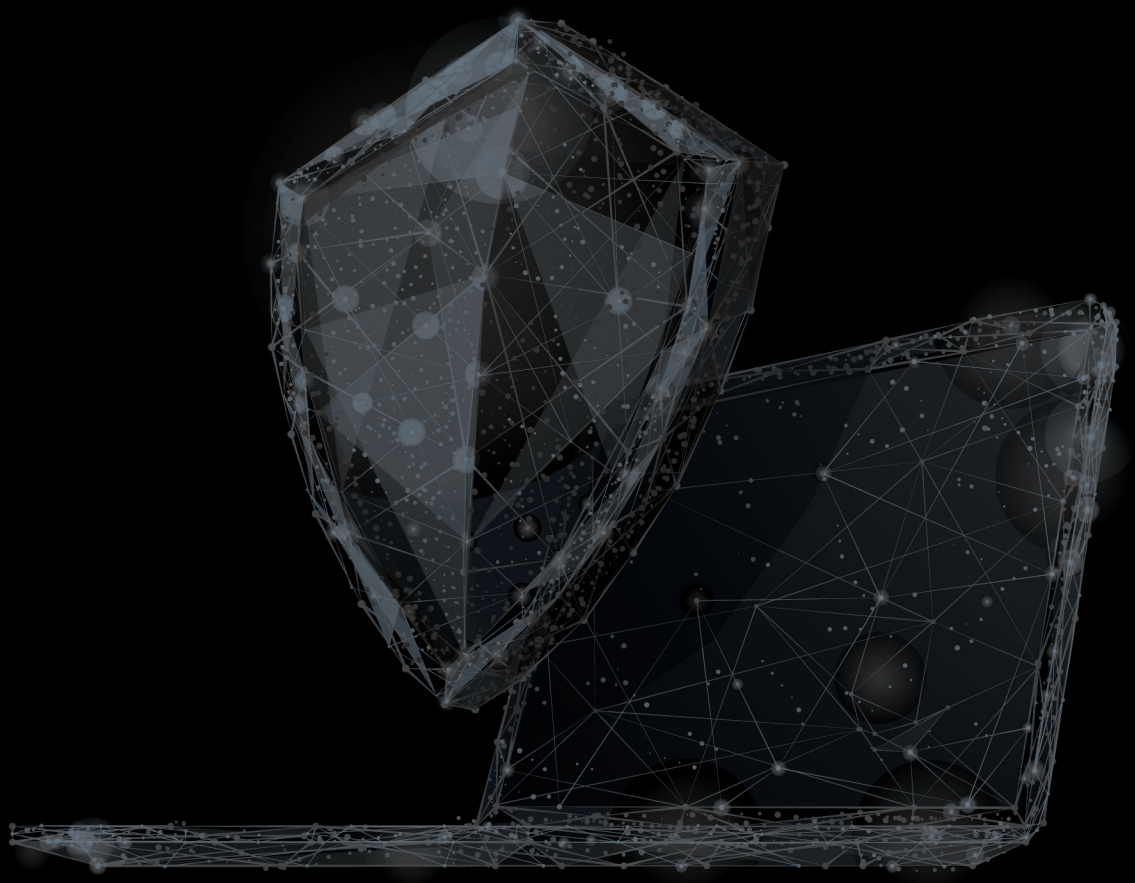
The SpyCloud **Ransomware Defense Report**

The state of current and future ransomware capabilities

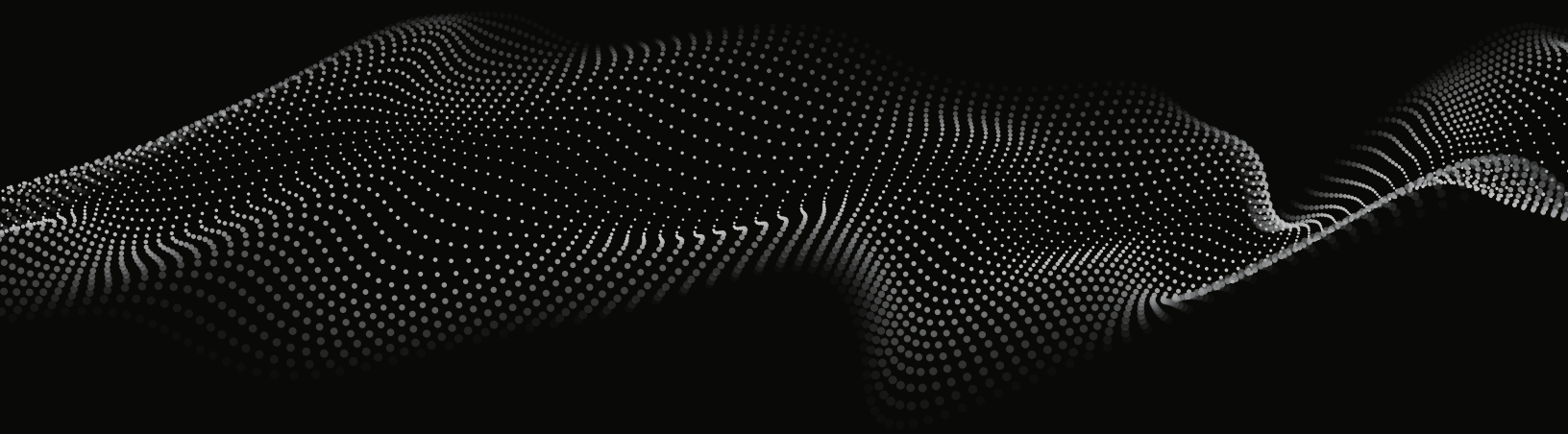
2021



SpyCloud

SpyCloud

Table of Contents



Overview of the Ransomware Problem

An avalanche of disruptive ransomware attacks in recent months have startled organizations across all industries in the public and the private sectors. These attacks shuttered businesses, harmed healthcare patients, and were deemed a growing national security threat.

