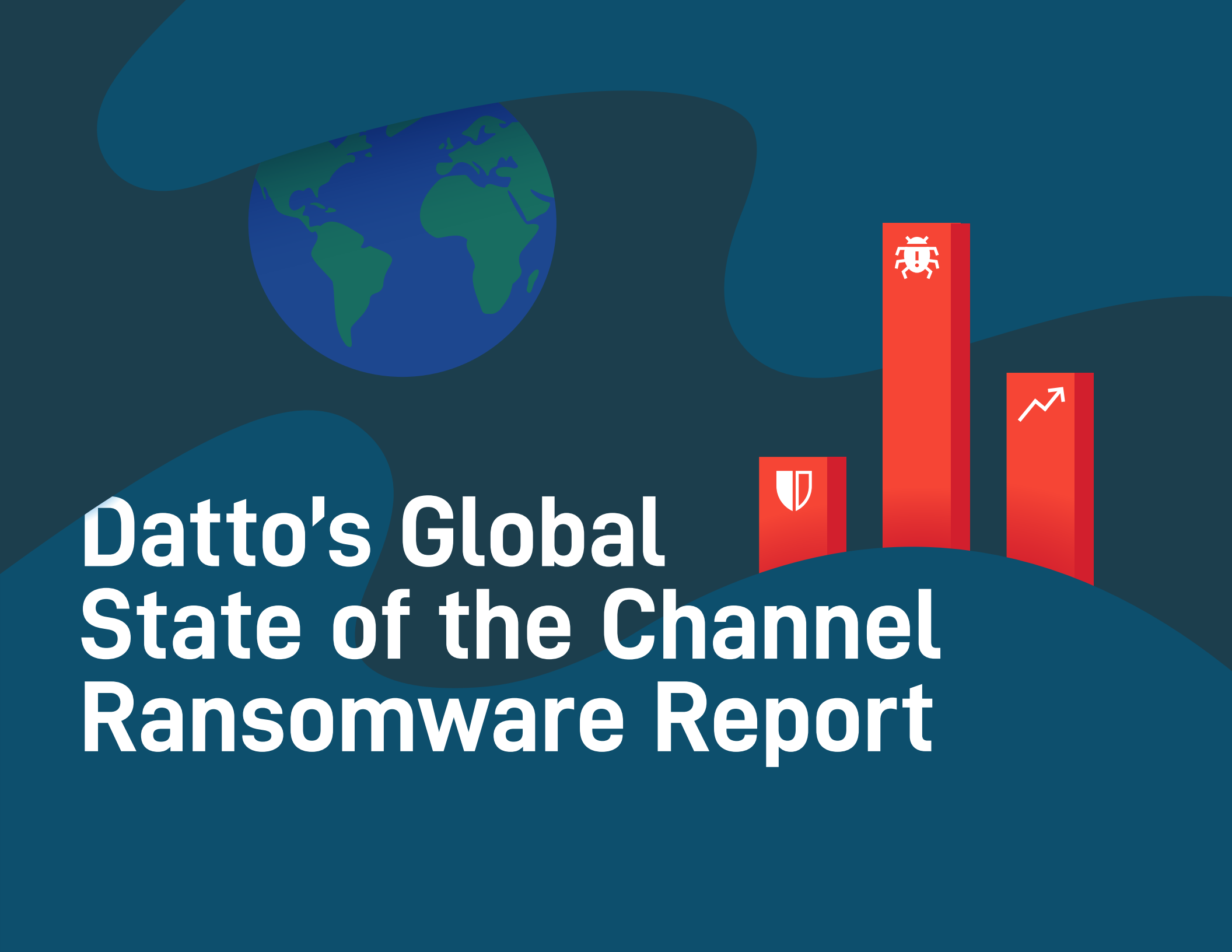


Datto's Global State of the Channel Ransomware Report

Table of Contents

Introduction

Datto's Annual Global State of the Channel Ransomware Report comprises statistics pulled from a survey of more than 1,000 managed service providers (MSPs) around the world. The report provides unique visibility into the state of ransomware from the perspective of the IT channel and their small and medium business (SMB) clients who are dealing with these infections on a daily basis. The report provides a wealth of detail on ransomware, including year-over-year trends, frequency, targets, impact, and recommendations for ensuring recovery and continuity in the face of this growing threat.

With respect to the current climate, the report also covers the impact that COVID-19 and the increase in remote work and cloud computing has had on ransomware trends.

The goal of this report is to help shed light on the current cybersecurity landscape businesses are facing. At Datto, we believe there is no limit to what small and medium businesses can achieve with the right technology. We hope the information compiled here educates your team and encourages you to work with an MSP to mitigate the risk ransomware poses on your organization.

Key Findings

1 **Ransomware is still the number one malware threat.** Nearly 70% of MSPs report ransomware as the most common malware threat to SMBs.

2 **COVID-19 has had an impact on security** — but not as much as you might think. MSPs were split on the security impact of the global pandemic.

3 **The ransomware disconnect between MSPs and SMBs remains.** 84% of MSPs are 'very concerned' about ransomware, but only 30% report that their clients feel the same.

4 **SMBs aren't the only businesses being targeted.** 95% of MSPs agree that their own businesses are increasingly being targeted with attacks.

5 **Phishing emails top the successful attack vector list.** Lack of cybersecurity education, weak passwords, and poor user practices are among the other top causes of ransomware.

6 **The aftermath of an attack is nothing nice.** 62% of MSPs said clients' productivity was impacted due to attacks, and 39% said their clients experienced business-threatening downtime.

7 **The average ransom requested by hackers stayed roughly the same year-over-year.** MSPs report the average requested ransom for SMBs is $5,600 per incident, compared to $5,900 last year.

8 **MSPs report that the average cost of downtime is 94% greater than it was in 2019.** Downtime costs are nearly 50X greater than the ransom requested in 2020.

9 **91% of MSPs report that clients with BCDR solutions** in place are less likely to experience significant downtime during a ransomware attack.

10 **92% of MSPs predict ransomware attacks will continue** at current, or worse, rates.

COVID-19 and Security

A Mixed Bag

Many MSPs reported that the number of ransomware attacks and security vulnerabilities increased during COVID-19 due to an increase in remote work and cloud computing. However, it is worth pointing out that it wasn't an overwhelming increase—more of an even split between those who saw an increase and those who did not.

