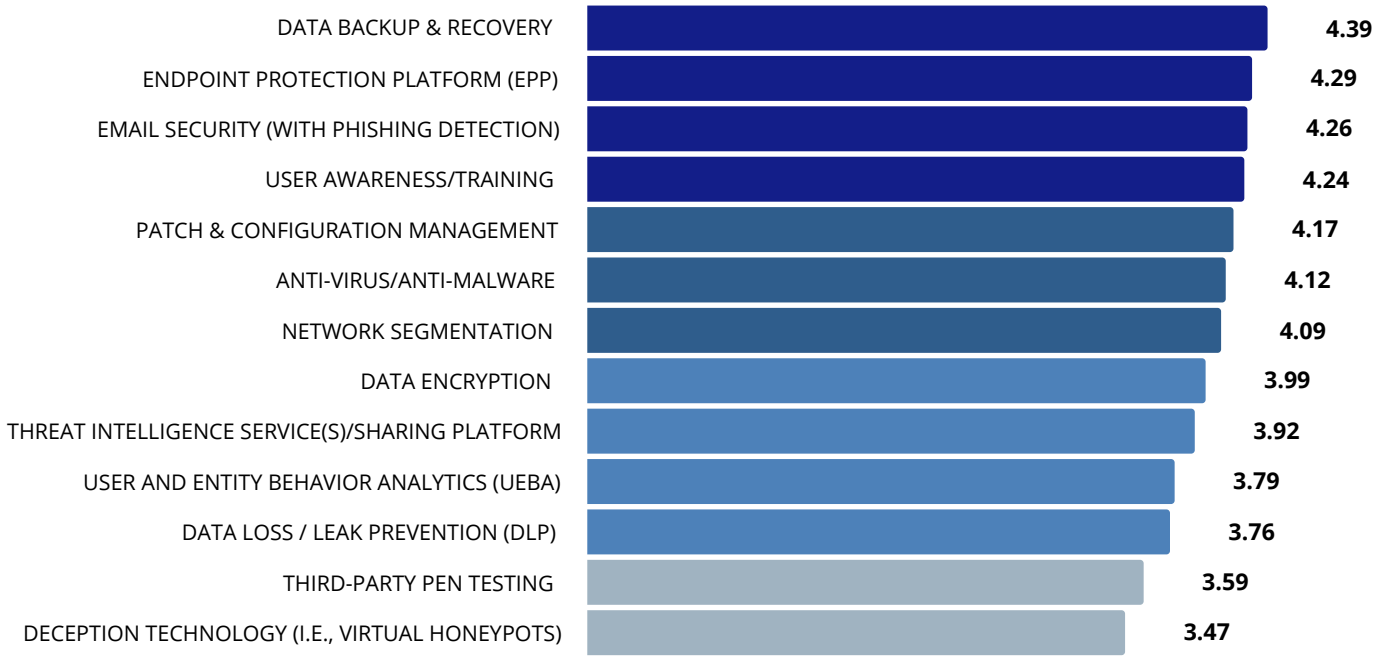


Strengthening Defenses

Obviously CISOs are laser-focused on countermeasures to mitigate the impacts of increasingly likely ransomware attacks. We asked respondents about their perceived importance of a variety of leading defensive technologies and practices. Not surprisingly, the most important countermeasure is data backup and recovery, followed by measures that involve endpoint and user vulnerabilities, where some of the greatest risks are found. In this regard, security teams also need to consider the growing population of IoT, IoMT, and OT devices – many of which are unable to accommodate agent software as the means for establishing visibility and protection.

> "Earlier this year, it was almost every two or three days a company was getting hit. It was becoming high visibility. I knew our Board would ask about it. So, I made it a key part of my reporting metrics at the Board level. I want to give them assurance that we recognize this is a huge risk area."
>
> Dave Ruedger, CISO, Invitae

Most Important Countermeasures **Figure 15.**



Pragmatically, all of the technologies and practices listed are, to a large degree, 'important,' with ratings having a spread of less than one point. This reflects the need for multi-layered defenses. It also suggests that whatever defenses respondents already have in place or are putting in place next is more a matter of an organization's cybersecurity program maturity than of the merit of any particular technology.

So where are respondents in that defensive journey?

Currently, the most widely used defenses for ransomware center around endpoint and user protections, and data backup and recovery, where plans show the intent to improve further. That respondents already feel confident in these defenses is encouraging given the nature of the ransomware threat and how it operates. This illustrates a focus on closing down key entry points and, of course, being ready to restore and recover critical business data.

"You need to be able to connect everything and to correlate everything. To do that, you need to be able to see everything. Without visibility, there's no way you can correlate, detect and prevent."

Angel Redoble, PDLT Group

Which of the following countermeasures are currently in use or planned for implementation/upgrade (within 12 months) by your organization to mitigate the impact of ransomware attacks?

Table 1.