While the ransomware problem isn't new, its scale and severity have escalated to unprecedented levels. In 2020, ransomware attacks soared a staggering 62% worldwide. And 2021 will shatter that record – the first six months alone brought 304.7 million attempted ransomware attacks, surpassing the 2020 total of 304.6 million.

The new generation of ransomware is not simply more prolific. It fuses automated and human-driven techniques, escalating recovery costs due to the resulting complexity. Organizations reported the average cost of ransomware recovery at $1.85 million in 2021, more than double the 2020 price tag of $760,000.

From our research, presented in this report, we learned that organizations are not optimistic about the ransomware problem in the next 12 months. Only 38% of SpyCloud survey respondents expect that a ransomware incident is unlikely to happen to them. Not surprising then, the increased frequency and sophistication of the attacks is the main factor impacting cybersecurity plans.

It's not all bad news, however. Our data shows that organizations are doing all the right things and moving in the right direction to fight back. And as we'll explain later, a few simple prevention steps can go a long way in alleviating the ransomware challenge.

Key Findings

1. **What we see is likely the tip of the iceberg.** The finding that 72% of surveyed organizations were affected by ransomware in the past 12 months is not unexpected. What's striking is that 13% were affected 6-10 times and 5% were affected more than 10 times. This indicates that the magnitude of the problem may be bigger than many people think – and the high-profile attacks that make the news are but a sliver of the full scope of the problem.

2. **Phishing emails and compromised credentials are the riskiest entry points.** Respondents ranked phishing emails with infected attachments or links as the riskiest vector for ransomware attacks; weak or exposed credentials aren't far behind. It wasn't surprising to see this dynamic duo at the top, on par with findings by various other researchers in the past year.

3. **People are the greatest barrier to effective ransomware defense.** Despite the rising costs of cybersecurity, budgets are the least of worries for organizations. The biggest hindrance is the lack of skilled security personnel, followed closely by low security awareness among employees. The pandemic has exacerbated both the talent shortage and the human vulnerability in a remote environment. But the problem goes deeper than that – and requires organizations to find new ways to protect employees from themselves.

4. **Ransomware incidents aren't going away any time soon.** At least not in the next 12 months, according to our findings. Only 18% of respondents believe a ransomware incident is not likely to happen at all in their organization in the next year, while 13% believe it's very likely to happen at least once and 22% believe it's very likely to happen multiple times.

Survey Demographics

SpyCloud solicited answers from individuals whose roles range from IT security analysts and architects/engineers, all the way to the executive suite. The majority of the 250 participants came from senior levels: 34% are CIOs, CISOs, and security executives; and 46% are security directors, managers or team leads (Figure 1).

We surveyed a cross-section of organization sizes (Figure 2), from small (500-999 employees) and midmarket (between 1,000 and 9,999 employees) to large enterprises (with 10,000 or more employees). The biggest cohort (40%) represents employers with 1,000-4,999 workers, while large enterprises comprise 23% in total (12% with more than 25,000 employees and 11% with 10,000-

Survey participants by IT security role

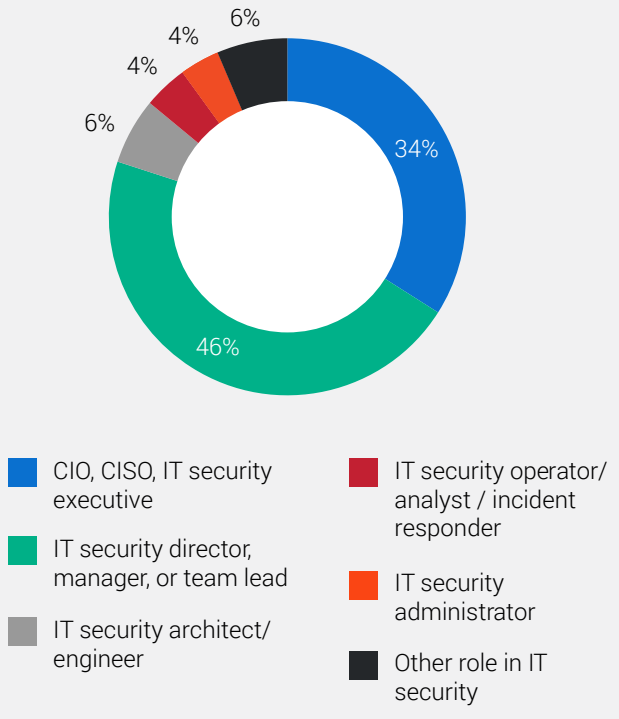


Figure 1

5. **The majority of organizations lack the most basic forms of prevention.** Despite seeing compromised credentials as a high risk for ransomware attacks, most organizations lack even the simplest practices for shoring up passwords and authentication. We were astounded to learn that 41% of organizations don't have a password complexity requirement, which is the easiest and least costly box anyone can check. Additionally, only 55.6% have implemented multi-factor authentication (MFA).

About the SpyCloud Survey

Given the crisis level that ransomware has reached across all sectors and organizations of all sizes, SpyCloud wanted to understand how security leaders and practitioners feel about the threat – and what they're doing to defend against it. We surveyed 250 individuals in active IT security roles at US-based organizations that have at least 500 employees.

