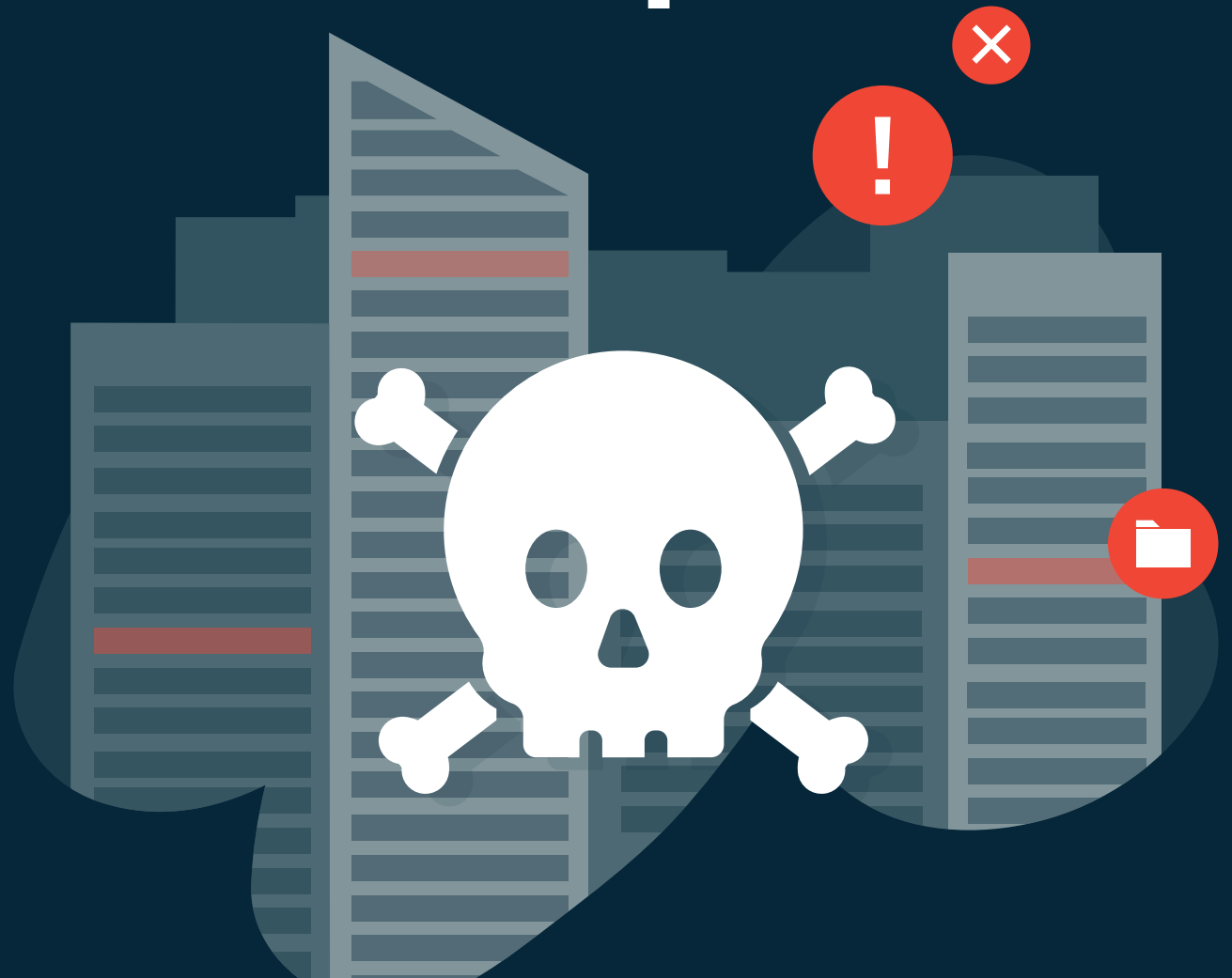# Datto's Global
Ransomware Report

About the Report

Datto's Global State of the Channel Ransomware Report is comprised of statistics pulled from a survey of **1,400+** managed service providers (MSPs), our partners, and clients, around the world. 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 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 the growing threat.

Key Findings

- **Ransomware remains the most prominent malware threat.** In 2019, 85% of MSPs report ransomware as the most common malware threat to SMBs.