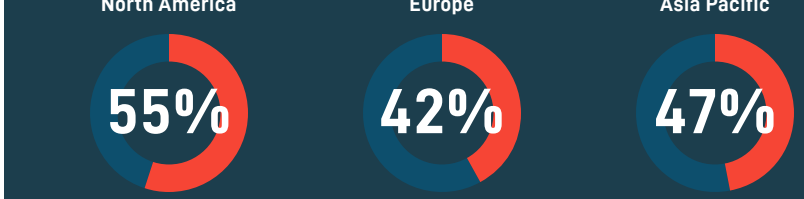
59%
of MSPs said remote work due to COVID-19 resulted in increased ransomware attacks.

52%
of MSPs reported that shifting client workloads to the cloud came with increased security vulnerabilities.

Increased risk can be attributed to user carelessness and security vulnerabilities associated with BYOD, according to respondents. "The risk comes from users lowering their guard as there are so many other things that have changed—health risks, working from home, etc," said one MSP.

"[Personal devices] have been introduced to corporate/business environments despite objections re: security policies/endpoint protection, etc. Additionally, there are significant additional remote work security threats, from device theft to family members using corporate machines for personal work/study," said another.

MSPs report healthcare as the most vulnerable industry during the pandemic (59%), followed by finance/insurance (50%), and government (45%).



GEO TRENDS

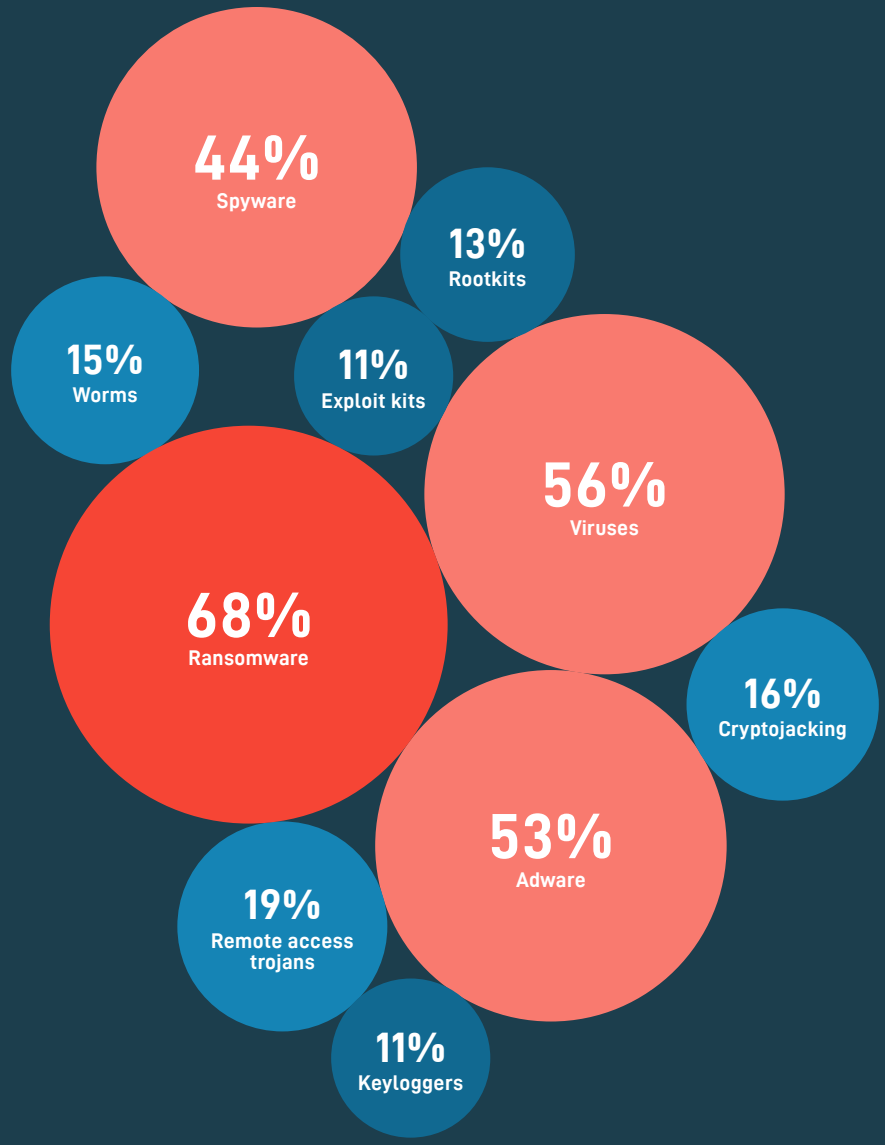
North American MSPs are somewhat more concerned about cloud security than their European and Asia Pacific counterparts.

A Variety of Malware Targeting SMBs

Among the malware threats impacting SMBs, ransomware is still at the top of the heap. However, it's far from the only threat on their plate. Viruses, adware, spyware, and remote access trojans rounded out the top five.

Cryptojacking, hot last year, cooled considerably, dropping 15 percentage points. This tracks with mainstream reports that cryptojacking is in decline as hackers have grown impatient with slow returns on coin mining.

In the last two years, MSPs report the following types of malware have affected clients:



**Survey respondents were able to select multiple answer choices.*

Ransomware Still a Major Challenge for MSPs

Ransomware continues to plague MSPs and the SMBs they serve. However, respondents reported a slight decline in the frequency of attacks. 78% of MSPs reported attacks on their clients in the past two years, down from 85% last year. That being said, **ransomware is still a very real threat with 60% of MSPs seeing attacks in the first half of 2020.**

It is worth noting that the general disruption of COVID-19 and resulting economic downturn may have impacted the frequency of attacks on the SMBs that MSPs serve. This is purely speculative, and outside of the research conducted for this report. However, it will be interesting to see whether MSPs report an uptick in ransomware attacks as the global economy continues to recover.

MSPs believe that will be the case. Nearly all respondents said they expect ransomware attacks will rise in the upcoming year.

78%
of MSPs report attacks against SMBs in the last two years

92%
of MSPs predict attacks will increase in the next year

60%
of MSPs report attacks against SMBs in 2020 alone

11%
of MSPs report that clients suffered multiple attacks in a single day

North America

Europe

Asia Pacific

European MSPs report that their clients suffered more attacks than any other region.

Ransomware is not going away, but attackers may have shifted their focus temporarily to other revenue streams during COVID-19. If you think of ransomware like a 'business' that needs to respond to changing market conditions, it makes sense for those attackers to focus on more stable sources of revenue, like larger enterprises, during an economic downturn. Enterprises both represent a larger 'return on investment' to hackers and are more resilient to fluctuations in the economy. Ransomware is a numbers game, and larger companies simply represent a better target in tough economic times.