The areas we examined include:

- The security practitioners' perceived maturity of their organizations' cybersecurity defenses
- Ransomware defense capabilities across the threat lifecycle
- The technologies and other preparedness steps that are the main priorities
- The top risks related to ransomware, as well as the biggest obstacles
- Expectations and plans for the next 12 months

In addition to highlighting the survey findings, this report identifies best practices organizations can implement to improve their ransomware defenses. We encourage you to use the actionable survey data as you make future decisions about your cybersecurity strategies and investments.

Survey participants by size of organization

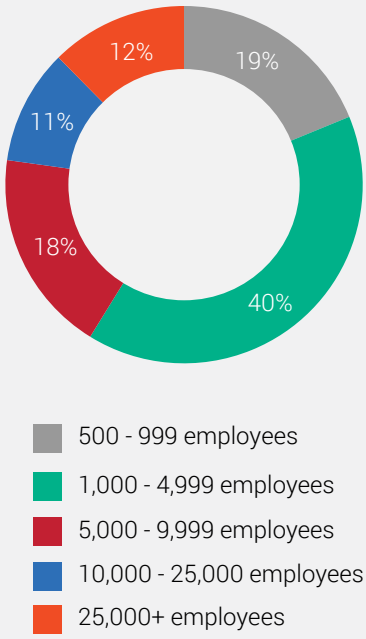


Figure 2

Section 1 | The Breadth of the Problem and Current Posture

Who's Affected by Ransomware?

Double-extortion tactics, new ransomware-as-a-service business models, targeted attacks combining automated techniques with human operators – these and other factors have contributed to the evolution of ransomware in the past year. The result was a surge in the number of attacks and record levels of disruption.

In 2020, ransomware rose to the top type of incidents, comprising 23% of all attacks analyzed by IBM Security researchers. Ransomware was also the root cause of 35% of data breaches disclosed publicly between January and October 2020.

The SpyCloud survey data reflects these trends – 72% of the security practitioners we surveyed said their organization was affected by ransomware at least once in the past 12 months (Figure 3).

Past Frequency of Ransomware Incidents

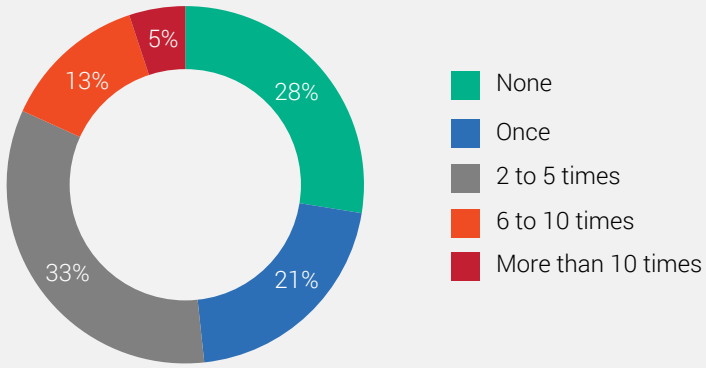


Figure 3

Organizations of all sizes were affected nearly to the same extent, with the exception of those with more than 25,000 employees (Figure 4). It's clear that smaller companies are not immune to ransomware attacks – and may, in fact, be an even bigger target. (The U.S. Department of Justice says attacks on small businesses make up 75% of ransomware cases.)

Affected at least once, by size of organization

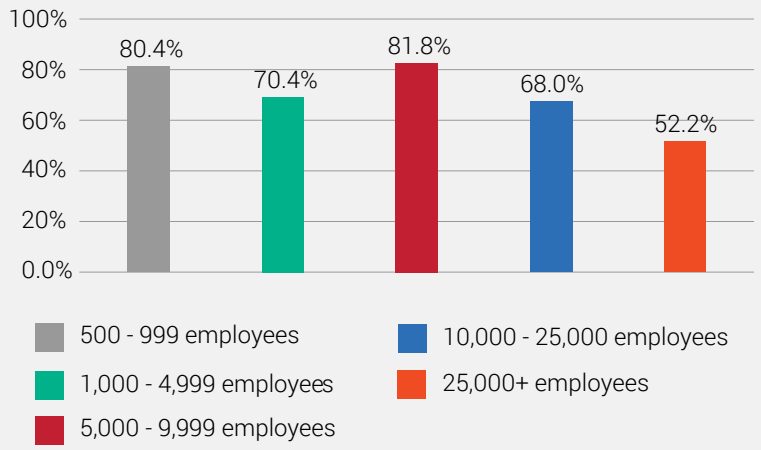


Figure 4

One surprising finding is that 13% of organizations were affected 6-10 times while 5% were affected more than 10 times. This may be due to the broad meaning of the term "affected," which could range from a security solution automatically stopping the malware to someone paying a ransom.

However, the data also suggests that the scope of the threat is much bigger than most believe. Many people base their understanding of the problem's scope on the attacks that make the news. Yet those successful, high-profile attacks are far from painting the full picture – and are only a fraction of the hundreds of millions of ransomware attacks launched over the course of the year.

The Rift Between Cybersecurity Maturity and Defense Capabilities

As we note later in this report, organizations are not only more aware of the ransomware threat but are also making inroads with their defense investments. So on the surface, it only makes sense that the majority feel good about the maturity of their cyber defenses, as well as about their ability to prevent, detect, and respond to ransomware attacks:

The Underground Ransomware Economy

Ransomware attack victims paid a total of $350 million in ransoms in 2020, an increase of more than 300% from the year before. The momentum continued in 2021, with a total of more than $208 million already paid out between January and July.