- **In the first half of 2019 alone, 56% of MSPs report attacks against clients.** 15% of MSPs report multiple ransomware attacks in a single day.

- **On average, 1 in 5 SMBs report that they've fallen victim to a ransomware attack.** 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.** 89% of MSPs are "very concerned" about the ransomware threat and 28% report their SMB clients feel the same.

- **MSPs rank phishing emails as the leading cause of successful attacks.** Lack of cybersecurity training, 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 victimized clients experienced business-threatening downtime.

- **The average ransom requested by hackers is increasing.** MSPs report the average requested ransom for SMBs is ~$5,900, up 37%, year-over-year.

- **Downtime costs are up by 200% year-over-year,** and the cost of downtime is 23X greater than the average ransom requested in 2019.

- **92% of MSPs report that clients with BCDR solutions in place are less likely to experience significant downtime during a ransomware attack.** 4 in 5 MSPs report that victimized clients with BCDR in place recovered from the attack in 24 hours, or less.

- **SMBs aren't the only businesses being targeted by hackers.** 4 in 5 MSPs agree that their own businesses are being increasingly targeted by ransomware attacks.

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

A Variety of Malware Targeting SMBs

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

61% of MSPs report SMBs **struck by viruses**

54% of MSPs report SMBs **struck by adware**

46% of MSPs report SMBs **struck by spyware**

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

26% of MSPs report SMBs **struck by remote access trojans**

20% of MSPs report SMBs struck by rootkits
18% of MSPs report SMBs struck by worms
14% of MSPs report SMBs struck by keyloggers
13% of MSPs report SMBs struck by exploit kits

Survey respondents were able to select multiple answer choices.

Ransomware is #1 Malware Threat to SMBs

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

RANSOMWARE
8 5 2 0 1 9

85% of MSPs report **attacks against SMBs** in the last two years

In the first half of 2019 alone, **56%** of MSPs report **attacks against clients**

15% of MSPs report **multiple ransomware attacks** in a single day

Geo Trend:

In **Australia and New Zealand**, **91%** of MSPs report **attacks against SMBs** in the last two years, the highest rate globally.

1 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.*

89%

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

In 2019

28%

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

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

# Ransomware Continues to Creep Past Cybersecurity Solutions

MSPs report clients fell victim to ransomware despite having implemented the following:

- **Antivirus software**

- **Email/spam filters**

- **Ad/pop-up blockers**

- **Endpoint detection and response platform**

Traditional cybersecurity 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.**
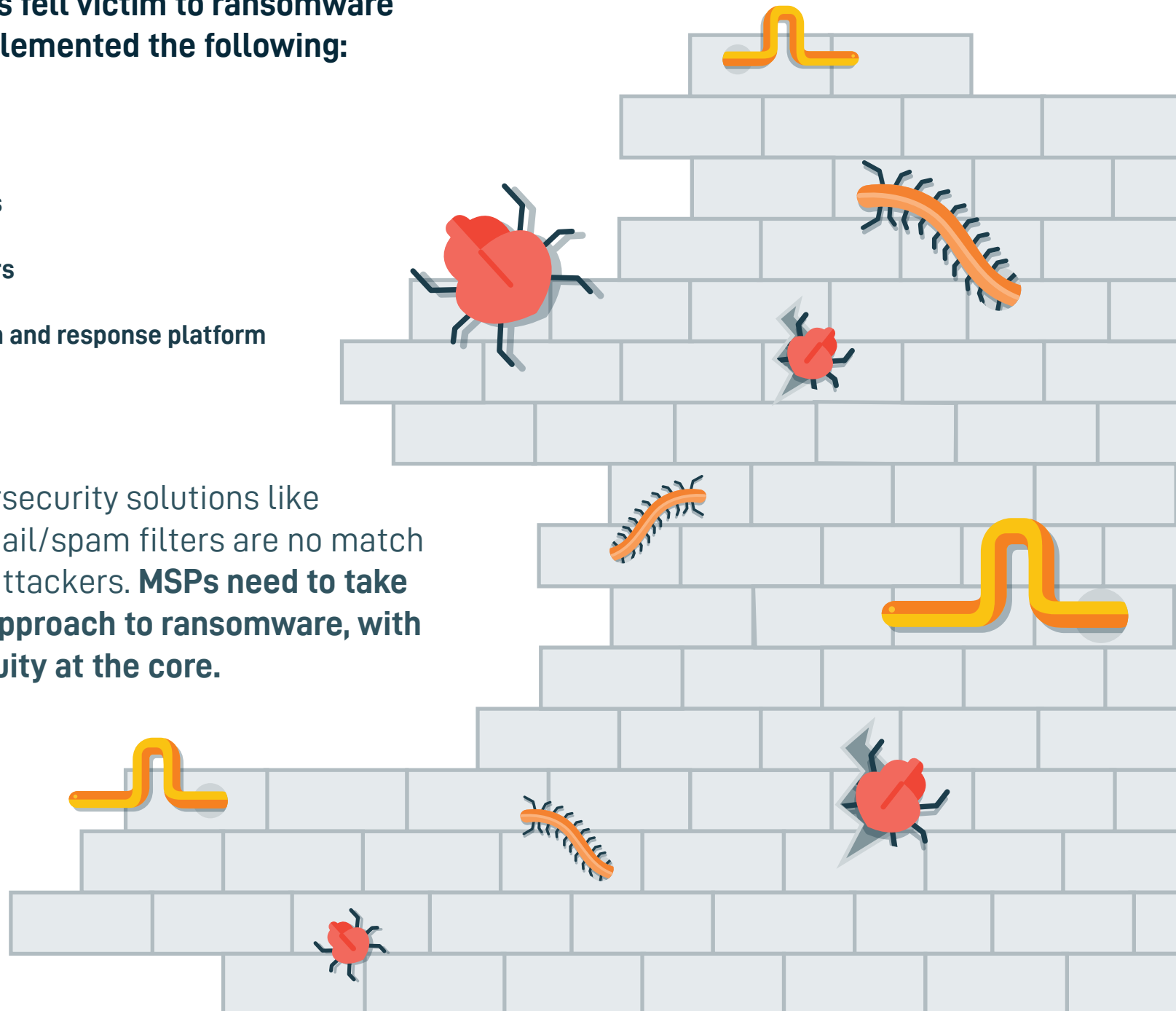
SMBs Continue to Take the Bait

Which of the following are the leading causes of ransomware?

67%
of MSPs report
phishing emails

36%
of MSPs report
lack of cybersecurity training

30%
of MSPs report
weak passwords/access management

25% of MSPs report poor user practices/gullibility
16% of MSPs report malicious websites/web ads
16% of MSPs report clickbait

Phishing, lack of cybersecurity training, and weak passwords are the top three **causes of successful ransomware attacks**.

Survey respondents were able to select multiple answer choices.

Ransomware Attacks: The Aftermath

Which of the following consequences resulted from a ransomware attack?

64% of MSPs report
loss of business productivity

33% of MSPs report
infection spread to other devices on the network

45% of MSPs report
business-threatening downtime

29% of MSPs report
decreased client profitability

34% of MSPs report
lost data and/or device

24% of MSPs report
clients paid a ransom and recovered the data

18% of MSPs report damaged reputations
**12%** of MSPs report stolen data
10% 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
4% of MSPs report clients paid ransom but data was never released

Survey respondents were able to select multiple answer choices.

