

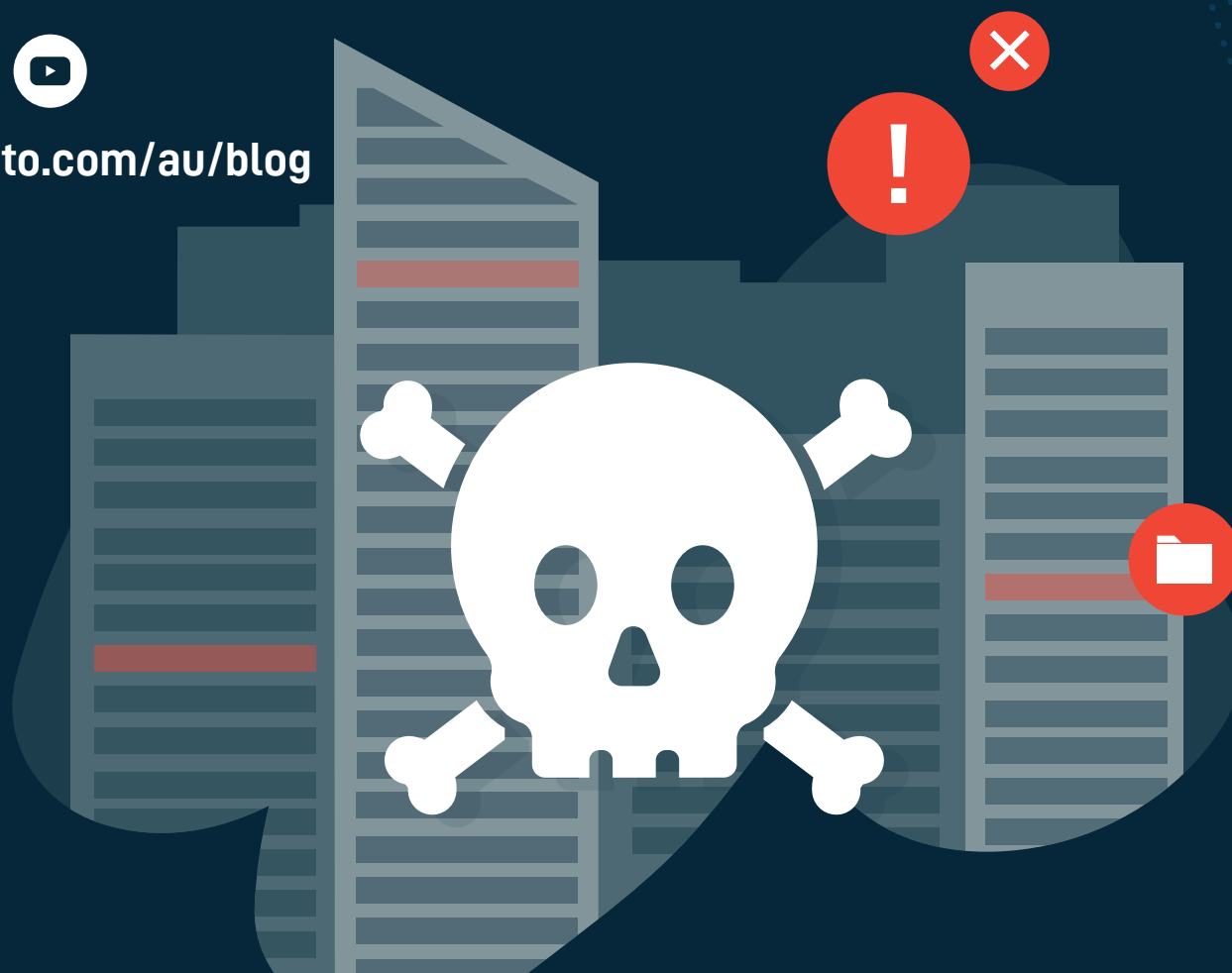
Report

datto

# Datto's ANZ State of the Channel **Ransomware Report**

Follow us on:     

Subscribe to our blog: [www.datto.com/au/blog](http://www.datto.com/au/blog)



## About the Report

Datto's ANZ State of the Channel Ransomware Report is comprised of statistics pulled from a survey of nearly 200 managed service providers (MSPs), our partners, and clients, across Australia and New Zealand. The report provides unique visibility into the state of ransomware from the perspective of the IT Channel and their SMB clients who are dealing with these infections on a daily basis. The report offers 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 the growing threat.