The underground ransomware industry is a well-oiled machine that drives the high success rate of the attacks. Cybercriminals specialize in different types of services, including ransomware-as-a-service, which charges a subscription fee or a "commission" for outsourced services and attack stages such as writing ransomware, obtaining stolen credentials, creating exploits, and so forth. Ransomware gangs even hire native English speakers to conduct negotiations with the victims in a more authentic manner.

Similar to a legitimate business, ransomware suppliers form relationships with their "customers," advertising their services, working to build their reputation, and even offering 24/7 support.

- A third (33%) of respondents rate their organization's maturity as exceptional and nearly half (48%) view it as above average (Figure 5).
- On a scale of 1 to 5, respondents ranked their ability to respond and recover a 4.27 average, followed closely by 4.22 for both their ability to detect and ability to prevent ransomware attacks (Figure 6).

Maturity of Cybersecurity Defenses

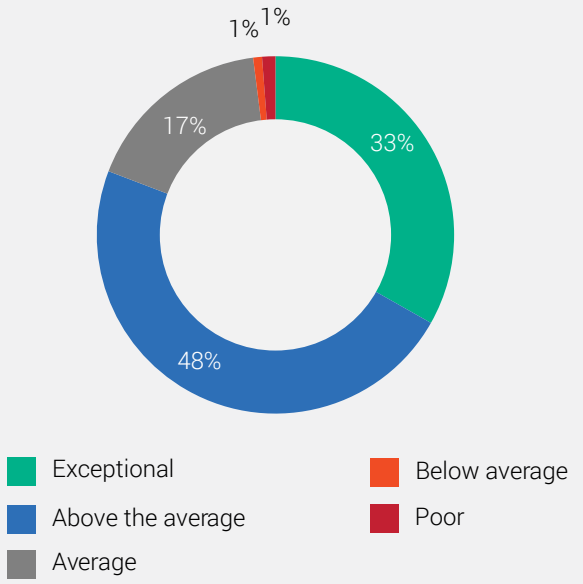


Figure 5

Perceived Ransomware Capabilities

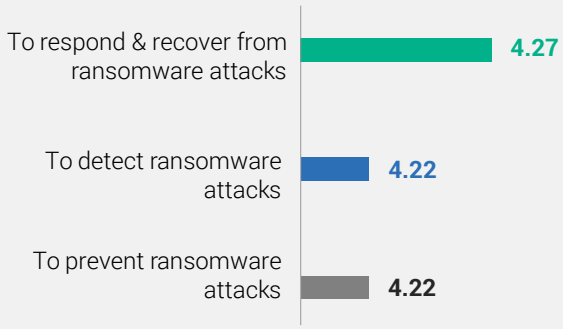


Figure 6

When we dig a little deeper, we find a dichotomy between that self-ranked maturity/perceived ransomware capabilities and both the past frequency of incidents (Figure 4 above) and expected future incidents. Not only were 72% of organizations affected by ransomware in the past 12 months, but 62% expect to be affected in the next 12 months as well. Additionally, 22% expect to be affected more than once (Figure 7).

Expectation of Future Ransomware Incidents

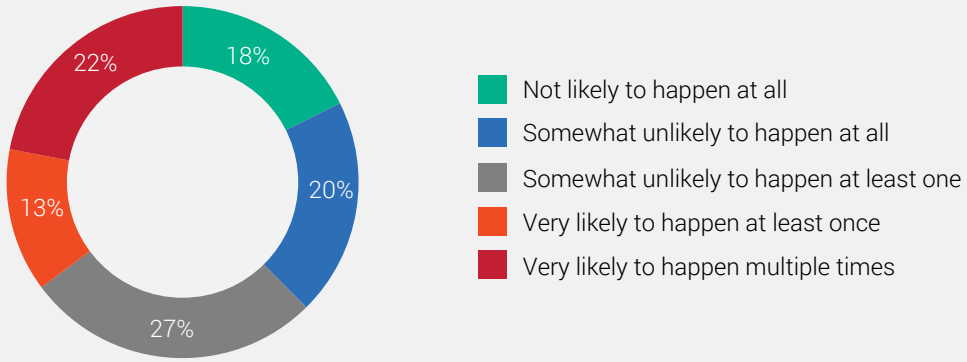


Figure 7

One way to explain this rift is a likely bias in the self-reported maturity and the self-reported capabilities. But it could also indicate that even the best defenses have limitations, especially considering the evolution ransomware and the growing sophistication of threat actors.

There's a good reason the U.S. Department of Justice called ransomware a growing national security threat in July 2021. And as ransomware attacks grow even more lucrative, funding improvements in the ransomware gangs' operations, defending against these attacks will get tougher still.

An Ounce of Prevention: Disrupt Early in the Lifecycle

Ransomware defense is a continuous cycle that starts with preparation and prevention. The earlier in the lifecycle that you can disrupt a ransomware attack, the more successful you'll be. It takes as little as 20 minutes to execute an attack – yet the median ransomware dwell time is five days and the average downtime after an attack is 23 days.

Account takeover (ATO), or the use of compromised credentials, has emerged as a top attack vector in the early stages of a ransomware attack. Last year alone, SpyCloud recovered 1.5 billion credentials from breaches and botnet logs. Considering the 60% password reuse rate among users (and 87% among government employees), ATO is not a colossal endeavor for threat actors.