Ransom, Downtime Costs, Skyrocket
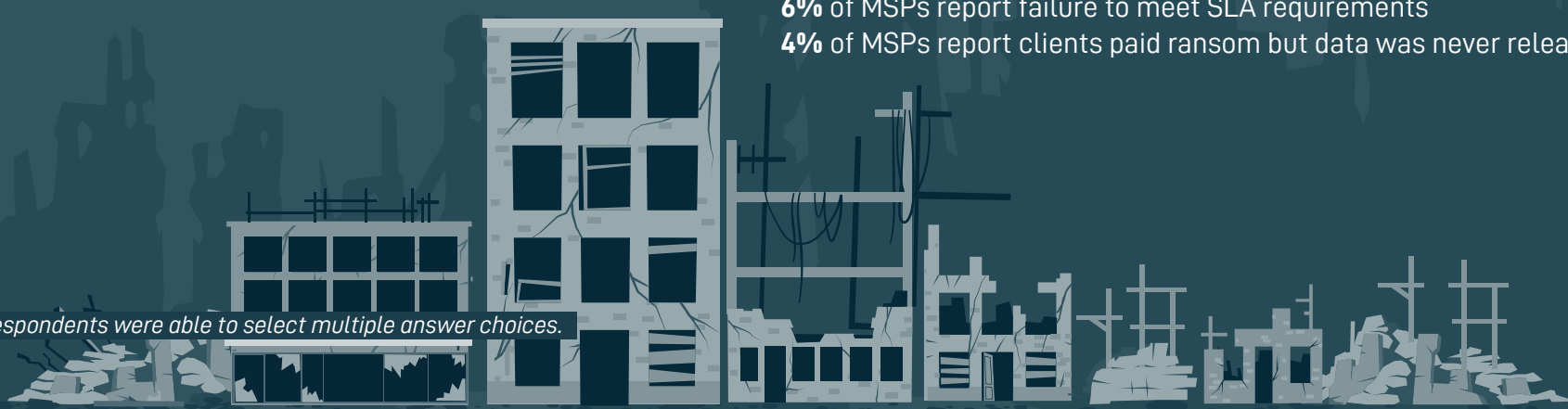
When it comes to ransomware attacks, MSPs report the **cost of downtime is** **23X** **greater than the ransom requested**

Average Ransom

2018 **$4,300** ↗ **2019** **$5,900**

MSPs report the average **cost of ransom increased by 37%** from previous year

Average Cost of Downtime

2018 **$46,800** ↗ **2019** **$141,000**

The average **downtime cost per incident** has soared **over 200%** from previous year
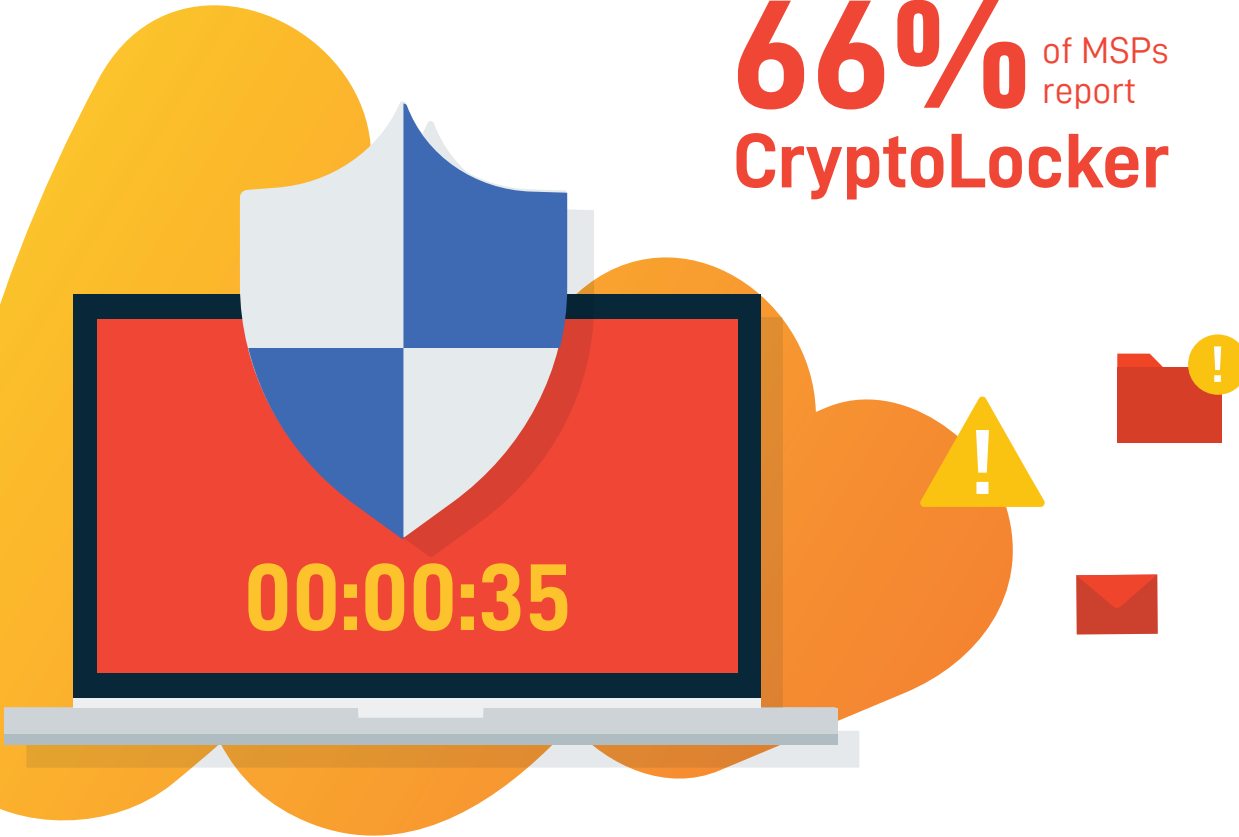
Geo Trend:
In Canada, MSPs report the highest **average cost of downtime at $180,000.**

