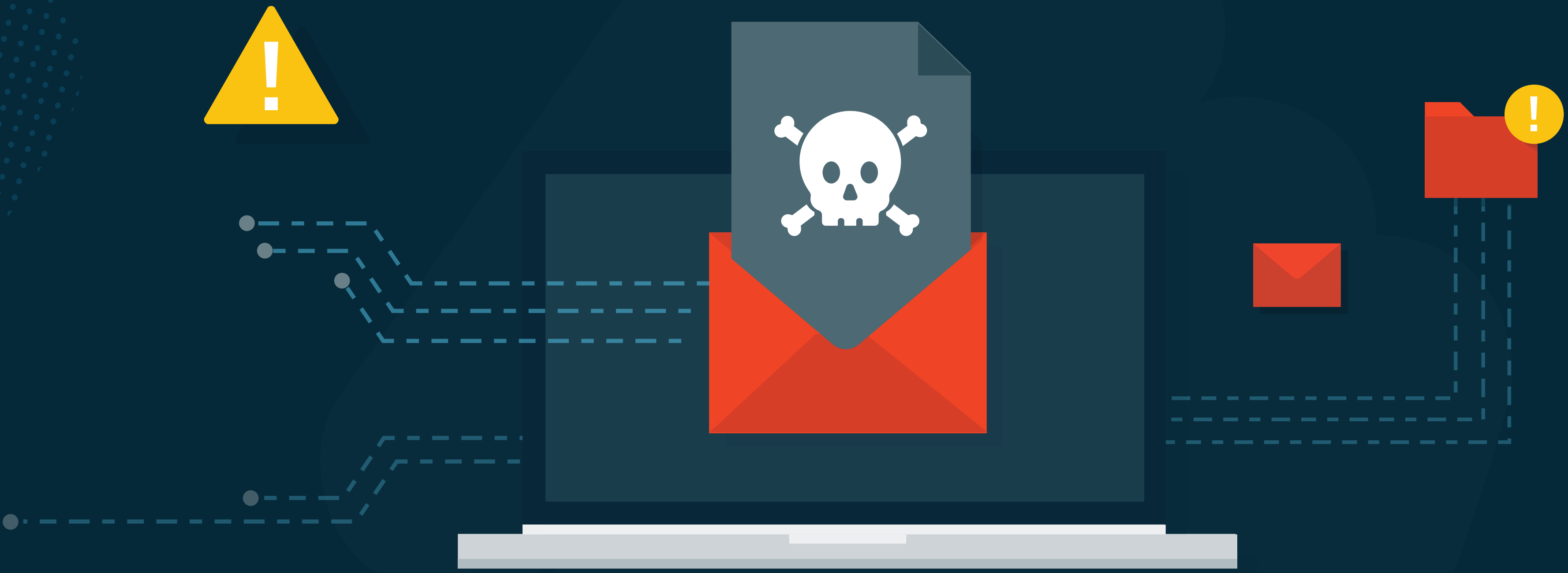
Report

datto



Datto's ANZ State of the Channel

Ransomware Report

Follow us on Twitter: **@Datto**

Visit our Blog: **www.datto.com/au/blog**

About the Report

Datto's State of the Channel Ransomware Report is comprised of statistics pulled from a survey of 200+ managed service providers (MSPs), our partners and customers, 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 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.

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.

Key Findings

- **Ransomware remains a massive threat to small-to-mid-sized businesses (SMBs).** From Q2 2016 - Q2 2018, 81% of MSPs report ransomware attacks against customers. In the first 6 months of 2018 alone, 64% report ransomware attacks against clients. 92% of MSPs predict the number of ransomware attacks will continue at current, or worse, rates.
- **The average managed service providers (MSPs) report 4+ of these attacks within their client base per year.** In the first half of 2018, an alarming 42% of MSPs report clients suffered multiple attacks in a single day (up 7%, year-over-year).
- **The problem is bigger than we know, as a startling number of attacks go unreported.** MSPs report that less than 1 in 5 ransomware attacks are reported to the authorities.
- **SMBs are largely in the dark about the frequency and severity of ransomware attacks.** Nearly 90% of MSPs are "highly concerned" about the ransomware threat and 44% report their SMB clients feel the same.
- **Lack of cybersecurity education is a leading cause of a successful ransomware attack.** MSPs rank phishing emails as the top ransomware delivery method followed by malicious websites, web ads, and clickbait.
- **The aftermath of a ransomware attack can be crippling for a business.** When asked about the impacts of a successful attack, 69% of MSPs report victimised clients experienced a loss of business productivity. Nearly 60% report clients experienced business-threatening downtime.
- **The cost of business downtime is nearly 10X greater than the cost of the ransom requested.** MSPs report the average requested ransom for SMBs is ~$6,000 AUD while the average cost of downtime related to a ransomware attack is ~ $58,000 AUD.
- **Attacks on Android systems peak in ANZ.** 11% of MSPs report ransomware attacks on Android systems, exceeding the global average of 8%.
- **Ransomware infections in the cloud continue to increase year-over-year.** Of MSPs that report cloud-based malware infections, nearly 45% called out Office 365 as the target.
- **In comparison to other solutions, the most effective for avoiding downtime caused by ransomware is business continuity and disaster recovery (BCDR).** Specifically, roughly 85% report that victimised clients with Datto BCDR in place fully recovered from the attack in 24 hours, or less.