Preventing ATO is very challenging, but not impossible. Continuous monitoring and remediation of exposed credentials is the key to early prevention. Without it, you can't be sure you've locked the front door to your corporate network, and you're vulnerable to threat actors looking for an easy way in.

The Early Life of Your Stolen Credentials

Some individuals and groups specialize in stealing credentials. They use scripts to discover vulnerabilities in backend servers, then look for databases with usernames or emails and passwords.

The credentials hold the highest value early in the lifecycle. These criminals, known as initial access brokers in the vendor community, try to monetize them as quickly as possible by selling them to ransomware operators, who use them as access points into their target organizations. While they have many methods at their disposal, operators have found that using compromised credentials is the fastest and most effective method, versus, for example, breaking through a firewall.

After a year or more, the credentials lose their value as some users reset passwords or turn on MFA, but their lifecycle continues. They're repackaged as commodity combo lists and sold at bargain prices. Cybercriminals use these cheap, massive password lists for credential stuffing attacks, which involve little sophistication and yield high success rates thanks to automation.

Section 2 | The State of Current and Future Ransomware Preparedness

The Silver Lining: Awareness at the Top

Not that long ago, cybersecurity leaders had to work hard to get buy-in from the top, and budgets were a common barrier. The tables have turned; now board support and budgets are the least of worries for organizations, even as costs of cybersecurity measures continue to rise.

High-profile attacks such as those on Colonial Pipeline and SolarWinds have fueled the leaders' awareness about ransomware in general and compromised credentials in particular. Among our respondents, 79% agree or strongly agree that recently reported attacks have "significantly elevated" their organization's concerns about weak or stolen credentials used by customers and employees; only 10% disagree. (Figure 8).

The general agreement was distributed fairly even among organizations of all sizes up to 25,000 employees. Among very large enterprises (25,000 and up), 67.7% generally agreed, compared to the 79% average overall – indicating that, perhaps, these large companies were already keenly aware of the risk of compromised credentials because of their more advanced practices.

Concerned About Using Weak or Stolen Credentials

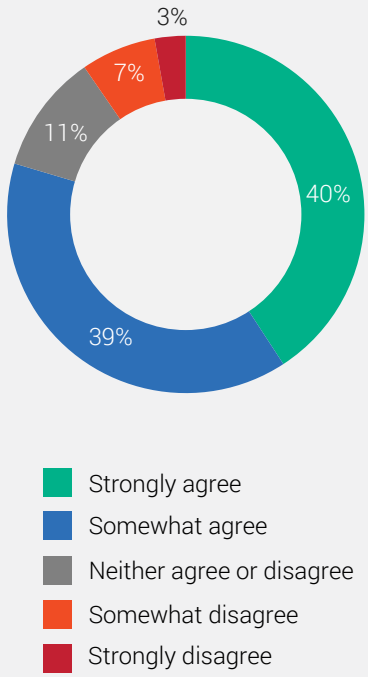


Figure 8

Another ripple effect of the media coverage is that boards now understand the multifaceted and acute impact of ransomware. Double extortion, for example, is now common. In early 2020, Maze operators were the ones primarily using this tactic, but by the end of the year, at least 17 other groups joined in and were publishing leaked data to incentivize victims to pay the ransom.

Based on data from insurance claims, ransomware incidents are more severe than other types by a factor of 2.5x. From direct costs and business disruption to intellectual property exposure and reputational damage, the massive jolt ransomware delivers is difficult to ignore, which has elevated this threat to a higher status and concern than other incidents.

Top Barriers to Defenses

With board buy-in and budgets out of the way, people are the main barrier to implementing security strategies. Respondents identified lack of skilled personnel and low employee awareness as their top two obstacles to effective ransomware defenses (Figure 9).

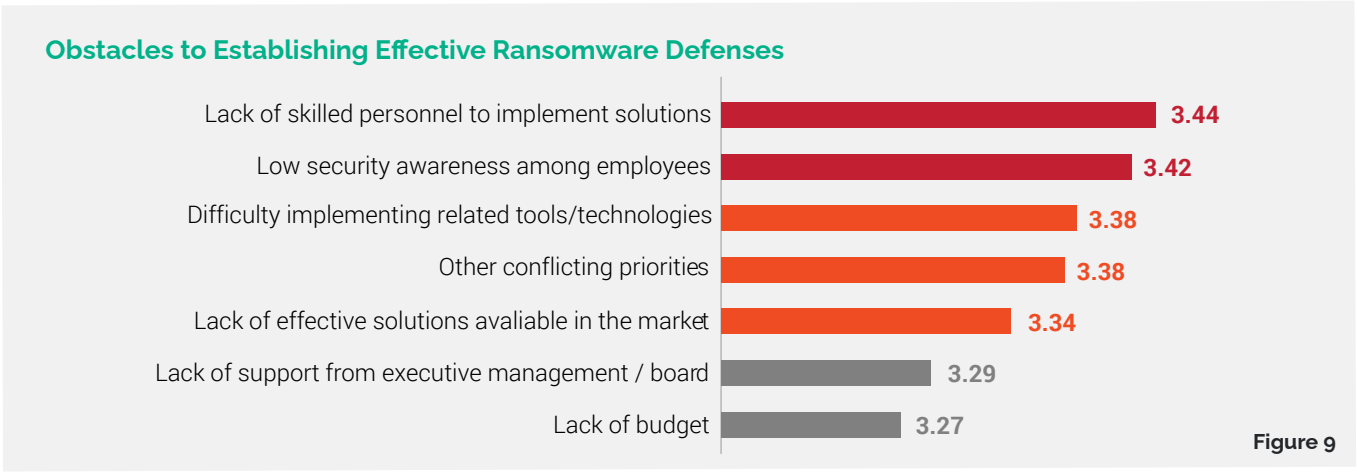


Figure 9

The talent shortage is not new. The estimated cybersecurity talent gap was 3.1 million globally in 2020, and has been in the millions for several years. Consequently, a 2021 survey of cybersecurity professionals found that the global skills shortage has impacted 67% of organizations.