All survey respondents answered in U.S. dollars.

CryptoLocker Remains Household Name

Which of the following strains of ransomware have affected your clients?
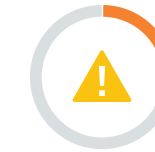
66% of MSPs report
CryptoLocker

00:00:35

49% of MSPs report
WannaCry

34% of MSPs report
CryptoWall

24% of MSPs report
Locky

17% of MSPs report Petya
14% of MSPs report CryptXXX
12% of MSPs report notPetya
11% of MSPs report TeslaCrypt
10% of MSPs report Emotet **(NEW)**
7% of MSPs report CBT Locker
7% of MSPs report TorrentLocker
7% of MSPs report CrySis
6% of MSPs report Bad Rabbit
5% of MSPs report Wallet **(NEW)**
4% of MSPs report CoinVault

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

Survey respondents were able to select multiple answer choices.

32% of MSPs report

Construction and Manufacturing most targeted by ransomware

It's not surprising that Construction and Manufacturing are top targets for ransomware. These industries are in a constant wave that flows with the ups and downs of the economy. Because of this, much of their work is project-based and recurring revenue is rare. As a result, it makes it difficult to invest in IT staffing or IT services that require monthly fees.

Vince Tinnirello, Managing Director, Anchor Network Solutions, Inc.

31% Professional Services
23% Healthcare
20% Finance/Insurance
18% Non-Profit
18% Legal
15% Retail
12% Real Estate
9% Architecture/Design
9% Government

8% Education
7% Consumer Products
5% Travel/Transportation
6% Media/Entertainment
4% High Technology
4% Energy/Utilities
2% Telecom
11% Other/None

Survey respondents were able to select multiple answer choices.

13

Windows Endpoint Systems Most Targeted by Hackers

89% of MSPs report

ransomware infecting endpoint systems

Of the 89%...

87% of MSPs report attacks on

Windows PC

11% of MSPs report attacks on Windows Tablet

7% of MSPs report attacks on MacOS X

5% of MSPs report attacks on Android

3% of MSPs report attacks on iOS

Geo Trend:
In Europe, 10% of MSPs report ransomware infecting Android systems, **exceeding the global average of 5%.**

Survey respondents were able to select multiple answer choices.

Ransomware Descends Over Office 365

28% of MSPs report **ransomware attacks in SaaS applications**

Of the 28%:

64% of MSPs report attacks within

Office 365

(up from 49% in 2018)

47% of MSPs report attacks within
Dropbox

18% of MSPs report attacks within
G Suite

6% of MSPs report attacks within Box
2% of MSPs report attacks within Salesforce

SMBs report 11% to 50% of their IT infrastructure is based in the cloud. This is expected to increase over the next 3 years, where most expect 21% to 75% to be in the cloud.**

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?

69% of MSPs report
reimaging a machine

53% of MSPs report
virtualizing the system from a backup image

37% of MSPs report
running software to cleanup threat

16% of MSPs report downloading a purpose-built software tool designed for ransomware recovery

15% of MSPs report relying on endpoint antivirus to recover

12% of MSPs report finding a decryption key

Survey respondents were able to select multiple answer choices.

BCDR Ranked Most Effective to Combat Ransomware

BCDR is ranked the #1 solution by MSPs.