	Already in good shape	Plan to upgrade	Plan to add	No plans
Anti-virus / anti-malware	74.1%	13.4%	10.9%	1.6%
Email security (w/ phishing detection)	64.9%	17.3%	15.3%	2.4%
Data backup & recovery	60.7%	23.5%	14.2%	1.6%
Endpoint protection platform (EPP)	59.8%	17.1%	19.5%	3.7%
User awareness/training	58.9%	20.2%	18.1%	2.8%
Patch & configuration management	51.4%	24.7%	18.6%	5.3%
Third-party pen testing	47.1%	15.7%	22.3%	14.9%
Data encryption	46.8%	27.8%	18.5%	6.9%
Threat intelligence services(s)/sharing platform	46.3%	22.0%	22.0%	9.8%
Network segmentation	38.4%	27.8%	27.8%	6.1%
Data loss/leak prevention (DLP)	38.2%	22.8%	27.2%	11.8%
User & Entity Behavior Analytics (UEBA)	34.8%	18.9%	31.6%	14.8%
Deception technology	34.3%	18.2%	21.5%	26.0%

For half or more of respondents, ransomware defenses that are at the top of the coming year's shopping list (whether for adding or upgrading) include network segmentation, data loss prevention (DLP), and user & entity behavior analytics (UEBA), with data encryption listed by close to half (46%). It makes sense to see these countermeasures prioritized; all are generally more difficult to implement and manage, and/or are newer technologies for organizations to adopt.

Network segmentation's top billing is not surprising given increasing adoption of Zero Trust Network Access (ZTNA). Zero Trust requires not only that every access attempt be verified, but also that the scope of access granted is minimized in accordance with the principle of least privileges. This approach limits the lateral movement an attacker can achieve after breaching a network, in turn limiting the damage that can be wrought. The practice of network segmentation was even included as a top recommendation in the White House guidance on ransomware protections for businesses issued in June 2021.

The high degree of interest in UEBA also makes sense. It speaks, in general, to the need for organizations to not focus solely on preventive measures. Getting hit by malware/ransomware and other classes of threats is inevitable. In such instances, having the means to efficiently and effectively detect and respond to the incident could be the difference between another routine malware event and one that has a $5M impact (see Figure 6).

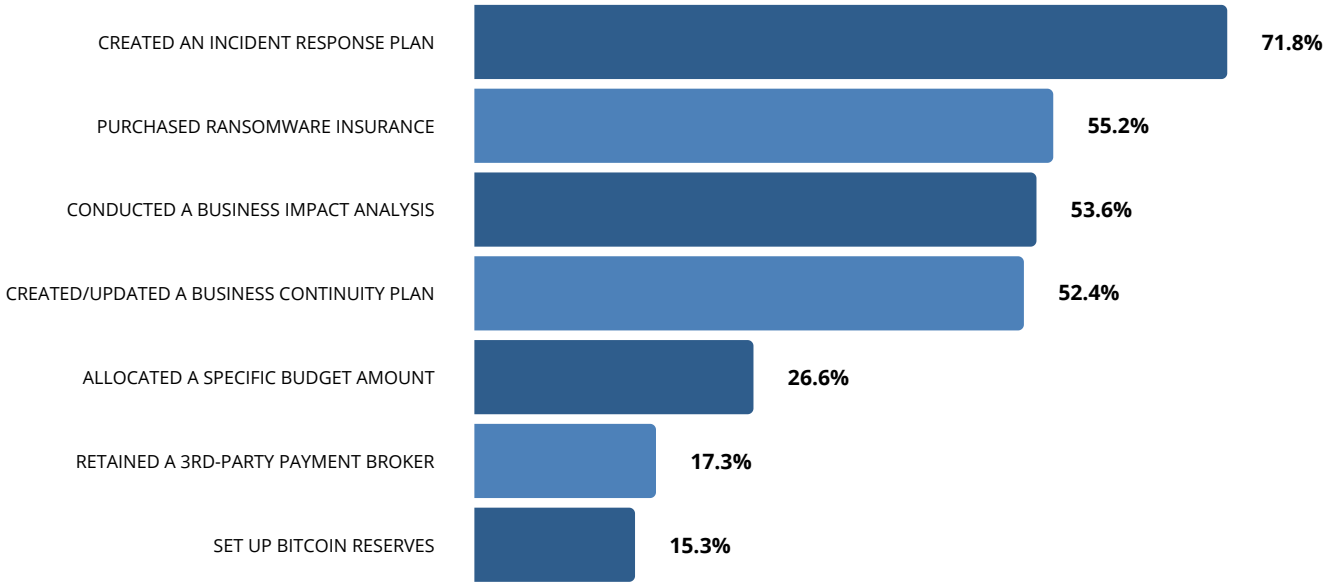
It is somewhat surprising to see the middle-of-the-road positioning of patching and configuration management, which is both central to good cyber hygiene and crucial to reducing the attack surface. Deception technology shows the lowest level of both current adoption and intent to adopt.

> "Do you have proper segmentation? I'm worried about east-west lateral movement. It does you no good if all an attacker needs is one entrance. Then, if he has lateral movement internally throughout the company, that actually puts you at severe risk. Treat your computing environment like a submarine, so that if any one portion fails, the whole sub doesn't go to the bottom of the ocean. You want to compartmentalize as much as you can, especially your mission critical assets."
>
> **CISO and VP of IT, Large Retail Enterprise**
>
> "The number one thing is good, isolated/immutable backups of everything you need to continue your business, that's your failsafe. Segmentation is also a huge mitigation strategy. The more you can segment your network the better. If you do get hit, ideally, you can limit the incursion to a specific segment of your network and it doesn't just run rampant. Doing tabletop exercises is another key activity along with having ransomware playbooks and good overall cyber hygiene."
>
> **David Levine, VP Corporate & Information Security, CSO, Ricoh USA, Inc.**

Along with defensive technologies and practices, we inquired about which proactive business preparations respondents have made in anticipation of a successful ransomware attack. Close to 72% have created an incident response plan, and 52% have created a business continuity plan. It is somewhat surprising that those percentages are not even higher, given the clear risks. It's also curious to note that relatively few respondents (one quarter or less) have made preparations for actual ransom payment, should it be needed. Since this data reflects action previously taken, it may be that more organizations are planning to adopt such preparations given the acknowledged increase in the level of threat. In any event, given the scope of the ransomware problem, proactively identifying an intermediary who can engage threat actors directly to negotiate asset reacquisition or payment settlement confidentially seems like a prudent step to us.

