# Ransomware Report

Current Ransomware trends and the best practices to mitigate the risks.

datto

cit Complete I.T.

# 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 cyber security 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 that the information compiled here enables MSPs to educate their clients and work with them to mitigate the risk ransomware poses on businesses.

# 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 cyber security 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 inplace 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.

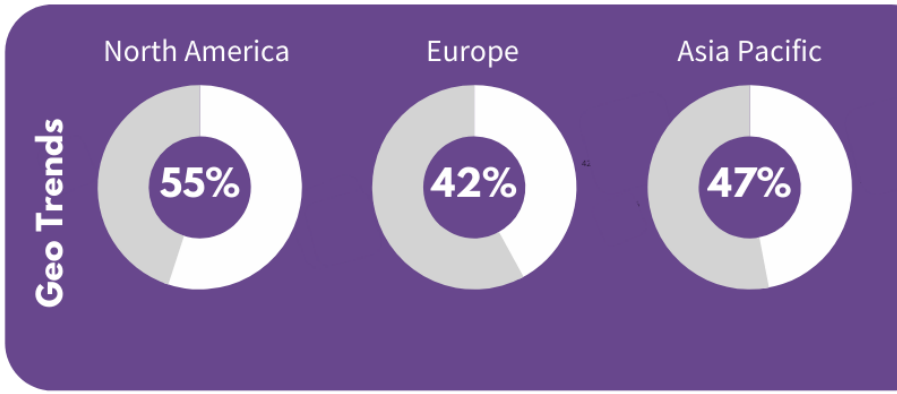
**52%**

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%).