Most SMBs Unaware of Ransomware Risk

Only 44% of MSPs report SMBs "highly concerned" about ransomware.

89% of MSPs think they should be.

Here's why...

Ransomware Most Prominent Malware Threat to SMBs

Which of the following malware attacks have affected your clients in the last 2 years? (Check all that apply)

81% of MSPs report clients struck by ransomware

62% of MSPs report clients struck by viruses

49% of MSPs report clients struck by adware

42% of MSPs report clients struck by spyware

39% of MSPs report clients struck by trojan horses

33% of MSPs report clients struck by cryptojacking

25% of MSPs report clients struck by rootkits

23% of MSPs report clients struck by worms

12% of MSPs report clients struck by keyloggers

Ransomware Attacks Continue to Climb

From Q2 2016 - Q2 2018

81% of MSPs

report ransomware attacks against SMBs. In the first half of 2018 alone, **64% report attacks against clients.**

92% of MSPs

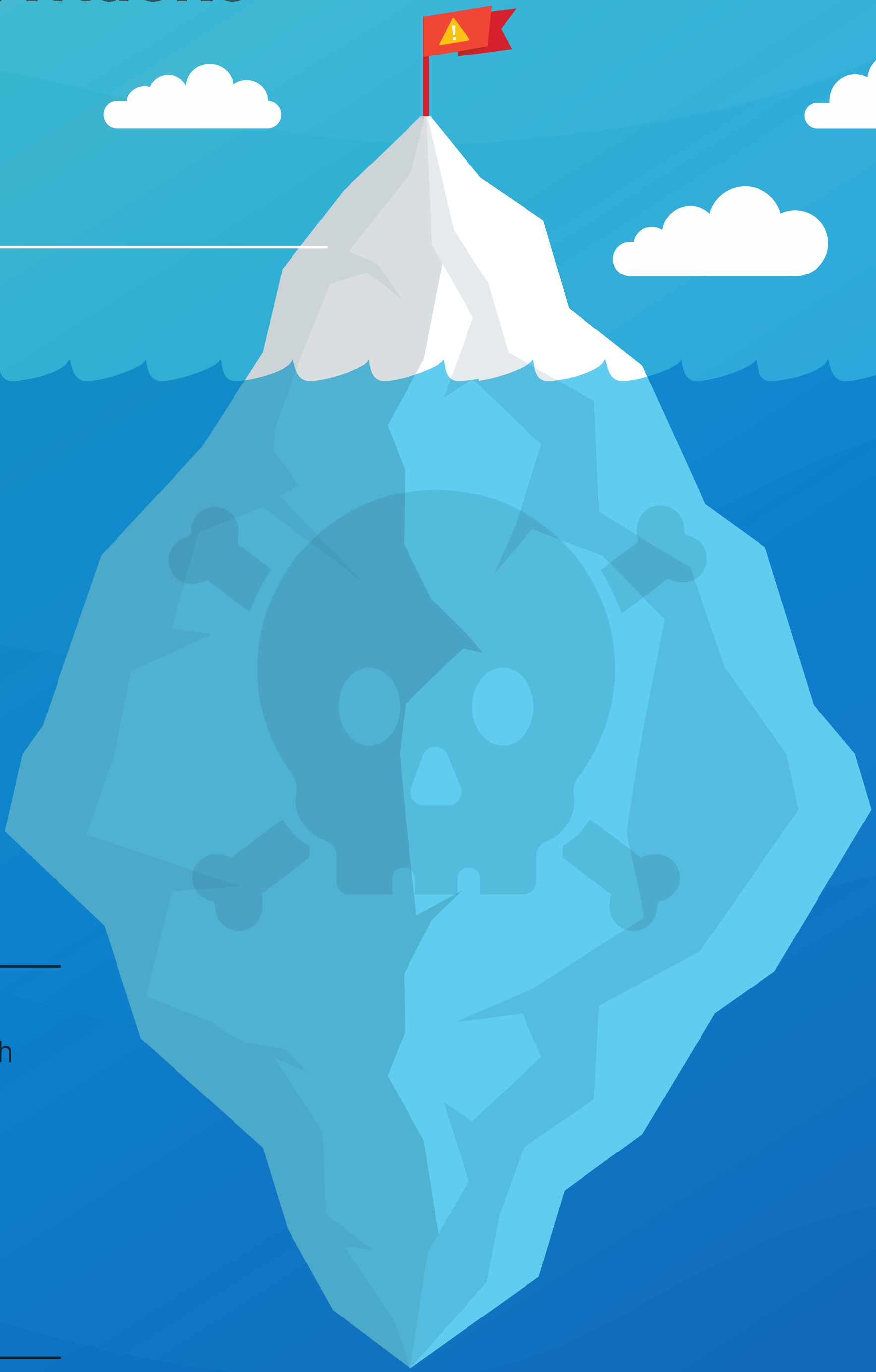
predict the number of **ransomware attacks will continue at current, or worse, rates.**