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

## About Datto

As the world's leading provider of IT solutions delivered 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 business continuity and disaster recovery, networking, business management, and file backup and sync solutions, and has created a one-of-a-kind ecosystem of partners that provide Datto solutions to half a million businesses across more than 130 countries. Since its founding in 2007, Datto has earned hundreds of awards for its rapid growth, product excellence, superior technical support, and for fostering an outstanding workplace. With global headquarters in Norwalk, Connecticut, Datto has international offices in the United Kingdom, Netherlands, Denmark, Germany, Canada, Australia, China, and Singapore. Learn more at [datto.com](https://datto.com).

# Key Findings

- **Ransomware remains the most prominent malware threat.** In 2019, 89% of MSPs report ransomware as the most common malware threat to SMBs.
- **In the first half of 2019 alone, 64% of MSPs report attacks against clients.** 5% of MSPs report multiple ransomware attacks in a single day.
- **On average, 2 in 5 SMBs report that they've fallen victim to a ransomware attack.** In particular, SMBs who don't outsource their IT services are more at risk.\*
- **When it comes to the ransomware threat, there is a disconnect between MSPs and SMBs.** 90% of MSPs are "very concerned" about the ransomware threat and 24% report their SMB clients feel the same.
- **MSPs rank phishing emails as the leading cause of successful attacks.** Lack of cyber security education, weak passwords, and poor user practices are among the other top causes.
- **The aftermath of a ransomware attack can be a nightmare for any business.** Nearly half of MSPs report victimised clients experienced business-threatening downtime.
- **The average ransom requested by hackers is increasing.** MSPs report the average requested ransom for SMBs is ~\$4,300 AUD.
- **Downtime costs up by 75% year-over-year,** and the cost of downtime is 24 times greater than the average ransom requested in 2019.
- **94% of MSPs report that clients with BCDR solutions in place are less likely to experience significant downtime during a ransomware attack.** 3 in 4 MSPs also report that victimised clients with BCDR in place recovered from the attack in 24 hours, or less.
- **SMBs aren't the only businesses being targeted by hackers.** 3 in 4 MSPs agree that their own businesses are being increasingly targeted by ransomware attacks.



*\*Strategy Analytics' proprietary research of the Australia and New Zealand SMB market.*

## A Variety of Malware Targeting SMBs

Which of the following malware attacks have affected your clients in the last 2 years?



**43%** of MSPs  
report SMBs  
struck by **viruses**



**33%** of MSPs  
report SMBs  
struck by **adware**



**30%** of MSPs  
report SMBs  
struck by **cryptojacking**



**29%** of MSPs  
report SMBs  
struck by **spyware**



**28%** of MSPs  
report SMBs  
struck by **remote access trojans**



**11%** of MSPs report SMBs struck by keyloggers

**9%** of MSPs report SMBs struck by exploit kits

**7%** of MSPs report SMBs struck by rootkits

**7%** of MSPs report SMBs struck by worms

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

Among the malware threats impacting SMBs, ransomware is the biggest offender.



**89%** of MSPs report **attacks against SMBs** in the last two years



In the first half of 2019 alone, **64%** of MSPs report **attacks against clients**



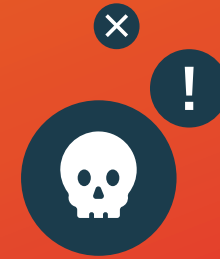
**5%** of MSPs report **multiple ransomware attacks** in a single day



### Geo Trend:

In **Australia and New Zealand**, **89%** of MSPs report **attacks against SMBs** in the last two years, the highest rate globally.

**2 in 5 SMBs**  
report that they've  
**fallen victim to a  
ransomware attack.\***



On average, SMBs who don't outsource their IT services report facing more ransomware attacks.\*



*\*Source: Strategy Analytics' proprietary research of the Australia and New Zealand SMB market.*

In 2019

**24%**

of MSPs report  
**SMBs are 'very  
concerned'** about  
ransomware

There is a  
**disconnect between  
SMBs and MSPs** on the  
significance of the  
ransomware threat.