Have you made any proactive business preparations specifically for a ransomware event?

Figure 16.



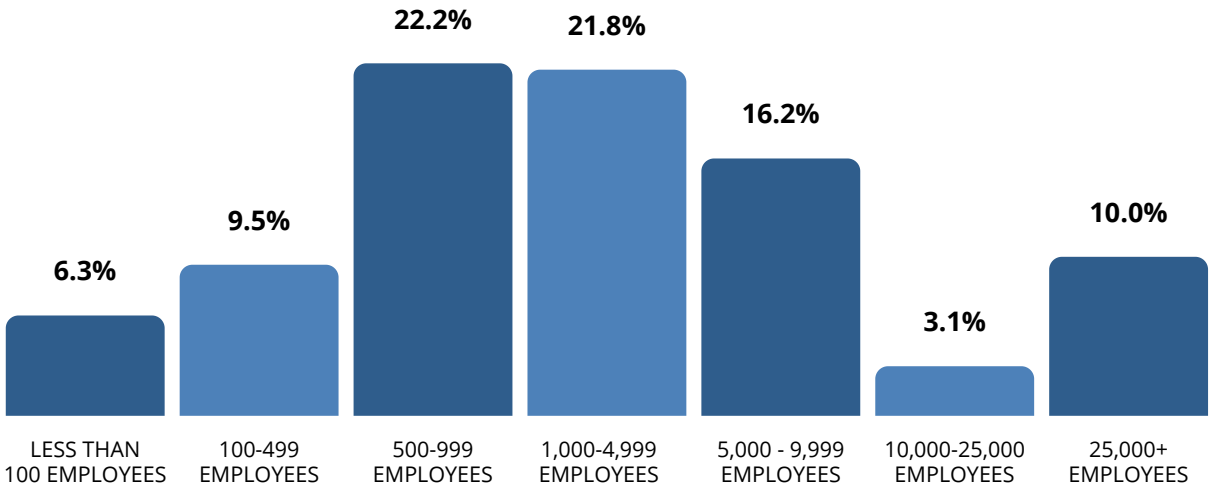
Cryptocurrencies like Bitcoin and related blockchain technologies are an interesting variable in the ransomware equation. They not only threw open the door for rampant ransomware attacks, but they also offer some frighteningly innovative ways to fuel its expansion, like establishing mechanisms to reward cybercriminals for specific malicious behaviors, and even to engage 'investors.'

Still, organizations are not proactively amping up their cryptocurrency reserves. While there have been some headlines about companies setting up accounts, only 15% of respondents had actually taken that step. It is true that companies could rely on third-party payment brokers to build reserves for them, but only 17% of respondents have retained such a broker. This could be setting a lot of organizations up for a scramble if they need to pay a ransom in short order.

Those who had purchased Bitcoin reserves included mostly smaller to mid-sized organizations. Companies in the tech sector led the way, followed by construction and machinery (an interesting tech-savvy position for a generally traditional sector).

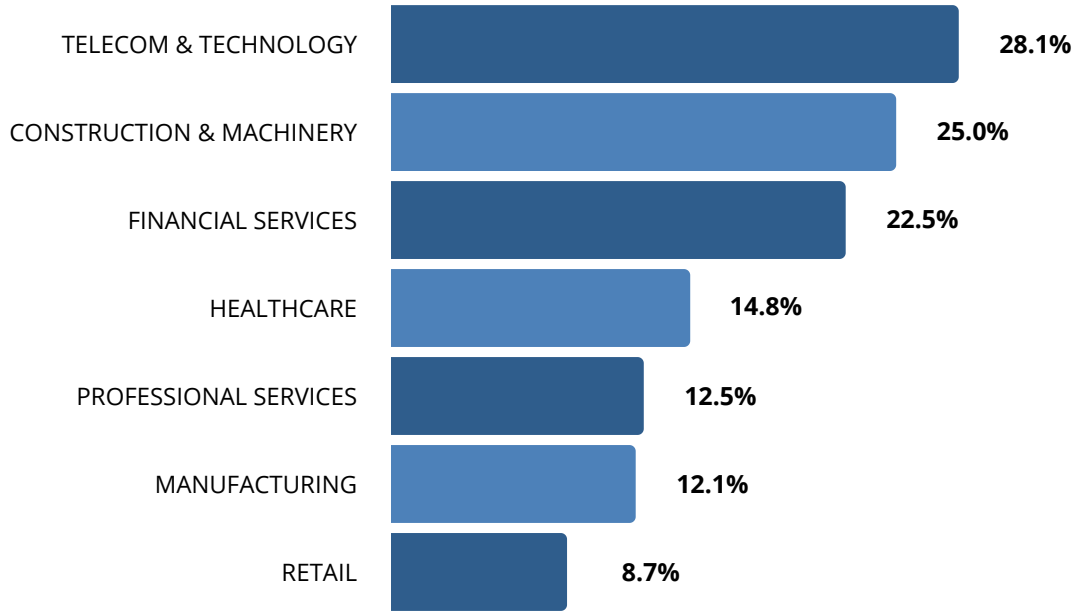
Set up bitcoin reserves, by size

Figure 17.



Set up bitcoin reserves, by industry

Figure 18.