42% of MSPs

report clients suffered **multiple attacks** in the same day **(up from 35% in the previous year).**

ANZ Trend: 64% marks the highest rate of MSPs reporting ransomware attacks in the first 6 months of 2018 globally.

On Average, MSPs Report 4+ Attacks Against Clients Per Year



But only about

18%

of those attacks are reported to authorities, which means the problem is likely **bigger than we know.**

Takeaway: in 2018, Australia joined other countries and regions in passing laws to require companies to report data breaches to both the authorities and their customers.

- **Australia: Notifiable Data Breaches law**
- **European Union:** The General Data Protection Regulation
- **California, USA:** California Consumer Privacy Act of 2018

It's likely that the number of reported attacks will increase as laws like these are adopted around the world.

Data Breaches Scheme Increases Awareness of Attacks

Australia's Notifiable Data Breaches (NBD) scheme came into effect at the beginning of 2018. Under the law, any business with an annual turnover of $3 million or more that is covered by the Australian Privacy Act (1998) is obliged to notify individuals whose personal information is involved in a data breach, as soon as practicable after becoming aware of a breach. Since the law passed, hundreds of breaches have been reported over the course of 2018, and a handful have already been reported in 2019. Of the breaches reported, nearly 60% were caused by malicious or criminal behavior, including cyber attacks. Various industries have been targeted by hackers, and data breaches don't seem to be slowing down across Australia.

2018

800+ Breaches Were Reported
over the course of the year

January - April

128 Breaches reported

May 2018

87 Breaches reported

Ransomware Attack Hits Family Planning NSW

- Personal details of around 8,000 clients potentially compromised
- One of several agencies targeted on the same day - cyber criminals demand $15,000 in bitcoin ransom
- Family Planning temporarily shuts down website to prevent any further data breaches and refuses to pay cyber criminals
- To date, there has been no evidence that client information has been used by the cyber-attackers

June - August

259 Breaches reported

Sept. - Dec.

338 Breaches reported

2019
January

5+ Breaches Reported

Including:

- My Health Records
- Nova Entertainment
- Victorian Government Directory

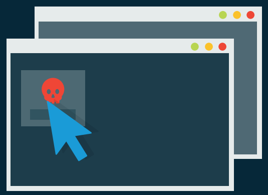
Sources: Office of the Australian Information Commissioner, Family Planning NSW

End User Error is the Common Denominator

Top Ransomware Delivery Methods:

56% of MSPs
Report Phishing Emails

25% of MSPs
Report Malicious Websites/Web Ads

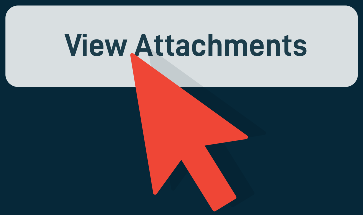


16% of MSPs
Report Clickbait

Top Cybersecurity Vulnerabilities:

34% of MSPs
Report Lack of End User Cybersecurity Training

29% of MSPs
Report Weak Passwords/Access Management



27% of MSPs
Report Poor User Practices/Gullibility

Ransomware Attacks Are Costly

Which of the following have your clients experienced due to a ransomware attack?
(Check all that apply)