Ryan Weeks
Chief Information Security Officer, Datto, Inc.

Ransomware Awareness

SMBs vs. MSPs

There is still a disconnect between SMBs and MSPs when it comes to perceptions about ransomware. The majority of MSPs believe businesses should be "very concerned" about the threat of ransomware, but only 30% report their clients feel this way. However, it appears that SMBs are beginning to understand how damaging ransomware attacks can be. 32% of MSPs report clients are "moderately concerned" and 34% say clients are "somewhat concerned".

30%
of MSPs report SMBs are "very concerned" about ransomware

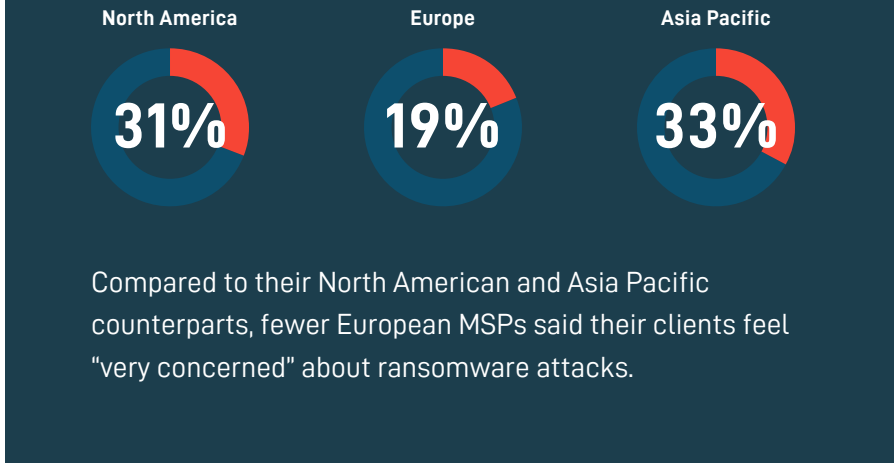
84%
of MSPs report SMBs should be "very concerned" about ransomware

SMB Security Budgets on the Rise

50%
of MSPs said their clients increased budget for IT security in 2020.

In addition to the growing awareness above, increased IT security spending shows that SMBs are beginning to take ransomware, and security in general, seriously. The slight decline in ransomware attacks this year might also indicate that these security efforts are having a positive impact.

GEO TRENDS



Compared to their North American and Asia Pacific counterparts, fewer European MSPs said their clients feel "very concerned" about ransomware attacks.

Ransomware Continues to Skirt Cybersecurity Efforts

Despite increased security spending, MSPs report that ransomware averted cybersecurity efforts including employee education, antivirus, email filtering, pop-up blockers, and endpoint detection solutions. Of them, 50% said ransomware averted antivirus/anti-malware solutions.

When asked about which antivirus/anti-malware solutions specifically, MSPs said:

59%
Anti-malware filtering (email-, network-, and web-based)

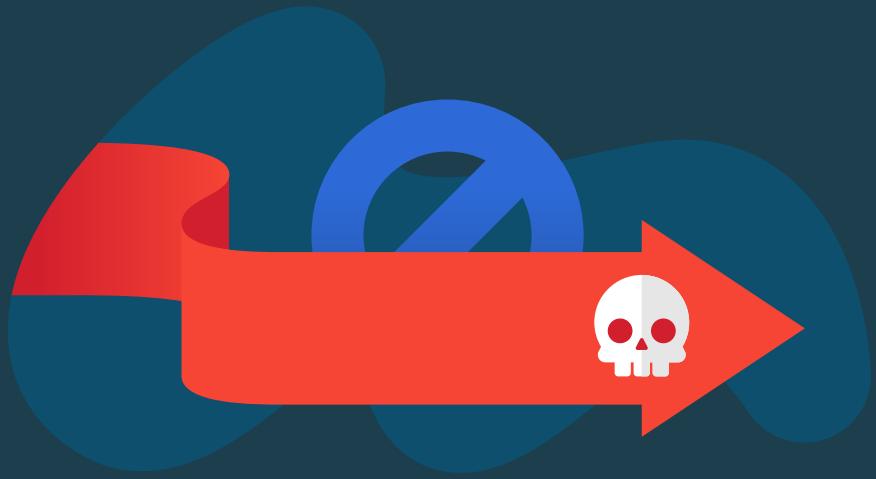
24%
Endpoint detection and response

42%
Legacy signature-based antivirus

12%
NextGen anti-virus

Ransomware is able to get around these solutions because the cybercriminals frequently modify their malware to avoid detection. What's worse, the social engineering tactics criminals use to dupe victims have become very sophisticated and hard to detect—even with security education (more on that below).

That's why a multilayered approach to ransomware that includes business continuity is so important. Security software and training are essential to prevent attacks before they happen. Business continuity enables organizations to resume normal operations quickly if security measures fail.