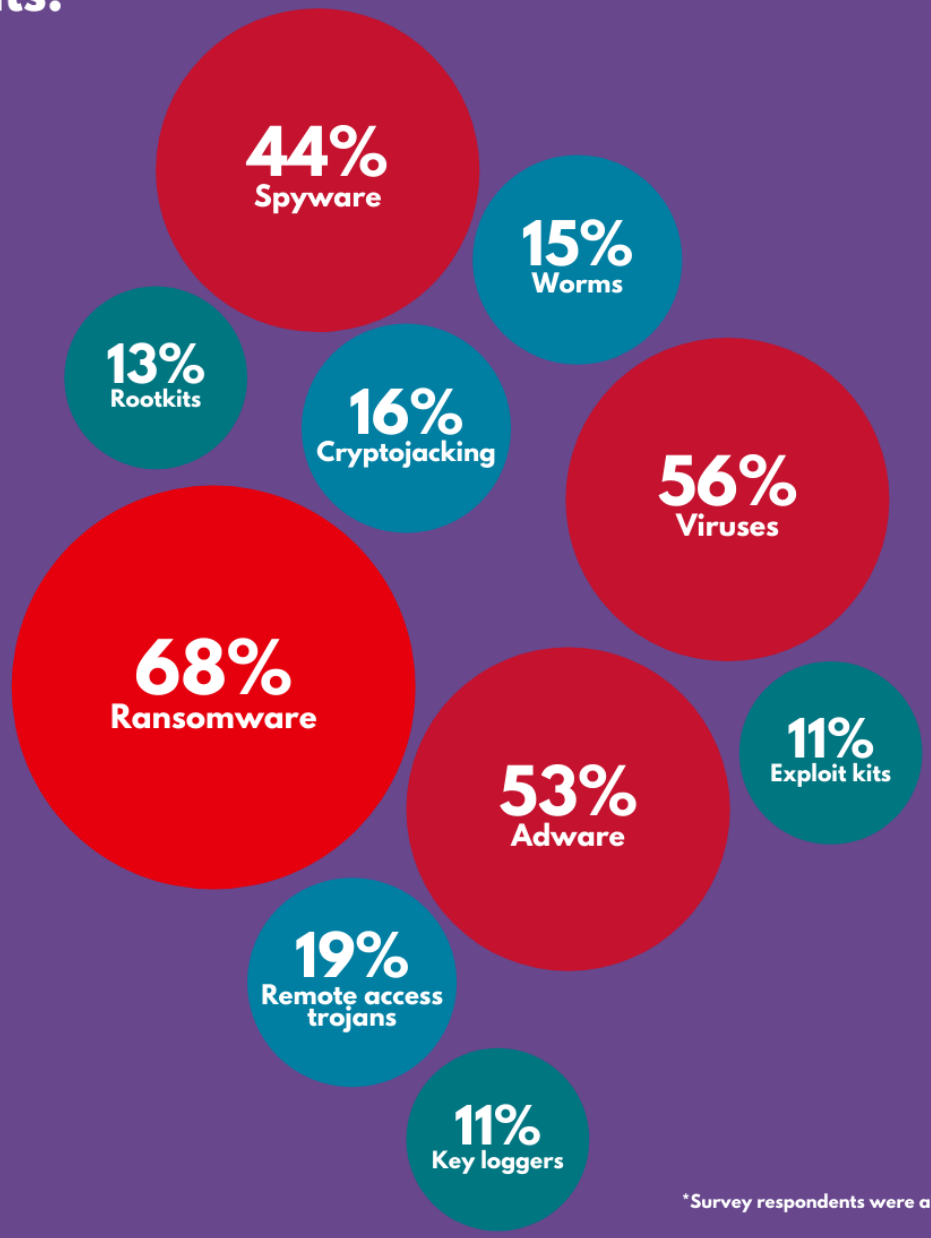

North American MSPs are somewhat more concerned about cloud security than their European and Asia Pacific counterparts.

# 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.

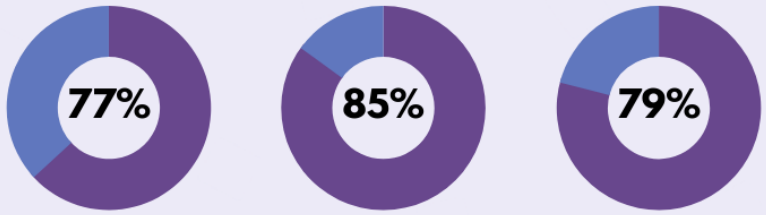
**78%**
of MSPs report attacks against SMBs in the last two years

**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

## Geo Trends




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

# Ransomware Continues to Skirt Cyber Security Efforts

Despite increased security spending, MSPs report that ransomware averted cyber security 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,

**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 organisations 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 cyber security 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:

# 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:

**62%** Loss of business productivity

**39%** Business-threatening downtime

**28%** Lost data and/or device

| | |
|---|---|
| 24% | Decreased customer profitability |
| 19% | Clients paid the ransom and recovered data |
| 17% | Damaged reputation |
| 13% | Stolen data |
| 10% | Hackers threatened to publicise data if ransom went unpaid |
| 6% | Ransomware remained on the system, struck again! |
| 6% | Failure to meet SLA requirements |
| 4% | Failure to achieve regulatory compliance |
| 4% | Paid a ransom but data was never released |

# 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 |
|---|---|---|
| £3,300 | £4,500 | £4,300 |

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 |
|---|---|---|
| £35,500 | £111,400 | £210,000 |

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.