Low security awareness among employees is a bit more surprising. It indicates that despite all the training that companies have been implementing, people remain their weakest link. The influx of remote workers during the pandemic has likely exacerbated both the talent shortage and the human vulnerability – especially since the remote environment brings new risks.

This indicates that employers need solutions that protect employees from themselves. Solutions that don't require intensive resources are especially effective because they're simple to implement and deliver fast time to value.

The Riskiest Vectors

Various research has consistently identified phishing emails and compromised credentials as the top vectors involved in security incidents. SpyCloud's respondents confirmed these rankings: they identified phishing emails with infected attachments and links as the riskiest ransomware attack vector, followed by weak or exposed credentials (Figure 10).

Riskiest Points of Entry for Ransomware

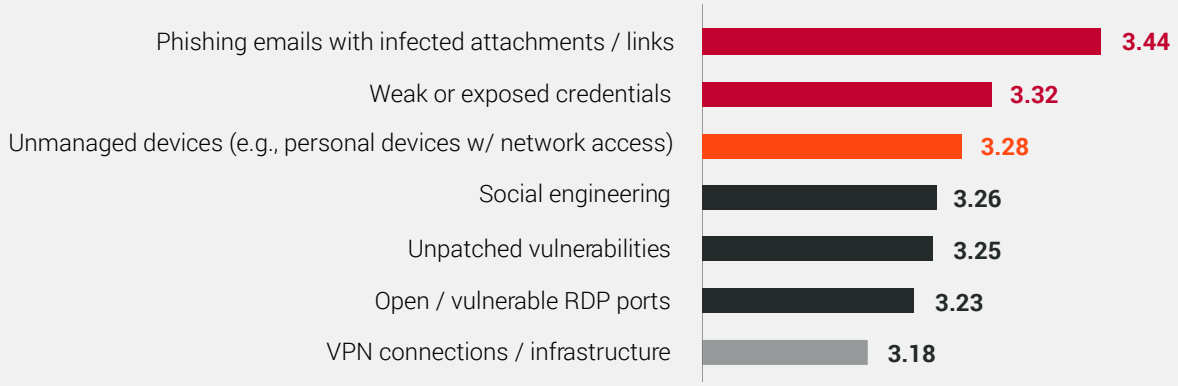


Figure 10

Worth noting is that unmanaged devices came in third, ahead of social engineering and unpatched vulnerabilities. Unmanaged devices are a bigger challenge in a remote environment, where 55% of employees can access managed applications.

This risk will persist as the trend of hybrid workplaces grows. What's particularly concerning is that SpyCloud data shows that 90% of organizations plan to continue support for remote workers, yet they believe the responsibility of security in the remote workplace falls on individual employees.

Lack of Basic Prevention

As we noted earlier, the majority of organizations see compromised credentials as a high risk for ransomware attacks. But this awareness doesn't translate into enacting best practices. The most basic form of password security is complex passwords – yet fewer than 60% of our respondents have this requirement (Figure 11). Fewer still (55.6%) have implemented MFA, another basic form of prevention.

Password and Authentication Practices

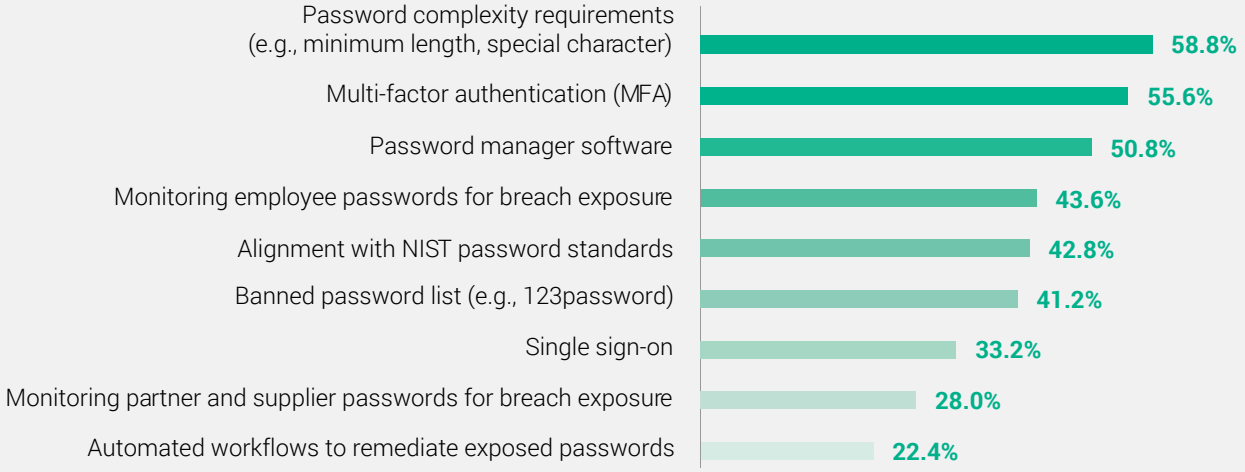


Figure 11

Passwords are a fact of modern life and are not going away any time soon. Although some see passwordless authentication as the answer to password risk, this alternative has its own challenges and vulnerabilities.