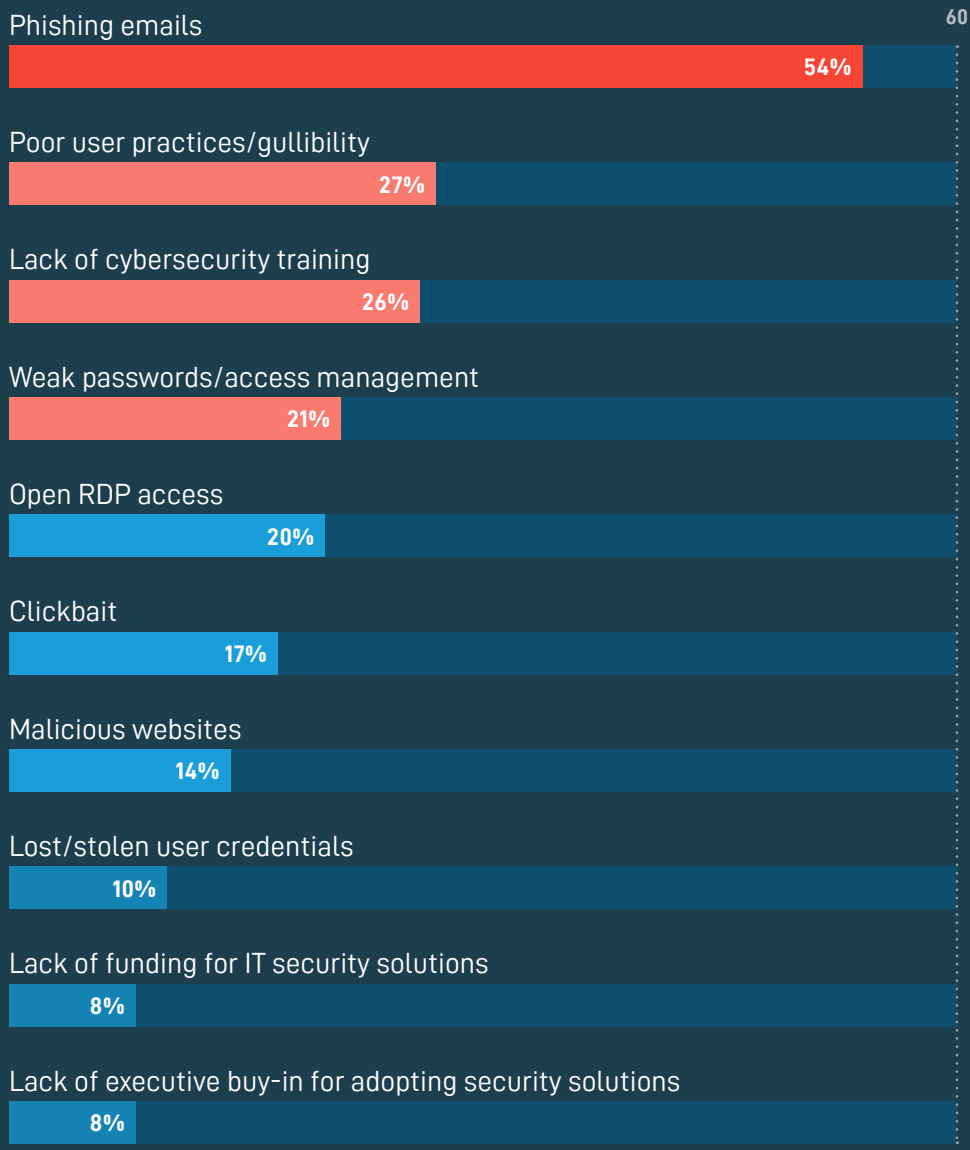


SMBs Keep Taking the Bait

As noted above, end user education is an essential piece of an effective ransomware protection strategy. This year's survey results bear that out: phishing, poor user practices, and lack of end user cybersecurity training were the three most common causes of successful ransomware breaches.

So, it is important to note that security training must go beyond just how to identify phishing attacks. While phishing topped the list, weak passwords, open RDP access, and a host of other user errors were also to blame for breaches.

Leading causes of ransomware attacks reported by MSPs:



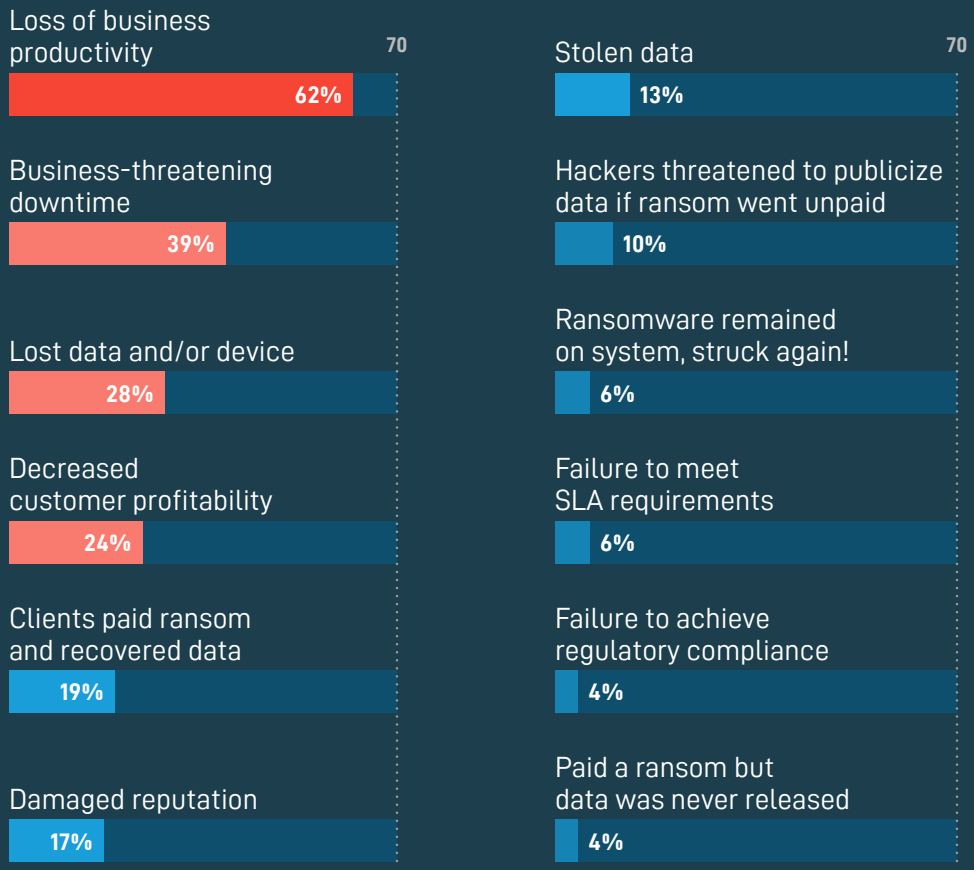
**Survey respondents were asked to select three answer choices.*

The Aftermath of Attacks

Ransomware attacks can result in considerable business downtime, because breaches are rarely limited to a single computer. Most of the ransomware in use today is designed to crawl business networks, looking for additional machines to infect. If the malware goes undetected, it doesn't take long for numerous user devices, servers, and even data in SaaS applications to become encrypted. Restores can be time consuming, especially using traditional backup tools.

So, it makes sense that loss of business productivity and business-threatening downtime were at the top of the list of ransomware results. It also explains why nearly 20% of MSPs reported that SMBs were forced to pay a ransom in order to return to normal business. All of this highlights the need for a business continuity solution that enables SMBs to return to work fast.

Consequences resulting from ransomware attacks reported by MSPs:



**Survey respondents were asked to select three answer choices.*

Downtime Far More Costly than Ransom

When it comes to ransomware attacks, MSPs report **the cost of downtime is nearly 50X greater than the ransom requested**.

Average Ransom in...

2018	2019	2020
$4,300	$5,900	$5,600

MSPs report the average cost of ransom stayed roughly the same in 2020 as it was in 2019. So while there has been a slight decline in the frequency of attacks, hackers are still demanding a high ransom payment. We saw a big uptick in average ransom from 2018 to 2019, when the demands increased by 37%.