**90%**

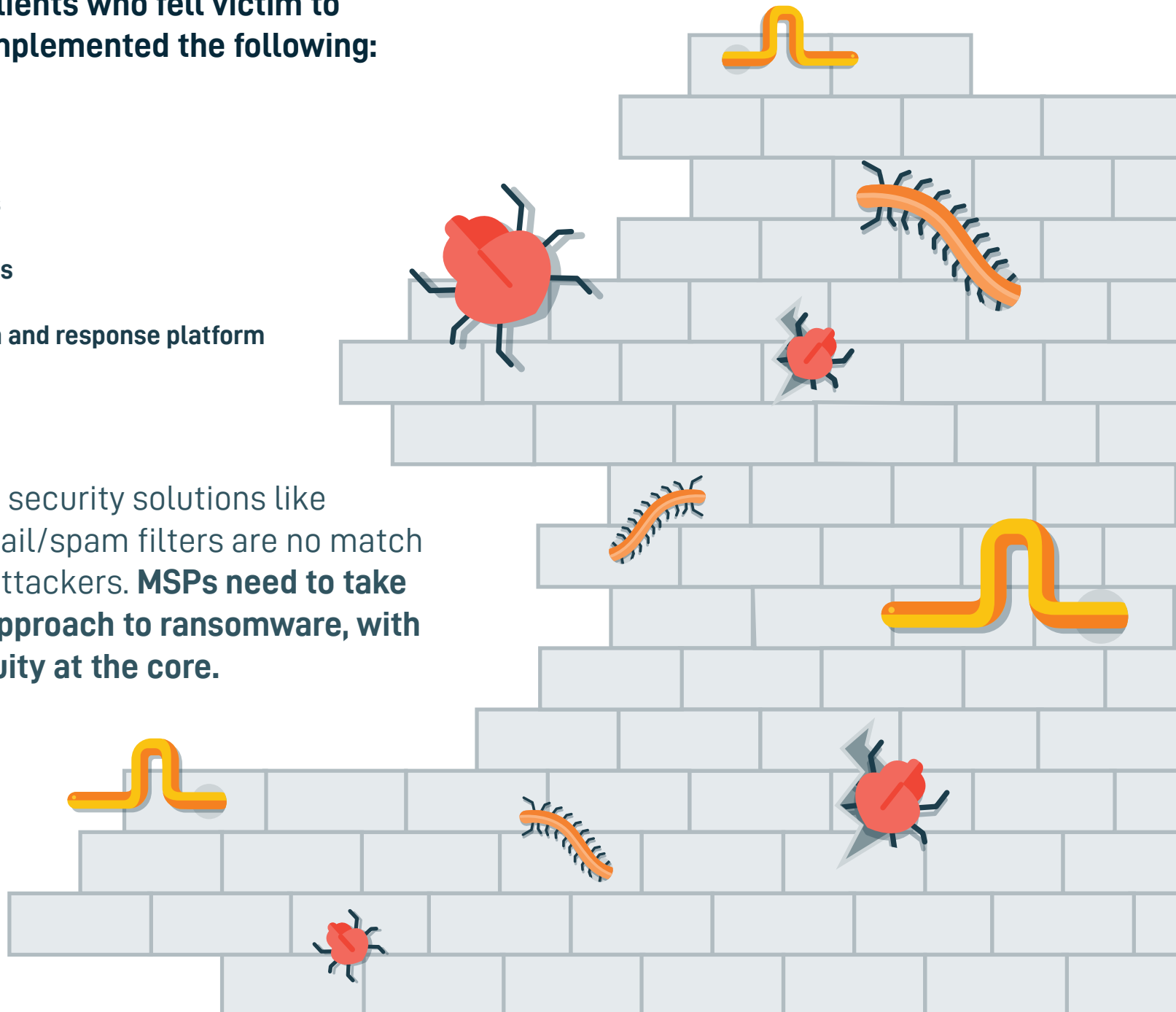
of MSPs report  
**SMBs should be 'very  
concerned'** about the threat

# Ransomware Continues to Creep Past Cyber Security Solutions

MSPs report that clients who fell victim to ransomware had implemented the following:

- Antivirus software
- Email/spam filters
- Ad/pop-up blockers
- Endpoint detection and response platform

Traditional cyber security solutions like antivirus and email/spam filters are no match for many cyber attackers. **MSPs need to take a multilayered approach to ransomware, with business continuity at the core.**





Which of the following are the leading causes of ransomware?