The truth is, replacing passwords doesn't necessarily improve security. But it's simple to strengthen authentication by protecting your passwords proactively, securing them from the moment an account is created, and then continuously monitoring them for compromise.

Common Defenses

In terms of defenses against ransomware, organizations are doing the right things and moving in the right direction. SpyCloud's survey shows that the majority either have a mix of basic countermeasures already in good shape or planned for upgrades (Figure 12).

At the top of the list of solutions organizations already have (either in good shape or in upgrade mode) are data backup, endpoint protection, MFA, and email security. This illustrates that the focus is on trying to stop malware and cover the biggest entry points, as well as prepare for an incident by backing up the data.

Countermeasures

	already have it
Data backup (at least weekly)	89.3%
Data backup (to an off-site location)	74.0%
Email security (with phishing detection)	74.3%
Multi-factor authentication (MFA)	77.0%
User awareness/training	75.5%
Endpoint/device protection	78.9%

Figure 12

Fewer organizations have more mature solutions but are planning to add them. The most common planned defenses are user and entity behavior analytics (UEBA), network and resource segmentation, and compromised credential monitoring (Figure 13).

The Power of One Compromised Password

The potential damage that one compromised password can unleash is no longer theoretical. The ransomware attack on Colonial Pipeline drove home the power of a single password when it crippled the operations of the largest fuel pipeline in the United States and cost $4.4 million in ransom alone.

The attackers gained initial access through an employee's virtual private network (VPN) account via a compromised password. While it's unknown how the threat actors obtained the credentials, researchers found them later on the dark web in a batch of leaked passwords.

It's highly likely that the employee reused a password that was stolen in a prior, unrelated data breach. As SpyCloud noted in its Annual Credential Exposure Report, across the 1.5 billion credentials we recovered during 2020, 60% of users reused at least one password across multiple accounts, potentially putting their corporate accounts at risk.

Security technologies in use or planned for ransomware mitigation

Already in good shape

Data backup (at least weekly)	67.8%
Data backup (to an off-site location)	53.3%
Email security (with phishing detection)	51.4%
Multi-factor authentication (MFA)	51.2%
User awareness/training	51.0%

Plan to Upgrade

Endpoint/device protection	29.3%
Deception technology (e.g., virtual honeypots)	27.3%
Patch & secure configuration management	26.9%
Intrusion detection system (IDS)	25.8%
Multi-factor authentication (MFA)	25.8%

Plan to Add

User and entity behavior analytics (UEBA)	39.7%
Network/resource segmentation	30.4%
Monitoring for compromised credentials	29.3%
Threat intelligence service(s)/sharing platform	27.2%
Deception technology (e.g., virtual honeypots)	26.5%

Figure 13

When planning your investment strategy, one thing to consider is your return on investment. Popular solutions like UEBA or resource segmentation (popular thanks to the growing zero trust security trend) are a big lift for most cybersecurity teams. These solutions are both hard to implement and hard to manage.

In contrast, monitoring for compromised credentials is simple to implement and is highly effective. It prevents not only ransomware from gaining a foothold, but other threats as well.

Ready with 'Plan B'?

Organizations may be bolstering their technical defenses, but not all of them are laying all their eggs in that basket (Figure 14). The majority (60.4%) are implementing ransomware-specific response plans and playbooks. Many are also purchasing ransomware insurance (50.4%) and even retaining third-party payment brokers (36.4%) and opening bitcoin accounts (30%).

Shifting the risk via cybersecurity insurance is a growing practice. But while insurance makes sense for some organizations, it's only a temporary measure that doesn't result in long-term improvements in security posture.

You may also find that obtaining a ransomware rider is increasingly difficult – and as the magnitude and costs of all security incidents escalate, so do the insurance premiums. Rather than relying on insurance, consider focusing on what you can better control: prevention.

Preparations for Ransomware Incidents

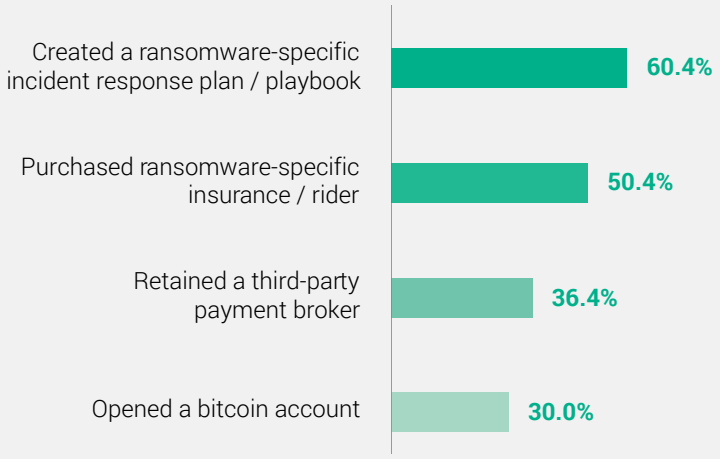


Figure 14

Ransomware: A Scourge Across All Sectors

The mean losses for ransomware attacks are nearly twice as much as for other types of malware. Losses like intellectual property, however, are tougher to quantify. Last year, more than 1,300 companies lost intellectual property and other sensitive data.

Ransomware attackers don't discriminate – they're hitting organizations across all industries. But some sectors, such as healthcare and government, are bearing the brunt of the attacks. Last year alone, ransomware attacks cost federal and local governments an estimated $18.8 billion.