Average Cost of Downtime in...

2018	2019	2020
$46,800	$141,000	$274,200

MSPs reported that the average downtime cost per incident has increased by 94% from 2019 and a staggering 486% from 2018. So, what does this mean exactly? Well, on face value it means that downtime costs are higher than reported two years ago, obviously. This may mean that downtime costs have increased, or it could mean that MSPs are getting better at calculating the real costs of downtime. Either way, it's clear that MSPs understand that the damage associated with business downtime is far more costly than the actual ransom.

Downtime costs vary widely among businesses and these numbers are based on MSP estimates. To calculate the cost of potential downtime for your business, check out our Recovery Time and Downtime Cost Calculator.

**All survey respondents answered in U.S. dollars.*

GEO TRENDS

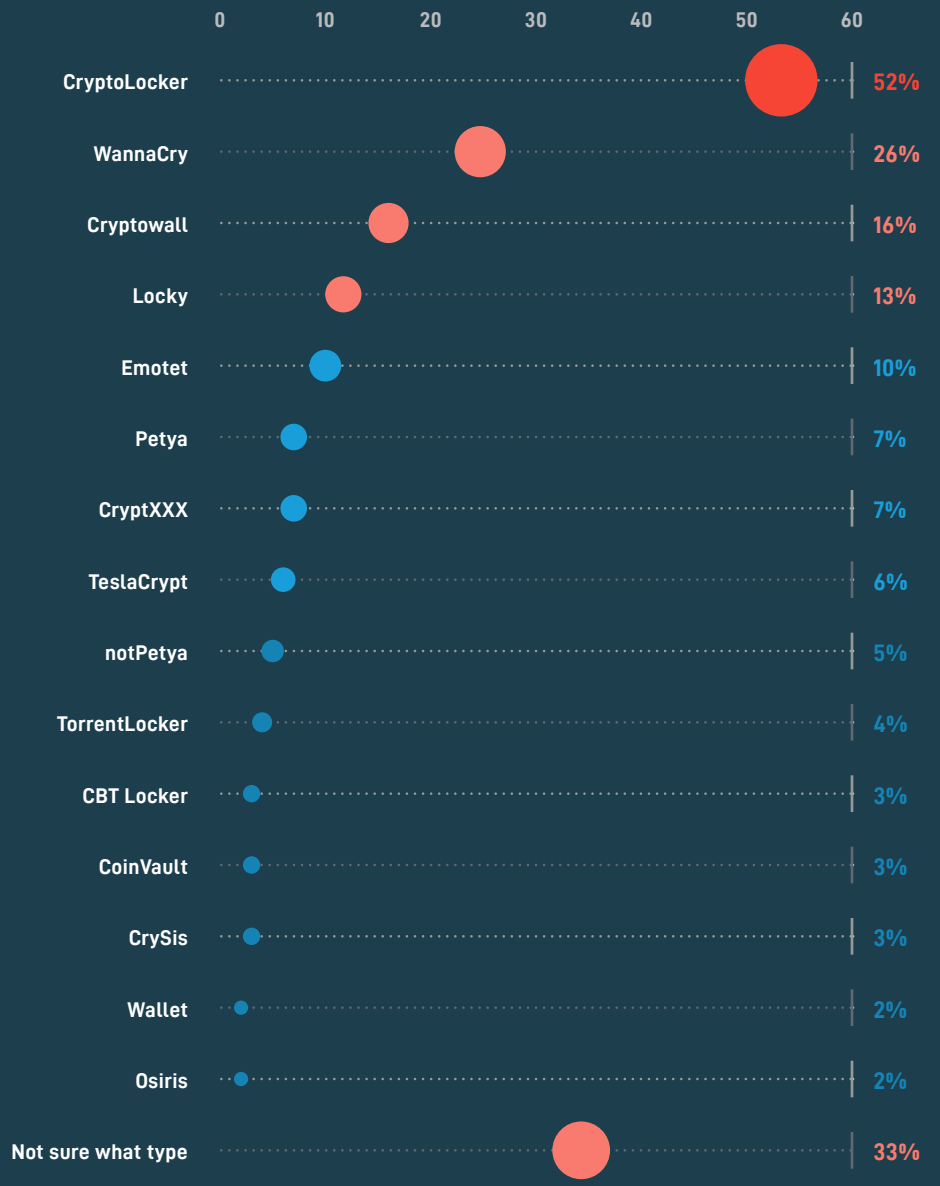
2020: Ransom vs. Downtime Costs

Region	Ransom	Downtime
North America	$6,200	$308,900
Europe	$3,500	$185,800
Asia Pacific	$4,400	$257,000

Still Locking (After All These Years)

For the 5th consecutive year in a row, MSPs reported CryptoLocker as the top ransomware variant impacting their clients (52%). WannaCry was next on the list at 26%, followed by Cryptowall (16%) and Locky (13%).

Interestingly, 33% of respondents said they weren't sure what kind of ransomware they dealt with. This is important to note for two reasons. First, the type of ransomware ultimately doesn't really matter—every type can result in business downtime. Second, the methods MSPs use to combat ransomware and recover following attacks are the same regardless of the strain.