Ransomware Insurance

Fifty five percent of our respondents had purchased ransomware insurance; clearly it's a rising trend. But all members of our CISO Board noted that the cost of that insurance, and the complexity of acquiring it, have increased significantly in the last year. Insurers are carefully examining an applicant's preventive and protective measures as qualifiers for coverage. (Getting very particular about specific measures also leaves room for loopholes through which providers may later deny benefit payout.)

Premiums for larger organizations can reach one hundred thousand dollars per year or more; deductibles can be in the millions. Given that, a total ransomware impact of $1M-$5M (which reflects the largest percentage of responses we received - see Figure 6) may be equal to or more than an organization's insurance benefit, and thereby is better coming directly out of the company coffers. It also seems appropriate that management teams should revisit the fundamental question of whether such coverage is really worth it. Perhaps those dollars would be better spent beefing up their prevention, detection, and response capabilities.

The purchase of ransomware insurance is more prevalent for larger organizations, leaving smaller organizations more vulnerable. Insurance is most frequently acquired by companies in the construction, technology/telecommunications, and manufacturing sectors.

"Insurance premium increases for this year are three figures percentage-wise. Even those companies that are mature and never had an issue are still going to see their insurance double. And those who have had an issue or whose security programs are not deemed to be mature will see 150% or more."

CISO and VP of IT, Large Retail Enterprise

"We saw a huge change in the last year relative to cyber insurance. It used to be you would get a short and fairly high-level questionnaire. This year, it was multiple multi-page questionnaires, including one specific to ransomware. They were asking the right questions and if they didn't understand your answer, they were coming back and seeking clarification."

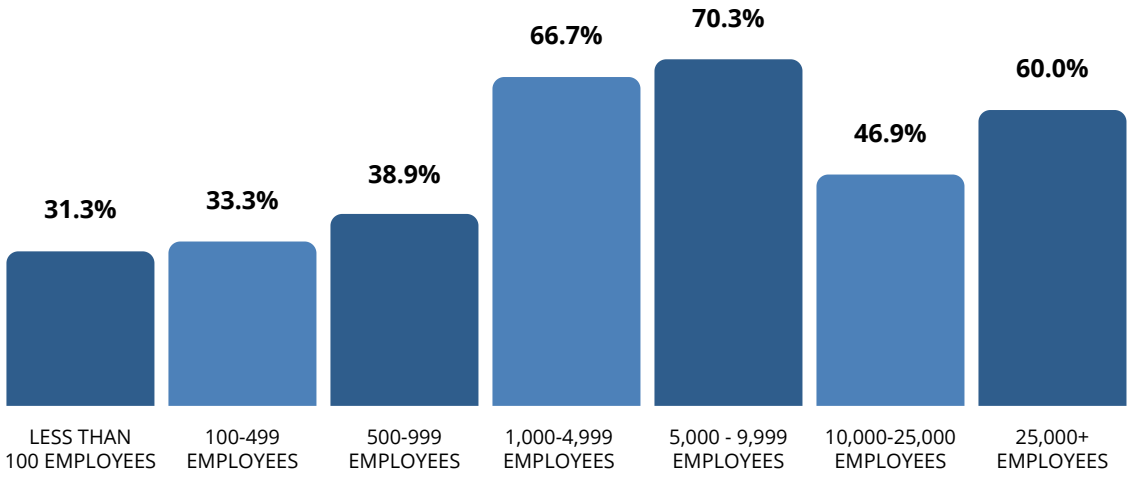
David Levine, VP Corporate & Information Security, CSO, Ricoh USA, Inc.

"Even the payment of a ransom is an engagement with the threat actor. The whole idea is to engage in communication with the threat actor. That will tell you how sophisticated they are, how serious they are, their background, their level of knowledge, and whether or not they will actually go through with it if you pay them. That puts you in a different negotiating posture."

Mark Rasch, Cybersecurity Legal Expert

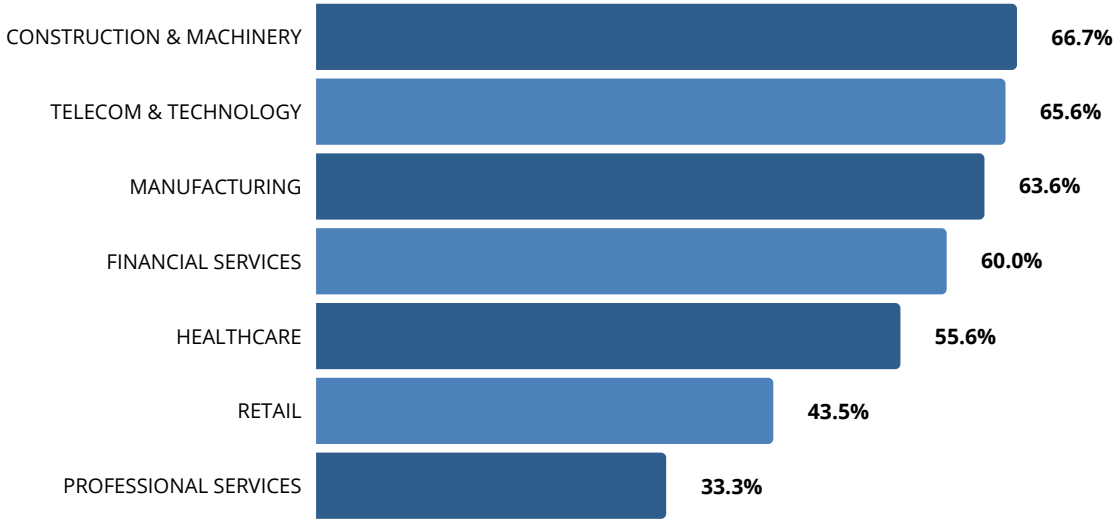
Purchased ransomware insurance, by size

Figure 19.