Like in any other sector, credentials are a big pain point for governments, contributing to the rash of ransomware attacks. SpyCloud's analysis of recaptured credentials found 269,690 plaintext credentials from government employees leaked in 465 breaches last year. Government employees are also prone to the same bad habits as everyone else: SpyCloud research shows that 87% are reusing their passwords across their personal and .gov email accounts.

Section 3 | Solving the Ransomware Problem

As we noted earlier, organizations' security strategies are evolving and maturing. Given the prevalence and breadth of ransomware, it's not unforeseen that the increased frequency and sophistication of attacks have the greatest impact on new investments. Our respondents ranked ransomware a 3.62 average on a 5-point scale (Figure 15), followed by the increased severity of data breaches (3.17 average) and an increase in the remote workforce (3.14).

Greatest Impact to Cybersecurity Plans

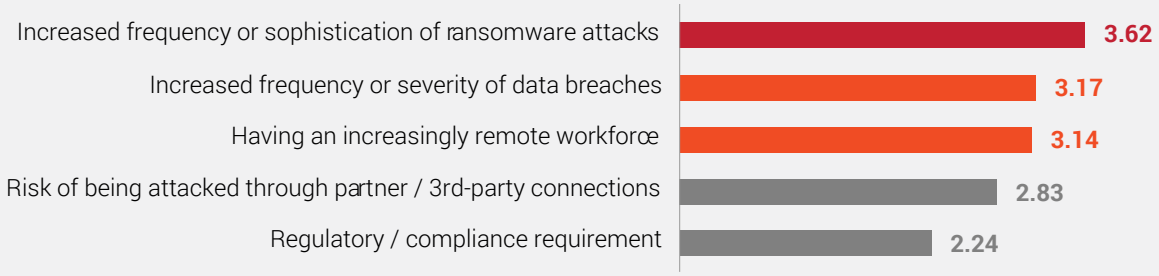


Figure 15

Ransomware is a hard problem to solve. Going back to our earlier point that you'll be the most effective early in the ransomware lifecycle, the best place to start is by preventing the infection in the first place. To get ahead of the attacks, focus on the most common entry vectors.

Stolen credentials are a major root cause that makes attacks possible. By monitoring for exposed credentials, you're remediating your ATO risk, and consequently drastically reducing the likelihood of an infection – not only with ransomware but with other forms of malware as well.

We expect that people will remain the biggest ransomware risk for the foreseeable future. You can't remediate that risk with awareness and training alone. Bad habits are tough to break, and this includes the propensity to reuse passwords. Besides, your employees are busy and shortcuts are simply a convenient way to boost productivity. Unfortunately, shortcuts like recycled passwords jeopardize your organization's security.

Look for ways to help save your employees from themselves. A simple solution is to detect compromised passwords and reset them before cybercriminals can go to town with them. Credential monitoring is different from many other preventative measures in two important aspects: it goes straight to the biggest root cause of the ransomware problem, yet it won't tax your resources because it requires little effort on the part of your IT and security teams.

Other Best Practices

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) recommends a series of steps for preventing ransomware attacks across the entire lifecycle. Best practices that CISA recommends include:

- Maintain offline, encrypted backups (and regularly test them).
- Reduce the attack surface and the likelihood of threat actors exploiting internet-facing vulnerabilities and misconfigurations.
- Properly secure remote services such as Remote Desktop Protocol (commonly used to gain initial access).
- Reduce the risk of phishing emails through technology and user training.
- Implement MFA as much as possible, especially for critical systems, webmail, and VPNs.
- Limit privileged user accounts through policies and access controls.

As we highlighted earlier, organizations are not very optimistic about the ransomware threat in the future, with only 18% confident they won't experience a ransomware attack at their organization in the next 12 months.

SpyCloud

The Future of Ransomware

Like remote work and passwords, ransomware is not going away any time soon. Cybercriminals have landed on a highly lucrative business model, and they'll continue to exploit this scheme for as long as victims are willing to pay, and pay handsomely.

The complexity of ransomware recovery will continue to increase as threat actors realize the benefits of intricate attacks such as those on the supply chain. And with this complexity, the recovery price tag will escalate further.

Prevention, on the other hand, costs a fraction of the recovery price. Organizations that want to boost their optimism about their future capabilities should reevaluate their strategies across the ransomware lifecycle – and focus their efforts on the much cheaper yet effective capabilities for prevention and early detection.

About SpyCloud

SpyCloud protects consumers, employees, suppliers, and citizens globally from the dangers of compromised identity. Its solutions make breached information actionable to prevent fraud, enabling a proactive, automated response that negates the value of stolen data before it can be used to cause harm. Its data also powers many popular dark web monitoring and identity theft protection offerings. SpyCloud customers include four of the ten largest global enterprises, mid-size companies, and government agencies around the world. Headquartered in Austin, TX, SpyCloud is home to over 100 cybersecurity experts who aim to make the internet a safer place.

To learn more and see an overview of your organization's exposed data, visit spycloud.com.

Employee ATO Prevention

Protect your agency from breaches and ransomware attacks.

Learn More

Active Directory Guardian

Automatically detect and reset exposed Windows accounts.

Learn More

Third Party Insight

Monitor suppliers' exposures and share data to aid in remediation.

Learn More

VIP Guardian

Protect your highest-risk users from targeted account takeover.

Learn More

Consumer ATO Prevention

Protect your users from account takeover fraud and unauthorized transactions.

Learn More

SpyCloud