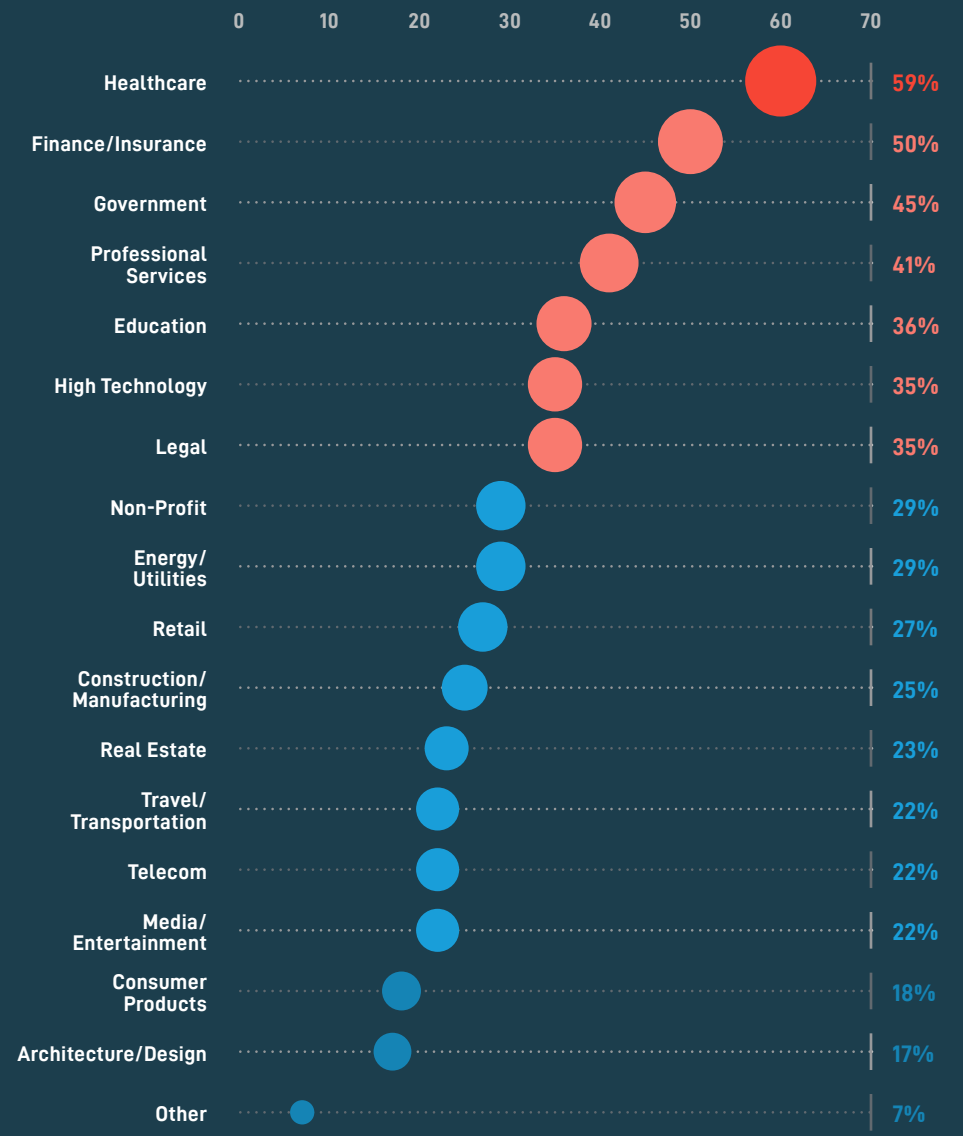
**Survey respondents were able to select multiple answer choices.*

Industries Most Susceptible to Ransomware

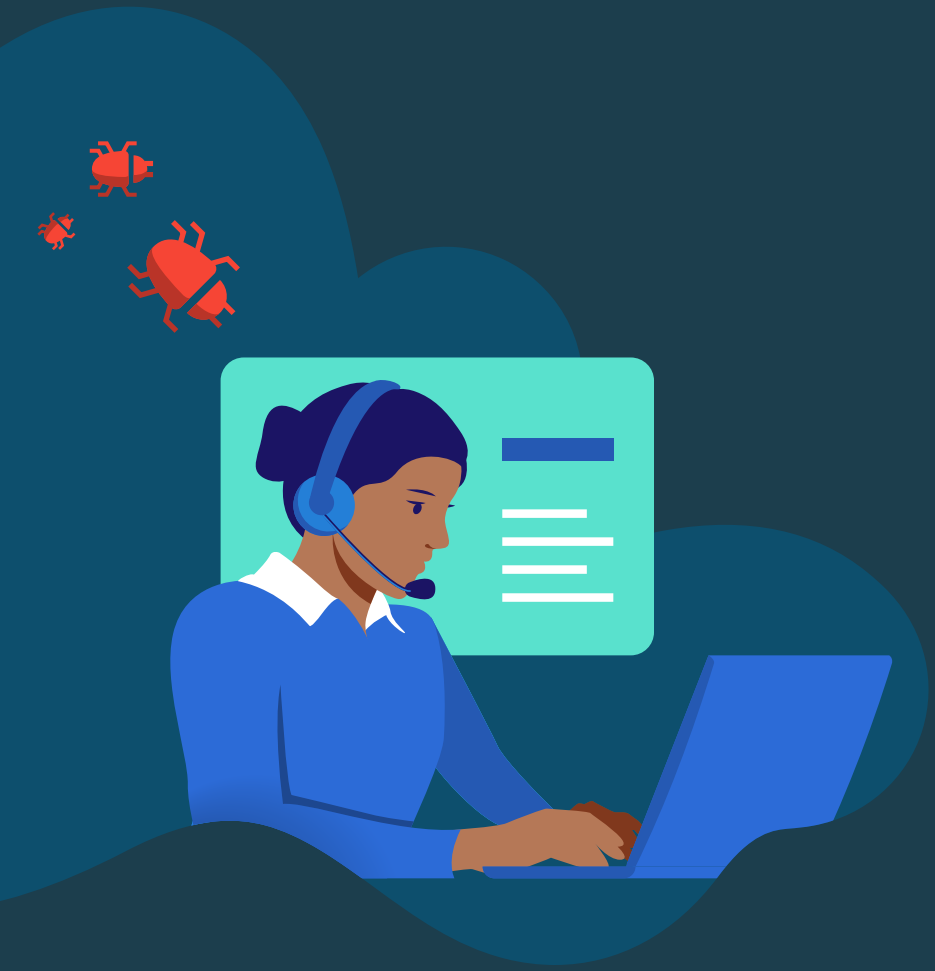
This year we asked MSPs what industries were most susceptible to ransomware attacks due to COVID-19. Perhaps not surprisingly, healthcare was in the top spot. 59% of MSPs said they believed healthcare to be the most vulnerable. Hackers are well known for staging attacks against victims that are already compromised in some way. So, it makes sense that cyber criminals would go after healthcare organizations during a global pandemic.

Finance/insurance was in the second slot (50%) and Government in third (45%). These verticals were also seriously impacted by the pandemic for obvious reasons. Outside of the top three, the rest of the list looks fairly similar to previous years' results.

Industries most susceptible to ransomware due to COVID-19:



**Survey respondents were able to select multiple answer choices.*



Hackers Aren't Only Targeting SMBs...

95% of respondents agreed that MSPs are being increasingly targeted by ransomware attacks. This is likely due to a number of high profile attacks on SMBs in recent memory. In attacks like these, hackers use MSP credentials to access and spread ransomware to their clients. In other words, by compromising an MSP, cybercriminals get more bang for their buck.

MSPs are taking the threat seriously. More than half are now using password management and multi-factor authentication tools, as you will see below.