**73%** of MSPs report  
**phishing emails**

**39%** of MSPs report  
**weak passwords/access management**

**33%** of MSPs report  
**lack of cyber security training**

**30%** of MSPs report poor user practices/gullibility

**13%** of MSPs report clickbait

**10%** of MSPs report malicious websites/web ads



Phishing, lack of end user cyber security training, and weak passwords are the three most common causes of successful ransomware breaches.

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

Which of the following consequences resulted from a ransomware attack?

**81%** of MSPs report

loss of business productivity

**34%** of MSPs report

decreased customer profitability

**47%** of MSPs report

business-threatening downtime

**27%** of MSPs report

infection spread to other devices on the network

**34%** of MSPs report

lost data and/or device

**21%** of MSPs report

damaged reputations



Calculate the cost of  
potential downtime with the  
Recovery Time and Downtime  
Cost Calculator

**CALCULATE**

- 18% of MSPs report clients paid a ransom and recovered the data
- 12% of MSPs report stolen data
- 7% of MSPs report ransomware remained on system and struck again!
- 7% of MSPs report failure to achieve regulatory compliance
- 6% of MSPs report failure to meet SLA requirements
- 5% of MSPs report clients paid ransom but data was never released

### Geo Trend:

81% of ANZ MSPs report loss of business productivity, soaring beyond the global average of 64%.

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



When it comes to ransomware attacks, MSPs report the **cost of downtime** is **24X** greater than the ransom requested

### Average Ransom

2019  
**\$5,900**

### Average Cost of Downtime

2018 **\$58,000** ↗ 2019 **\$100,000**

The average **downtime cost per incident** has soared **over 75%** from previous year

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

Which of the following strains of ransomware have affected your clients?

**55%** of MSPs report  
**CryptoLocker**

00:00:35

For the 4th consecutive year, **MSPs report CryptoLocker as the top ransomware variant** attacking clients.



**43%** of MSPs report  
**WannaCry**



**21%** of MSPs report  
**Petya**



**19%** of MSPs report  
**CryptoWall**

16% of MSPs report Locky

13% of MSPs report notPetya

9% of MSPs report CryptXXX

7% of MSPs report CrySis

6% of MSPs report TeslaCrypt

6% of MSPs report CBT Locker

6% of MSPs report Wallet (**NEW**)

5% of MSPs report TorrentLocker

4% of MSPs report Bad Rabbit

4% of MSPs report CoinVault

3% of MSPs report Emotet (**NEW**)

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

**39%** of MSPs  
report

### Professional Services most targeted by ransomware



The Professional Services sector has been an ongoing phisher's favourite. It's not surprising that this industry continues to be targeted by ransomware. Businesses in this industry typically have a high reliance on cloud applications, productivity suites, and email. In our experience, it's still employees that are the weak link in the chain. Unfortunately, it only takes one well-constructed phishing email and a link or attachment to unleash ransomware on the network.

**Adam Nightingale**, Managing Director, Lucid IT

<b>30%</b> Construction/Manufacturing	<b>10%</b> Other/None
<b>26%</b> Finance/Insurance	<b>9%</b> Architecture/Design
<b>22%</b> Real Estate	<b>9%</b> Government
<b>21%</b> Non-Profit	<b>5%</b> Travel/Transportation
<b>20%</b> Healthcare	<b>4%</b> Media/Entertainment
<b>19%</b> Legal	<b>2%</b> Energy/Utilities
<b>16%</b> Retail	<b>2%</b> Telecom
<b>10%</b> Education	<b>1%</b> High Technology
<b>10%</b> Consumer Products	

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





**92%** of MSPs report  
**ransomware infecting  
endpoint systems**

Of the 92%...