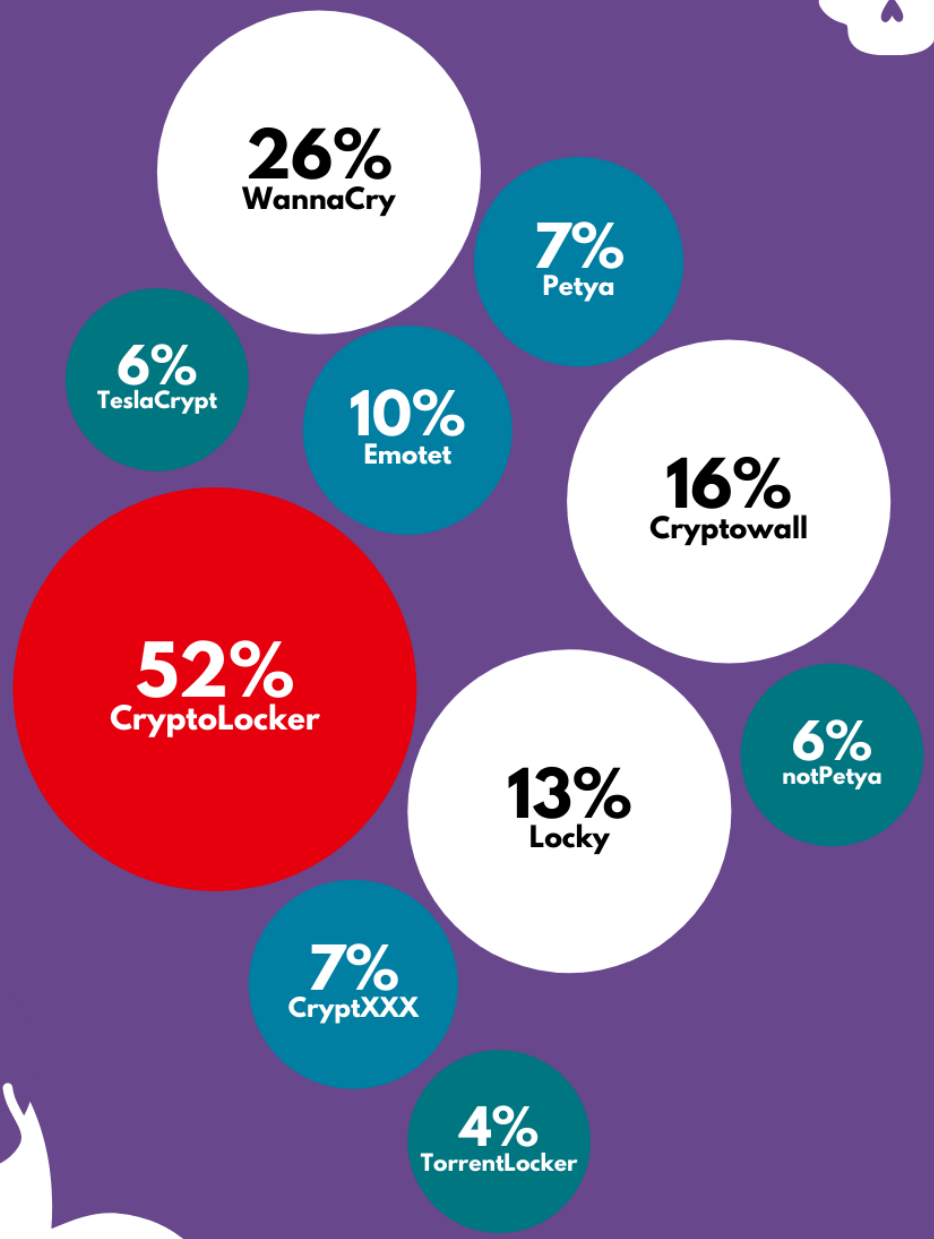
**Geo Trends**

**2020: Ransom vs. Downtime Costs**

| Region | Ransom | Downtime |
|---|---|---|
| North America | £4,700 | £235,000 |
| Europe | £2,700 | £141,000 |
| Asia Pacific | £3,400 | £195,000 |

# 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.



# 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 organisations 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.

**59%** Healthcare

**50%** Finance/Insurance

**45%** Government

| | |
|---|---|
| 41% | Professional Services |
| 36% | Education |
| 35% | High Technology |
| 35% | Legal |
| 29% | Non-Profit |
| 29% | Energy/Utilities |
| 27% | Retail |
| 25% | Construction/Manufacturing |
| 23% | Real Estate |
| 22% | Travel/Transportation |
| 22% | Telecom |
| 22% | Media/Entertainment |
| 18% | Consumer Products |
| 17% | Architecture/Design |
| 7% | Other |

# Most Common Ransomware Recovery Methods

RRe-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 virtualising 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%**
Virtualise the system from a backup image

**15%**
Paid ransom

# BCDR Clients Are Less Likely To Experience Significant Downtime

**91%**

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

complete-it.co.uk

## 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

# Additional Resources

**Knowledge is power**

- How to spot a phishing email
- How to create a strong password
- Why you need 2FA?
- Request a Cyber Security audit
- Visit our Cyber Security Resources page
- Visit our webinars

# About Complete I.T.

CIT provide market leading IT support services, and have done since 1992; it's what we do and it's what we do well.

We have the highest levels of technical expertise and accreditations to resolve your issues, but we also have a genuine passion for understanding your organisation, its goals and challenges. We don't just fix your problems, we find ways to improve your systems and positively impact your team and business.

Whether you have no in-house IT expertise, or you are an IT Manager looking for additional help, we will build a service that meets your specific needs and priorities. We provide you with the advice and guidance that you need to take advantage of ever evolving technology, and help you to plan your IT Roadmap for the future.

# About the Report

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. To learn more about the report, please reach out to Katie Thornton, Director of Content & Marketing Programs at Datto, Inc.

info@complete-it.co.uk

www.complete-it.co.uk

datto

cit Complete I.T.