2FA and SSO Use

44% reported that they are using an identity provider for Single Sign-on (SSO). Microsoft Azure Active Directory was by far the top choice of SSO identity providers among respondents. 47% of MSPs said they use Azure AD for SSO. Of that 44%, nearly 70% use the same provider for two-factor authentication (2FA).

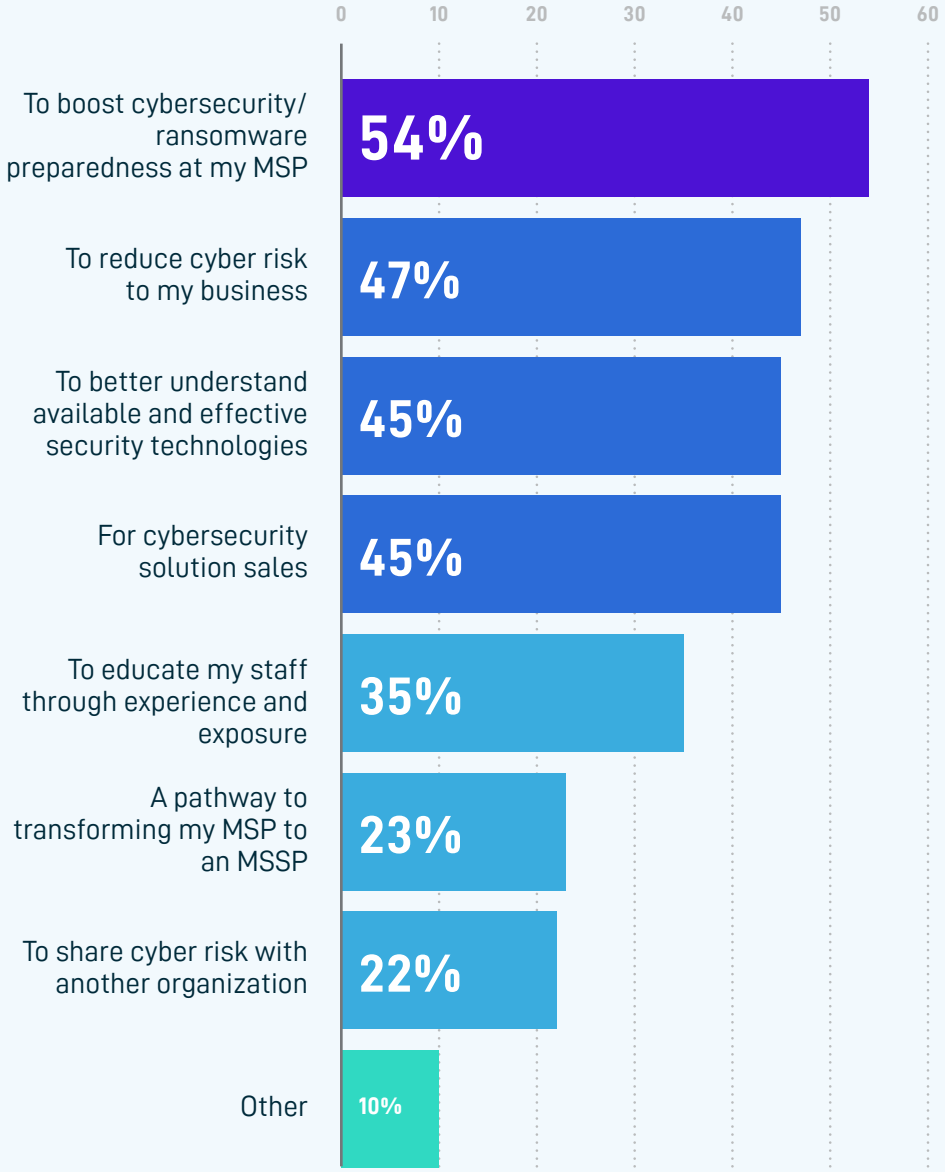
Almost Half of MSPs Partner with MSSPs

46% of MSPs now partner with managed security service providers (MSSPs) for assistance with IT security—for their clients and their own businesses. In fact, the number one reason MSPs reported doing so was to improve their own security preparedness—another sign that MSPs are taking the possibility of attacks on their own businesses seriously.

Ultimately, partnering with an MSSP boils down to accessing expert guidance. IT security is a broad, complex discipline which requires specialization to develop expertise. MSSPs have it, and MSPs need it.

46% of MSPs now partner with MSSPs for assistance with IT security

MSPs that partner with MSSPs cited the following reasons:



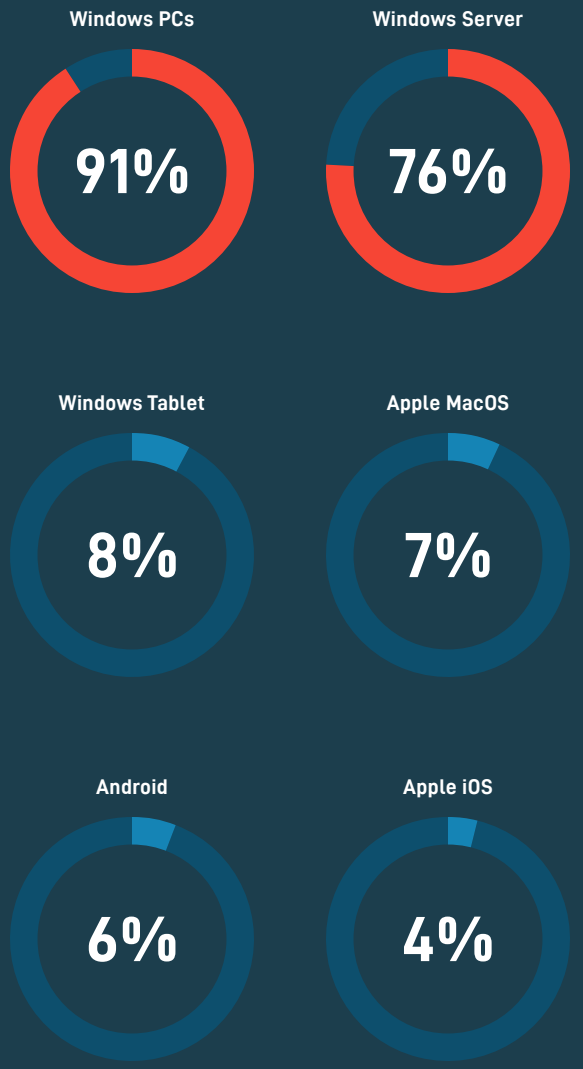
**Survey respondents were able to select multiple answer choices.*

Windows Endpoint Systems Applications Most Targeted by Hackers

91% of ransomware attacks targeted Windows PCs this year, according to MSPs. This tracks with phishing emails being the number one attack vector and the sheer number of Windows PCs in use today. It also highlights the need for endpoint protection and backup solutions. Ransomware attacks on these systems have a significant impact on user productivity, and in turn, a business' ability to generate revenue. Solutions that allow employees to return to work quickly following attacks should be considered essential.