Purchase ransomware insurance, by industry

Figure 20.



What Holds CISOs Back?

For all of the actions already taken and plans made, CISOs still may face some obstacles to establishing what they consider to be effective ransomware defenses.

Countering long-term CISO frustration about the Board and senior leadership not really understanding cyber threats, our findings show this is not the case for ransomware, with Board support at the bottom of the obstacle list! Lack of support from executive leadership ranks only one quarter point above that. Even budgeting is not the obstacle it has traditionally been. This is a testament to the high-profile nature of the threat and the multi-faceted, high-value impacts that it can have.

At the other end of the spectrum, difficulty implementing related tools and technology, as well as the availability of technologies that are effective, rank as the biggest obstacles. And of course there is the perennial problem of the cyber talent shortage to implement solutions, along with 'other conflicting priorities,' lest we forget the plethora of security challenges today's organizations are facing. It's also worth noting that the aforementioned challenges seem well suited to a managed detection and response (MDR) solution -- especially for organizations where resource constraints preclude having their own full-blown Security Operations Center (SOC).

On a scale of 1 to 5, with 5 being highest, rate how each of the following affects your organization's ability to achieve effective ransomware defenses:

Figure 21.

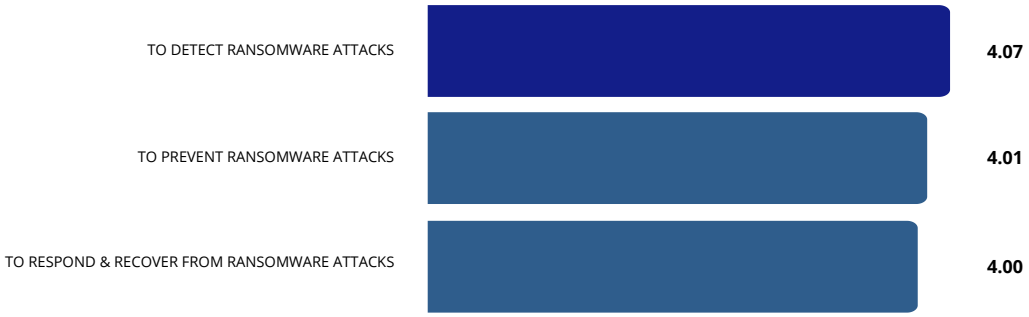
CISOs Remain Confident

Even with all of these concerns, respondents still seem to think they're in pretty good shape when it comes to ransomware mitigation. (That does make us wonder why so many are getting successfully hit or worrying about it.)

Ratings are tightly grouped with regard to respondents' ability to mitigate across the attack/defense lifecycle. Respondents are in just slightly better shape for attack detection, but still rate a strong 4.0 (WAVG) for their ability to respond and recover. Despite the newness of the ransomware explosion, most organizations by now have at least some experience dealing with other types of cyber incidents and breaches, which may account for their high confidence level.

On a scale of 1 to 5, with 5 being highest, rate your organization's capability:

Figure 22.



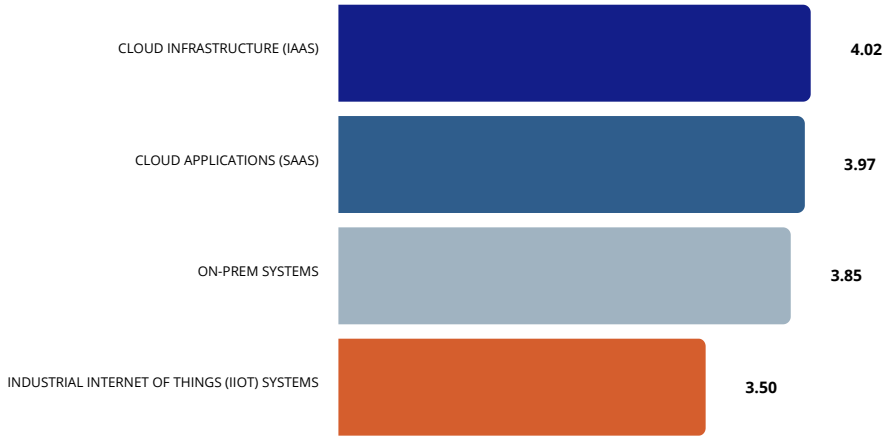
When it comes to their confidence in mitigating across system classes, on-prem systems are not at the top. That is a surprising finding given that those devices are physically present and most familiar to the organizations running them.

A possible explanation is that with the growth of outsourced cloud adoption, security resources are, in effect, doubled. Organizations mind their cloud environments, and count on the additional strengths of the cloud provider's mitigation capabilities. Even with the shared responsibility model cloud providers impose, there are areas that overlap, bolstering defenses.

The position of Industrial Internet of Things (IIoT) systems at the bottom of the chart is not surprising, as such devices are greatly proliferating, with security teams often lacking insight into exactly where they are being installed. The unfortunate reality is that IIoT devices are harder to manage, more diverse, and poorly covered by most technical countermeasures.

On a scale of 1 to 5, with 5 being highest, rate your organization's ransomware mitigation capabilities for each of the following class of systems (i.e., apps/devices/infrastructure):

Figure 23.