🏆 **Business Continuity and Disaster Recovery (BCDR)**

⭐ **Employee training**

⭐ **Patch management**

⭐ **Unified threat management**

⭐ **Identity and 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

92% of MSPs report

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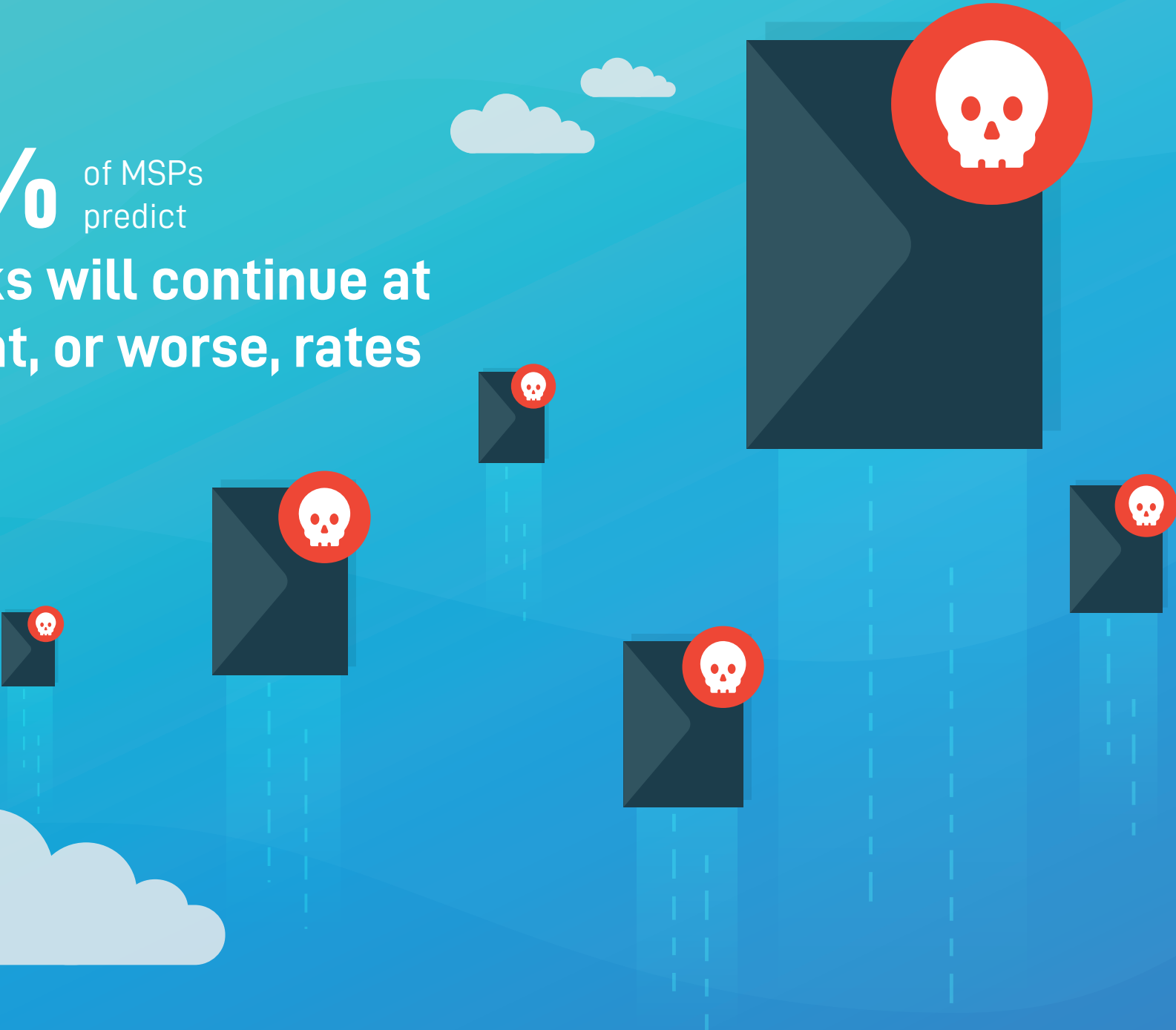
With BCDR,