Windows Servers followed at 76%. That's because ransomware may enter a network via a phishing email, but as noted above, it doesn't take long before the malware spreads across networks to infect other systems. A business continuity solution that can recover server workloads locally or in the cloud is critical to minimize business interruption following a ransomware attack.

Endpoint systems most targeted by ransomware attacks:



**Survey respondents were able to select multiple answer choices.*

Ransomware Creeps Into SaaS Apps

Nearly 1 in 4 MSPs reported ransomware attacks on clients' SaaS applications. Of them, Microsoft was hit the hardest. This isn't particularly surprising, since so many organizations rely on Microsoft 365. It was somewhat surprising, however, to see that more than half saw ransomware in Dropbox. Google Workspace rounded out the top three at 25%.

64%
of MSPs report attacks within Microsoft 365

54%
of MSPs report attacks within Dropbox

25%
of MSPs report attacks within Google Workspace

**Survey respondents were able to select multiple answer choices.*

Most Common Ransomware Recovery Methods

Re-imaging a machine from a backup was the number one ransomware recovery method this year. This is a significant change from last year, when re-imaging from default took the top spot. This year that was in the third spot tied with virtualizing the system from a backup image.

76%
Restore a machine from a backup

33%
Re-image from default

27%
Run software to cleanup threat

36%
Restore from files

31%
Virtualize the system from a backup image

15%
Paid ransom

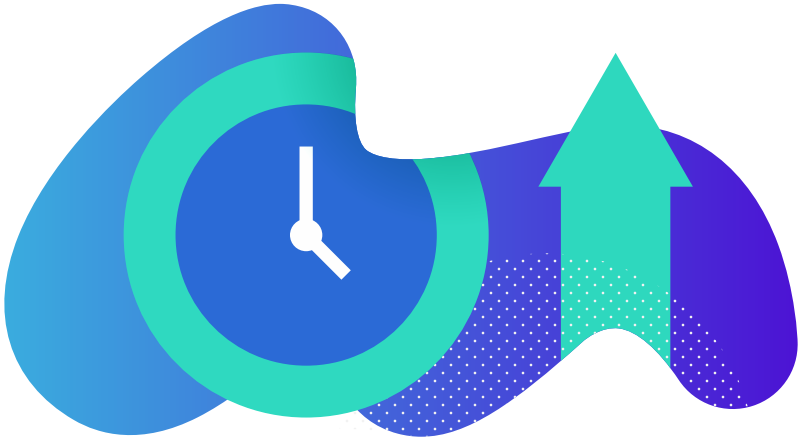
**Survey respondents were able to select multiple answer choices.*

I'm pleased to see that 're-imaging from backup' was the top method MSPs are using to recover from ransomware attacks. This shows MSPs have matured their recovery methods. Two years ago, MSPs were still dealing with the shock of ransomware, scrambling to put something in place for recovery and largely re-imaging machines from scratch. Last year, they were in the process of changing how they do things, putting the right solutions in place with their customers to minimize downtime and data loss. Now, we are starting to see results of those efforts manifest in more mature recovery mechanisms.

Ryan Weeks
Chief Information Security Officer, Datto, Inc.

BCDR Clients Are Less Likely To Experience Significant Downtime

of MSPs said clients with BCDR products in place are less likely to experience significant downtime from ransomware.



Most Effective Solutions to Combat Ransomware

- Business continuity and disaster recovery (BCDR)
- Employee training
- Endpoint detection and response platform
- Patch management
- Unified threat management
- Identity access management solution
- Antivirus / Anti-malware software
- Email / Spam filters
- Endpoint / Mobile management platform
- Browser isolation

We require Datto SIRIS as a minimum for all our clients as one of the security/continuity layers we put in place. To me, it's just as important as cybersecurity insurance. When talking to prospects about BCDR, we discuss ransomware detection and remediation in addition to sharing stories about how quickly we have gotten clients running on local failover. Recently, a local police station we support experienced server failure, and we were able to get them back up and running in just minutes with Datto SIRIS.

Brian J. Weiss
CEO, ITECH Solutions

Final Takeaways

1 **Ransomware awareness seems to be increasing.** Across the board, there were indicators that MSPs and SMBs are taking steps to combat ransomware attacks. And, their efforts are having an impact. While still the most common type of malware attack, ransomware attacks declined slightly from last year. Increased SMB security spending, MSPs partnering with MSSPs, and use of security measures like SSO and 2FA all point to an increase in security awareness.

2 **SMBs need multiple solutions to combat attacks.** Today's standard security solutions alone are no match for today's ransomware, which can penetrate organizations through phishing attacks and avert detection from security solutions. Reducing the risk of infections requires a multi-layered approach rather than a single product.

3 **SMBs must prepare the front line of defense: their employees.** Today's companies must provide regular and mandatory cybersecurity training to ensure all employees are able to spot and avoid potential attacks. While attacks declined slightly this year, phishing attacks remained the most successful attack vector, followed by a number of other employee errors that could be mitigated with better security training.

4 **SMBs need a continuity strategy.** Once again, survey data shows that there is no surefire way of preventing ransomware attacks, even with proper security solutions in place. That's why business continuity was ranked the number one solution to combat attacks again this year. Since ransomware is designed to spread across networks and SaaS applications, endpoint and SaaS backup solutions designed for fast restores are critical.

About the Report

Datto's Global State of the Channel Ransomware Report is comprised of statistics pulled from an online survey of 1,000+ Datto partners that was distributed throughout the month of August 2020.

About Datto

As the world's leading provider of cloud-based software and technology solutions purpose-built for delivery by managed service providers (MSPs), Datto believes there is no limit to what small and medium businesses can achieve with the right technology. Datto offers Unified Continuity, Networking, and Business Management solutions and has created a unique ecosystem of MSP partners. These partners provide Datto solutions to over one million businesses across the globe. Since its founding in 2007, Datto continues to win awards each year for its rapid growth, product excellence, superior technical support, and for fostering an outstanding workplace. With headquarters in Norwalk, Connecticut, Datto has global offices in the United Kingdom, Netherlands, Denmark, Germany, Canada, Australia, China, and Singapore.