**91%** of MSPs report  
attacks on  
**Windows PC**

**14%** of MSPs report attacks on Windows Tablet

**6%** of MSPs report attacks on MacOS X

**4%** of MSPs report attacks on Android

**4%** of MSPs report attacks on iOS

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

## Ransomware Descends Over Office 365

**37%** of MSPs report ransomware attacks in SaaS applications, the highest rate globally.

Of the 37%:

**22%** of MSPs report attacks within



**Office 365**

(up from 49% in 2018)

**21%** of MSPs report attacks within  
 **Dropbox**

**5%** of MSPs report attacks within  
 **G Suite**

The majority of SMBs report 30% of their IT infrastructure is based in the cloud. In the next three years, more expect they'll use the cloud for a larger percentage of their infrastructure.



### Geo Trend:

In **Australia and New Zealand**, **37%** of MSPs report attacks on SaaS applications, the **highest rate globally**.

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

*\*\*Source: Strategy Analytics' proprietary research of the North American SMB market.*

## Most Common Ransomware Recovery Methods

Which methods have you used to recover a client from a ransomware infection?

**66%** of MSPs report  
reimaging a machine



**47%** of MSPs report  
virtualising the system  
from a backup image



**34%** of MSPs report  
running software  
to cleanup threat

**13%** of MSPs report relying on end-point antivirus to recover

**12%** of MSPs report downloading a purpose-built software tool designed for ransomware recovery

**12%** of MSPs report finding a decryption key

How Rapid Rollback Helps MSPs  
Recover Clients from Ransomware

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





It can be difficult to identify the source of a ransomware threat or how long that threat has been latent in a given environment. Because of that, we suspect MSPs are using a variety of methods to recover clients on a case-by-case basis. Today's MSPs need robust recovery plans that address the tactics of the different threats their clients are facing. They can achieve this by selecting vendors who offer multiple recovery options that can be customised based on the incident at hand. They should also develop a plan to assure the safe operating state of a backup where threats may have lain dormant for a period of time.

**Ryan Weeks, Chief Information Security Officer, Datto, Inc.**



### Business Continuity and Disaster Recovery (BCDR)

- ★ Employee training
- ★ Patch management
- ★ Unified threat management
- ★ Identity access management solution
- ★ Antivirus / Anti-malware software
- ★ Email / Spam filters
- ★ Endpoint / Mobile management platform
- ★ Browser isolation
- ★ Endpoint detection and response platform (NEW!)



Traditional antivirus solutions are only effective for detecting threats that have been seen before, and ransomware is good at evading these detection engines. Endpoint detection and response software looks at how processes interact with an operating system, and call out or prevent activities that look and behave like malware.

**David Thomas**, Group Managing Director, Bluegrass Group Ltd

## With BCDR, Ransomware Recovery 4X More Likely Than Without



**94%** of MSPs report

that clients with BCDR products in place are **less likely to experience significant downtime** from ransomware