GOING FORWARD

As the ransomware problem continues to worsen and the ability to obtain and/or maintain insurance coverage becomes increasingly problematic, shoring up technical defenses is a necessity. In this regard, organizations will be well served by using a Prevent-Detect-Respond model – consistent with the organizing principles of the NIST Cybersecurity Framework and ransomware-specific best-practice guidelines published by the Cybersecurity and Infrastructure Security Agency (CISA) – to align their efforts and investments.

Based on these and other industry leading resources, core capabilities and technologies to pursue include:

Prevent

- Internal attack surface reduction, for example through regular vulnerability scans, aggressive patching, secure configuration management, and elimination of unnecessary networks services and apps
- External attack surface reduction, for example through third-party risk management (TPRM), as well as continuous monitoring of apps/resources/environments beyond the enterprise firewall – like social media, collaboration services, and the dark web – for malicious activity such as impersonations and account takeovers
- Endpoint/device protection, such as anti-virus/malware and network access control (NAC) – ideally including coverage for unmanaged/connected devices
- Email security (with phishing detection)
- Web and cloud security (for controlling and protecting access to infected websites)
- Strong authentication and privileged account management
- Monitoring/blocking the use of compromised credentials (i.e., ATO prevention)
- Cybersecurity user awareness and training

Detect

- Data loss prevention (DLP)
- Intrusion detection
- Anomaly detection (e.g., UEBA)
- Threat intelligence

Note 1: many of the technologies included in the Prevent stage also include significant detection capabilities (e.g., endpoint, email, and web security).

Respond

- Incident response plan (ideally with ransomware specific details/scenarios)
- Data backup (preferably immutable and easy/fast to restore)
- Network segmentation (for isolation purposes)

Note 2: Managed Detection and Response (MDR) and other forms of external assistance should also be considered, especially by organizations struggling to achieve the breadth, depth, and speed of the associated detection and response functions required to effectively handle a typical ransomware incident.

It is imperative to keep in mind that your adversaries are not standing still. Therefore, you shouldn't be either. It is critical to continually assess your organization's biggest vulnerabilities, strengthen your existing cybersecurity infrastructure and practice attack response plans. Getting ahead of the curve, and staying there, also depends on considering additional layers of protections. These include more advanced and/or less widely deployed solutions already available in the market (e.g., zero trust networking, deception technology), and even completely new innovations/technologies, as they emerge.

ABOUT OUR SPONSORS

Alert Logic is the only managed detection and response (MDR) provider that delivers comprehensive coverage for public clouds, SaaS, on-premises, and hybrid environments. Since no level of investment prevents or blocks 100% of attacks, you need to continuously identify and address breaches or gaps before they cause real damage. With limited expertise and a cloud-centric strategy, this level of security can seem out of reach. Our cloud-native technology and white-glove team of security experts protect your organization 24/7 and ensure you have the most effective response to resolve whatever threats may come. Founded in 2002, Alert Logic is headquartered in Houston, Texas and has business operations, team members, and channel partners located worldwide. Learn more at alertlogic.com. Alert Logic – unrivaled security for your cloud journey.

Avast Business provides integrated, 100% cloud-based endpoint and network security solutions for businesses and IT service providers. Backed by the largest, most globally dispersed threat detection network, the Avast Business security portfolio makes it easy and affordable to secure, manage, and monitor complex networks. Our easy-to-deploy cloud security solutions are built to offer maximum protection businesses can count on, so they can stay safe online.

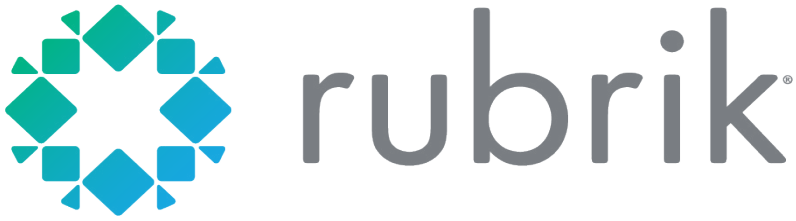
Our all-in-one cybersecurity solutions are built for today's modern workplace, providing total peace of mind. We help SMBs keep their data safe, so they can grow their business without worrying about the repercussions of cyber threats and devastating ransomware attacks. Avast Business protects against ransomware by delivering comprehensive security through a multi-layered defense that includes cloud backup, patch management, our cloud security platform, the Business Hub, and powerful, next-gen antivirus solutions equipped with four-shield protection. For more information about our cloud-based cybersecurity solutions, visit www.avast.com/business.

One in four organizations suffered from a cyber-attack in the last year, resulting in production, reputation and financial losses. The real problem is adversaries attack companies via third parties, island-hopping their way into target organizations. At Black Kite, we're redefining vendor risk management with the world's first global third-party cyber risk monitoring platform, built from a hacker's perspective. With 300+ customers across the globe and counting, we're committed to improving the health and safety of the entire planet's cyber ecosystem with the industry's most accurate and comprehensive cyber intelligence. While other security ratings service (SRS) providers try to narrow the scope, Black Kite provides the only standards-based cyber risk assessments that analyze your supply chain's cybersecurity posture from three critical dimensions: technical, financial and compliance.