4 in 5 MSPs report clients **fully recovered** in 24 hours, or less
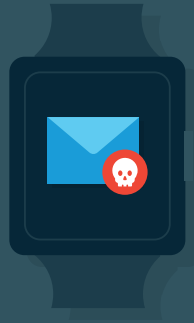
Without BCDR,

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

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

IoT Tops the List of Future Ransomware Attack Targets

64% 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

63% of MSPs predict ransomware will **target social media accounts**

56% of MSPs predict ransomware will **capture critical utility infrastructures (e.g., power grids)**

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

49% of MSPs predict ransomware will **target users based on demographics**

Hackers Aren't Only Targeting SMBs

4 in 5 agree

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

But the best offense is good defense:

60% of MSPs report
carrying **cyber liability insurance** should they or their clients become subject to a ransomware attack

50% of MSPs report
having **external expertise lined up** to help them in the event of a large scale attack against them or their clients

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.

MSPs Enable 2FA to Double Down on Ransomware Preparation

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

71% **Remote Monitoring and Management (RMM)**
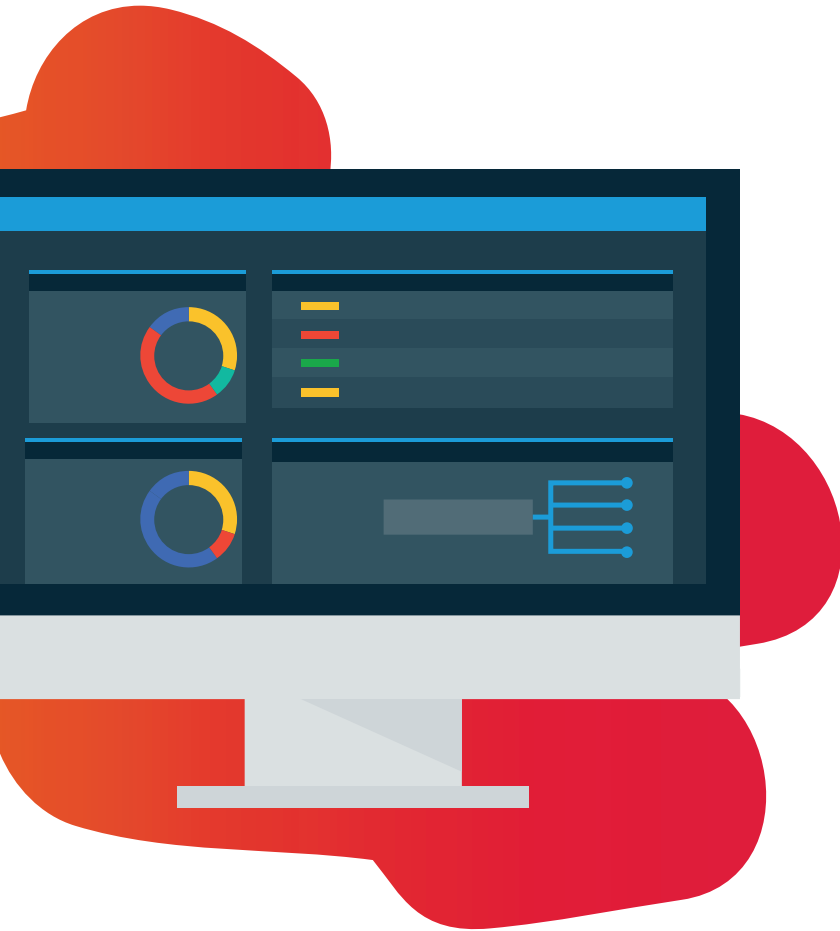
61%
Password Manager

56%
IT Documentation

60%
Email Client

43%
BCDR

58%
Professional Services Automation (PSA)

Final Takeaways:

Businesses must prepare the front line of defense: your employees. Today's companies must provide regular and mandatory cybersecurity training to ensure all employees are able to 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. Today's standard security solutions are no match for today's ransomware, which can penetrate organizations 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, although 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 cybersecurity 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 cybersecurity monitoring, they should be leveraging a managed service provider (MSP) who has the time and resources to anticipate and protect a company from the latest cybersecurity threats.

E-TECH

For more information please contact:

Ian Evans | President and CEO | Phone: 647-361-8191 x 105 | Email: marketing@etechcomputing.com | E-Tech | https://www.etechcloud.ca