**With BCDR,**



**3 in 4 MSPs** report clients **fully recovered** in 24 hours, or fewer

**Without BCDR,**



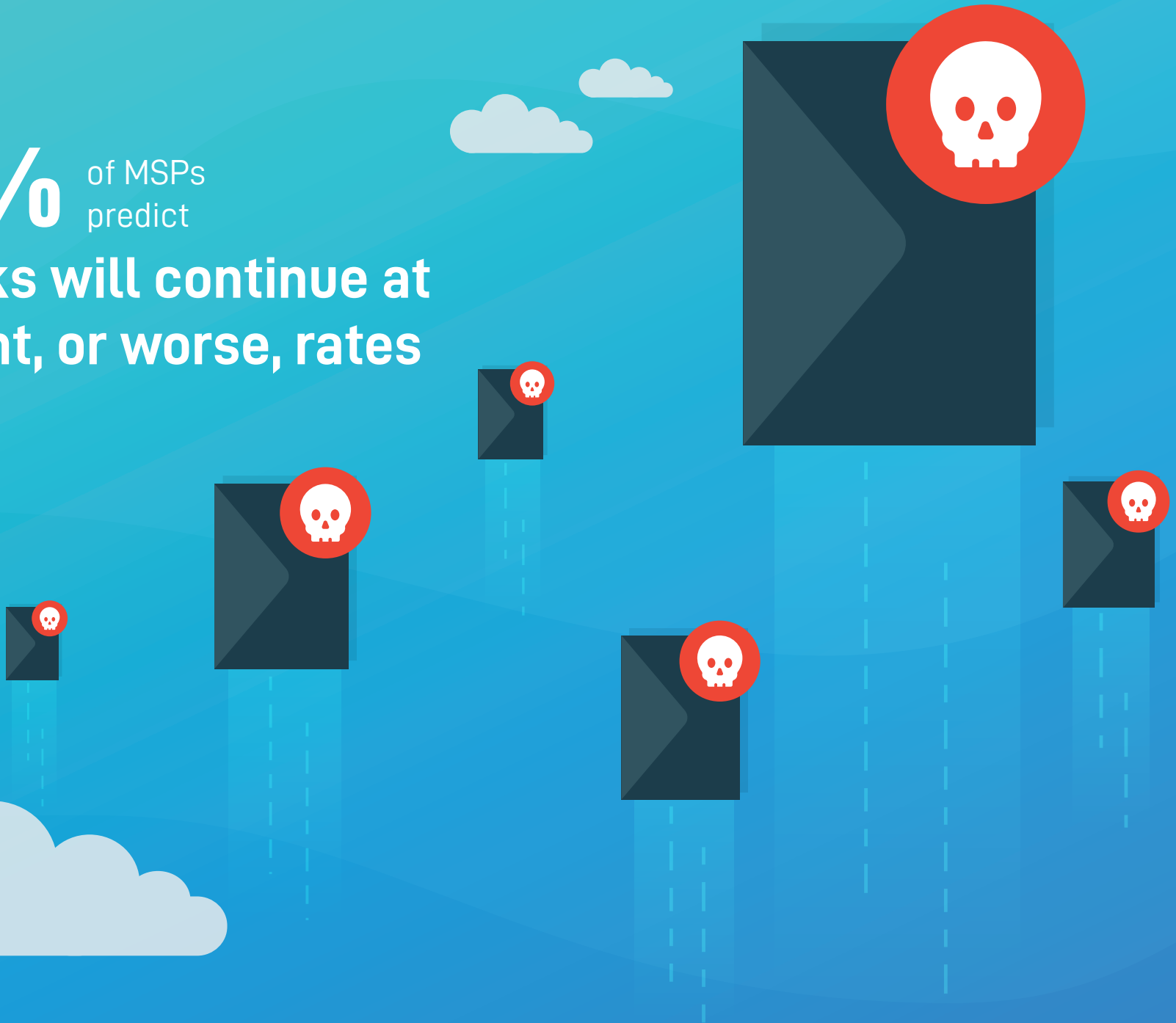
**less than 1 in 5 MSPs** report clients were able to do the same

Check out a demo  
of Datto BCDR

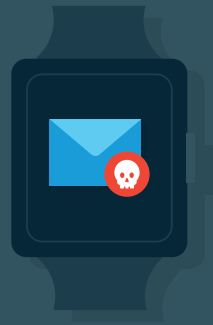


[Learn More](#)

**96%** of MSPs  
predict  
**attacks will continue at  
current, or worse, rates**



# IoT Tops the List of Future Ransomware Attack Targets



**68%** of MSPs predict ransomware will **target IoT devices**

## Why IoT?

Many of these devices aren't designed with security in mind, and cyber attackers will find ways to exploit this vulnerability. There are projected to be over 20 billion IoT devices in use by 2020, offering hackers more entry points into networks.

**Dale Shulmistra**, CEO, Invenio IT



**62%** of MSPs predict ransomware will **target social media accounts**



**52%** of MSPs predict ransomware will **target users based on demographics**



**62%** of MSPs predict ransomware will **bankrupt whole companies**



**49%** of MSPs predict ransomware will **capture critical utility infrastructures (e.g., power grids)**



# 3 in 4 agree

that MSP businesses are being **increasingly targeted by ransomware** attacks

But the best offence is a good defence:



**52%** of MSPs report carrying **cyber liability insurance** should they or their clients become subject to a ransomware attack



**38%** of MSPs report having **external expertise lined up** to help them in the event of a large scale attack against them or their clients



In The News: **Major Technology Companies Targeted by Ransomware Attacks**



MSPs considering purchasing cyber liability insurance should **start by checking with their existing insurance carrier** that provides their errors and omissions coverage to see what is offered.