Ordr discovers, profiles risks and behavior, and automates policies to secure every connected asset--from traditional IT devices to more vulnerable IoT, IoMT, and OT. Ordr can help organizations prepare for a ransomware attack, rapidly mitigate risks during an attack, and retrospectively identify prior infections. Ordr Systems Control Engine uses deep packet inspection and advanced machine learning to:

- Identify all assets that may be at risk such as devices with vulnerabilities and running outdated operating systems
- Track East-West movement and external malicious communications via an integrated threat detection engine and threat intelligence feeds
- Baseline device behavior to identify anomalies that may be early indications of compromise
- Automate policies to secure assets on existing security and networking infrastructure

Ordr is backed by top investors including Battery Ventures, Wing, and TenEleven Ventures. For more information, visit www.ordr.net and follow Ordr on Twitter and LinkedIn.



Rubrik, the Zero Trust Data Management Company™, enables cyber and operational resilience for enterprises; including ransomware protection, risk compliance, automated data recovery, and a fast track to the cloud. For more information please visit www.rubrik.com and follow @rubrikInc on Twitter and Rubrik, Inc. on LinkedIn.

ZeroFox provides enterprises protection, intelligence and disruption to dismantle external threats to brands, people, assets and data across the public attack surface in one, comprehensive platform. With complete global coverage across the surface, deep and dark web and an Intel-backed artificial intelligence-based analysis engine, the ZeroFox Platform identifies and remediates targeted phishing attacks, credential compromise, data exfiltration, ransomware, brand hijacking, executive and location threats and more. The patented ZeroFox Platform technology processes and protects millions of posts, messages and accounts daily across the social and digital landscape, spanning LinkedIn, Facebook, Slack, Instagram, Pastebin, YouTube, mobile app stores, domains, cloud-based email and more.

The way the world does business has changed, but the networking and security technologies that businesses rely upon are stuck in the past. They were designed when applications were in the data center and employees were on the network. Today's business doesn't look like that. It takes place off the network, with applications in the cloud and employees connecting from everywhere using a range of devices. Everything in this digital world is connected—user-to-app, app-to app, machine-to-machine—and it's all connected over the internet. This is exactly the world that Zscaler™ was designed to enable and secure.

Zscaler was founded on the belief that a new approach was needed to prevent cyberattacks, protect data, and enable fast, secure connections over the new enterprise network: the internet. We pioneered the Zscaler Zero Trust Exchange™, a global cloud platform distributed across more than 150 data centers. Instead of securing the network, the Zero Trust Exchange uses business policies to secure connections between any user, any application, and any device— from anywhere.

CISO BOARD OF ADVISORS

ANGEL REDOBLE, FVP & GROUP CISO, PLDT GROUP & SMART COMMUNICATIONS, INC.

Angel Redoble is a First Vice President and the Chief Information Security Officer of PLDT Group, Smart Communications and ePLDT Group. He is currently the Chairman and Founding President of the Philippine Institute of Cyber Security Professionals and The Chairman of the MVP Group Cyber Security Council.

Angel is an Adjunct faculty and course director for the Cybersecurity Executive Course at the Asian Institute of Management. He is the former Chairman of the PNP Anti Cybercrime Group National Advisory Council. Angel is also an alumnus of the National Defense College of the Philippines, where he is also a regular lecturer on the topics Cyber Security and Cyber Warfare.

Internationally, Angel completed the Cyber Warfare: Weaponry and Strategies of Digital Conflict program from the Technolytics Institute in the USA, and a course in International Cyber Conflict authorized by New York State University. Backed by his rich cyber security expertise and experience, Angel received the 2013 Asia Pacific Information Security Leadership Award from ISC2. He also received the 2013 and 2016 Awards from the Philippine National Police Anti Cybercrime Group for his contributions in the Anti-Cyber Crime campaign. He completed the online program Cybersecurity: Managing Risk in the Information Age from Harvard University and is an alumnus of Harvard Kennedy School on "Executives in National and International Security." Angel recently completed the Cyber Security for Business Leaders Program at SAID Business School University of Oxford. He was most recently recognized by his colleagues from Fortune 1000 companies as the Visionary CISO in the CISOs Connect C100.

HUSSEIN SYED, VP & CISO, RWJBARNABAS HEALTH

At RWJBarnabas Health, Hussein is responsible for information security and the organization's HIPAA compliance and security governance program. Hussein and his team are responsible for information security functions for the healthcare system.

Prior to joining RWJBarnasbas Health, Hussein started his professional career as a consultant in the network and systems management practice with a solutions integrator. He later joined a startup to lead development and management infrastructure as well security function of the online supply chain management provider.

A seasoned Information Technology professional with more than 25 years of experience.

KEVIN MCKENZIE, CISO & VP OF INFORMATION TECHNOLOGY, DOLLAR TREE INC.

Dr. Kevin McKenzie is Chief Information Security Officer (CISO) and Vice-President of Information Technology for Dollar Tree Inc. which encompasses Dollar Tree and Family Dollar stores following the acquisition of Family Dollar by Dollar Tree. Headquartered in Chesapeake, VA, Dollar Tree is the largest and most successful single-price-point retailer in North America. Kevin joined the leadership team at Dollar Tree Inc. in June 2016 where he is responsible for setting the strategic vision and establishing the security posture of the combined enterprise.

Prior to joining Dollar Tree Inc., Kevin was CISO and Executive Director for Clemson University where he was charged with establishing the information security strategic direction and leading a team to protect one of the nation's most dynamic and challenging higher education environments. In addition to his CISO role, he was also a Research Professor in Electrical and Computer Engineering where he frequently taught information technology courses and mentored future cybersecurity professionals.

FRED KWONG, CISO & ASSISTANT VICE PRESIDENT OF SECURITY, IDENTITY AND OPERATION, DELTA DENTAL PLAN ASSOCIATES

Dr. Fred Kwong has been in the information technology field for the past 15 years-working in education, financial, telecommunication, and insurance sectors. Fred currently works at Delta Dental Plan Associates where he currently serves as the Chief Information Security Officer. In his role, Fred acts as a thought leader for the Delta Dental member organizations and is working to drive risk-based security within the organization.