During this period of extreme turbulence, MSPs need to buckle up and put on their oxygen masks. They need to protect themselves in order to keep their customers safe. MSPs must adopt two-factor authentication universally for any technology they use to service clients as well as their own business. In a climate where cyber attacks have become an everyday occurrence, **2FA across all technology solutions is one of the most effective controls to reduce the likelihood of a successful attack.**

**Ryan Weeks**, Chief Information Security Officer, Datto, Inc.

MSPs report enabling two-factor authentication (2FA) on the following tools and applications:

# 61% Password Managers



**60%**  
Email Client



**44%**  
IT Documentation



**57%**  
Remote Monitoring  
and Management  
(RMM)



**40%**  
BCDR



**50%**  
Professional Services  
Automation (PSA)



In The News: [New Cyber security Threat Highlights the Need for MFA](#)

Datto RMM Demo



[Learn More](#)



## Final Takeaways:



Businesses must prepare the front line of defence: your employees. Today's companies must provide regular and mandatory cyber security training to ensure all employees can spot and avoid a potential phishing scam in their inbox, a leading entrance point for ransomware.



Businesses must leverage multiple solutions to prepare for the worst. Standard security solutions are no match for ransomware which can penetrate organisations in multiple ways. Reducing the risk of infections requires a multilayered approach rather than a single product.



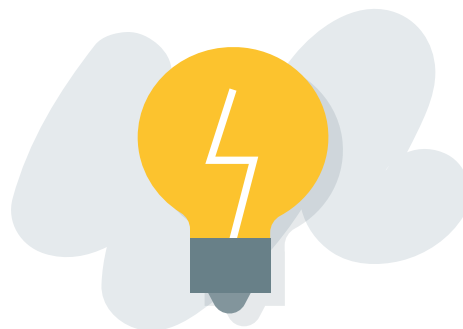
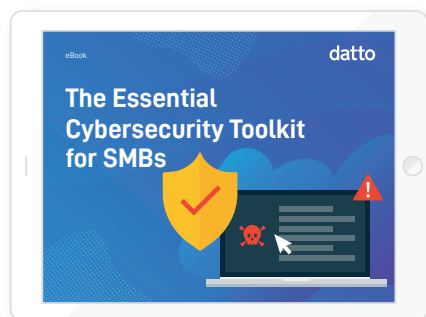
Businesses need a continuity strategy. There is no sure-fire way of preventing ransomware. However, antivirus, perimeter protection, and patch management are essential. Businesses should focus on how to maintain operations despite a ransomware attack. A solid, fast, and reliable business continuity and disaster recovery solution is one part of that strategy. Since ransomware is designed to spread across networks and SaaS applications, endpoint and SaaS backup solutions designed for fast restores are also critical.



Businesses need a dedicated cyber security professional to ensure business continuity. SMBs often rely on a "computer savvy" staff member to handle their IT support and not an IT expert. If a company cannot afford a complete IT staff for 24/7 cyber security monitoring, they should be leveraging an MSP who has the time and resources to anticipate and protect a company from the latest cyber security threats.

## Additional Resources:

### You Also Might be Interested in:



### Knowledge is Power: Ransomware Education for Employees:

- ➔ What is Ransomware?
- ➔ Common Types of Ransomware
- ➔ 5 Types of Social Engineering Attacks

### Ransomware Survivor Stories:

- ➔ Datto and Interplay Save Client from Ransomware
- ➔ masterIT Keeps Flight Training Company Soaring During Ransomware Attack
- ➔ Cole Informatics Saves Vick Insurance from Ransomware Disaster

### For a Multi-Layered Ransomware Approach:

- ➔ Request a Datto BCDR Demo
- ➔ Request a Datto SaaS Protection Demo
- ➔ Request a Datto RMM Demo



- ➔ Subscribe to the Datto Blog
- ➔ Visit the Datto Website

### Already a Datto partner?

[Check out MarketNow](#)  
for the complete  
end-user campaign  
on ransomware.