Before joining Delta Dental Plan Associates, Fred's work includes the creation of security and privacy policies, standards, and procedures. He has helped build risk-based security programs and has driven security strategy within organizations. With an extensive background in IT technologies, Fred continues to challenge the status quo by providing guidance in security and network architecture creating holistic designs that align to today's threat vectors for organizations. Fred has a passion for combining IT skills with organization development values. His broad range of IT skills has allowed him to view IT from many different paradigms and present them to the business partners in an easy to understand language.

He is a highly recognized thought leader in security and is often asked to speak and chair at national/international security conferences. Fred serves on several advisory boards and is often asked to consult on matters of security and leadership.

Fred serves as an adjunct professor at Benedictine and Roosevelt University teaching courses in international business, organization behavior, project management, and information systems. He holds a Ph.D. from Benedictine University and earned his master's degree in business administration from Roosevelt University. Fred is a Certified Project Management Professional (PMP), a Certified Information Systems Manager (CISM), a Certified Information Systems Auditor (CISA), a Certified Information Systems Security Professional (CISSP), Certified ITILv3 and a PCI Professional (PCIP).

DAVID LEVINE, VICE PRESIDENT OF CORPORATE AND INFORMATION SECURITY AND CSO, CISM FOR DIGITAL SERVICES AND INFORMATION MANAGEMENT PROVIDER, RICOH USA, INC.

David Levine is Vice President of Corporate and Information Security and CSO, CISM for digital services and information management provider, Ricoh USA, Inc. In this role, he oversees cyber and physical security, trade compliance, access management, eDiscovery and litigation support, select compliance functions and is routinely engaged in customer discussions on risk and security.

In addition, David chairs Ricoh's security advisory council and leads the company's global security team. He has held a diverse variety of positions during his 26-year tenure with Ricoh, including IT engineering, project management, vendor management, Six Sigma, technology infrastructure and end-user services leadership, giving him a great perspective on technology, the business and security. Levine is also part of Forrester Research's security and risk leadership board and the FBI's InfraGard program and is an Atlanta governing body co-chair with Evanta. In addition, he regularly speaks at industry events and is quoted in security articles with organizations and outlets including the Quartz Network, Interop Digital, Security Magazine and IDG Connect, discussing topics including third party risk management, authentication and the human factor in cybersecurity.

In 2021 he was named to the CISOs Top 100 CISO (C100) list by CISO Connect, a CISO-only member community of Security Current. The C100 peer recognition honors the top 100 CISOs across industries who are experienced and proven leaders as demonstrated by their commitment to sharing expertise with others and regularly giving back to the industry to help secure and protect organizations in the U.S. and globally. He holds a bachelor's degree in information systems with minors in computer science and business from Eckerd College.

RESEARCH TEAM

MARK BOUCHARD, CISSP

As CEO at AimPoint Group, Mark oversees the firm's research and consulting operations, while also serving as a senior research and marketing consultant. Mark's areas of specialization include information security, compliance management, application delivery, and infrastructure optimization. Before APG, Mark co-founded and was COO for CyberEdge Group, a marketing firm catering to the needs of high-tech solution providers. Previous positions include operating as an independent IT research and marketing consultant (7 years) and Vice President at META Group (acquired by Gartner), where he analyzed business and technology trends across a wide range of information security, networking, and systems management topics, helping hundreds of organizations worldwide address their IT challenges.

KATHY STERSHIC, CIPM, CIPP-US

Kathy is VP of Research, Messaging and Content Marketing at W2 Communications. She leads the agency's research efforts, and applies research findings as an informed foundation for client messaging and marketing initiatives. She is well versed in many of the leading technology issues relevant to modern private and public sector enterprises, including AI, cybersecurity, cloud, data-privacy, and risk-management.

Prior to joining W2 Communications, she headed boutique consultancy Dialog Research & Communications for 17 years. She previously served as Vice President for Cognitiative, Inc., a San Francisco-based consultancy specializing in marketing research and communication strategy for e-commerce clients; she also worked as a Senior Analyst for Jupiter Media Metrix Custom Research Group; and earlier in her career, worked on staff for several fast-growth software and hardware companies. She holds a Master's Degree from the George Washington University's Elliott School of International Affairs, and certifications from the International Association of Privacy Professionals.

AIMEE RHODES, CEO, CISOS CONNECT

Aimee is a former foreign correspondent with the Reuters News Agency serving out of Israel where she interviewed leading politicians and influencers as well as covered the then burgeoning cybersecurity sector. Previously, she served as Director of Israel Radio's English News Service where she was responsible for management and execution of four daily broadcasts, aired locally and internationally. Aimee also worked as an on-air news presenter for Jerusalem Online, broadcast globally. Aimee also is a seasoned marketer having led marketing at several security companies including Corero Network Security, Inc., Xceedium, AlgoSec and Whale Communications Ltd., acquired by Microsoft. She also served as Vice President of Media and Editorial Content at GenerationA, where she was responsible for launching an Internet-based news and information portal. She holds a Masters in Journalism and a Bachelors in Political Science both from Michigan State University.

CISOs CONNECT

CISOs Connect

201-835-9205

https://cisosconnect.com

AimPoint Group

AimPoint Group

https://aimpointgroup.com

W2Communications

W2 Communications

https://w2comm.com