69% of MSPs report loss of business productivity

59% of MSPs report business-threatening downtime

51% of MSPs report data and/or device was lost

39% of MSPs report infection spread to other devices on the network

37% of MSPs report decreased customer profitability

35% of MSPs report clients paid a ransom and recovered the data

29% of MSPs report damaged reputations

24% of MSPs report stolen data

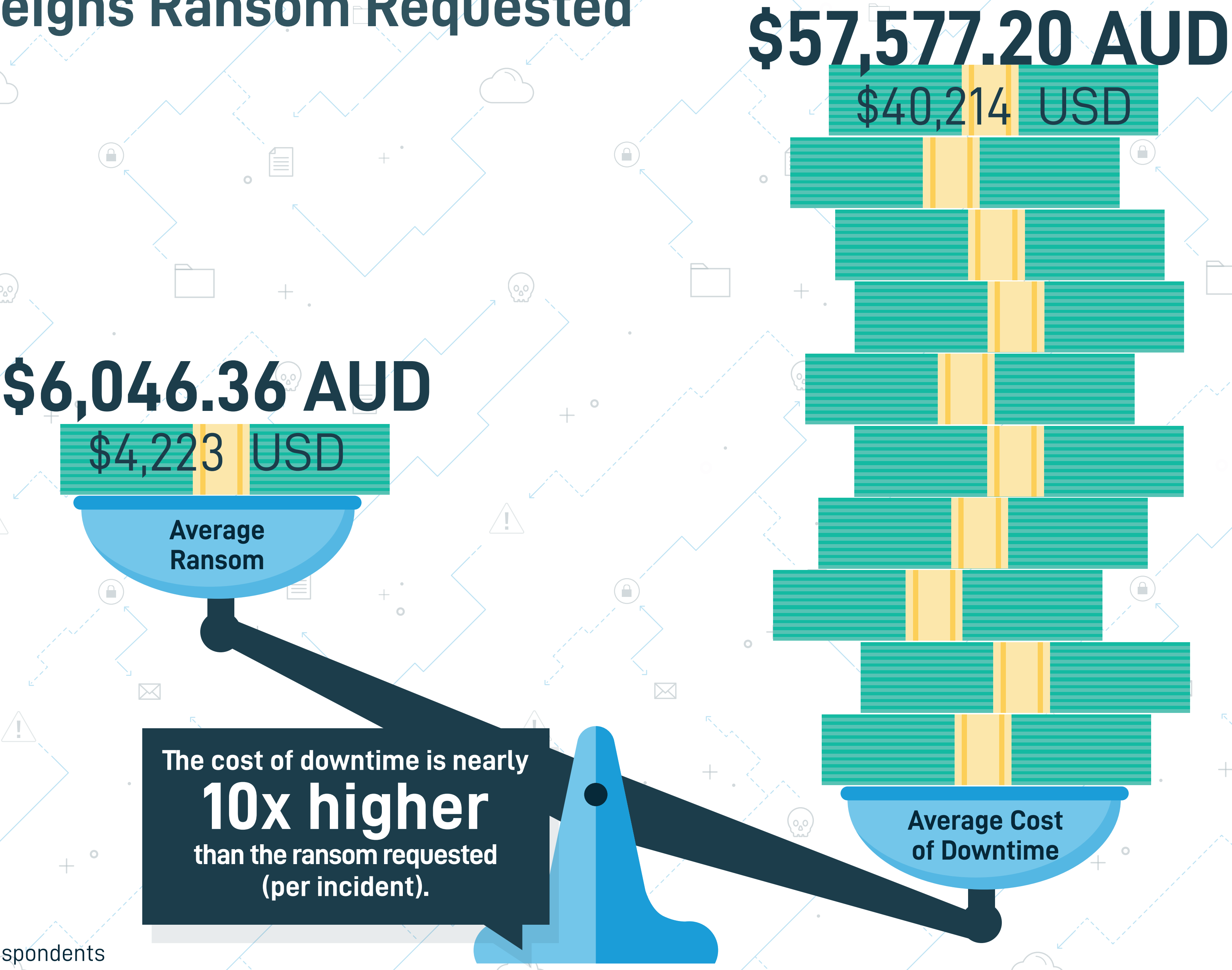
23% of MSPs report ransomware remained on system, struck again!

21% of MSPs report failure to meet SLA requirements

17% of MSPs report paid a ransom, data was never released

12% of MSPs report failure to achieve regulatory compliance

Cost of Downtime Significantly Outweighs Ransom Requested



The cost of downtime is nearly

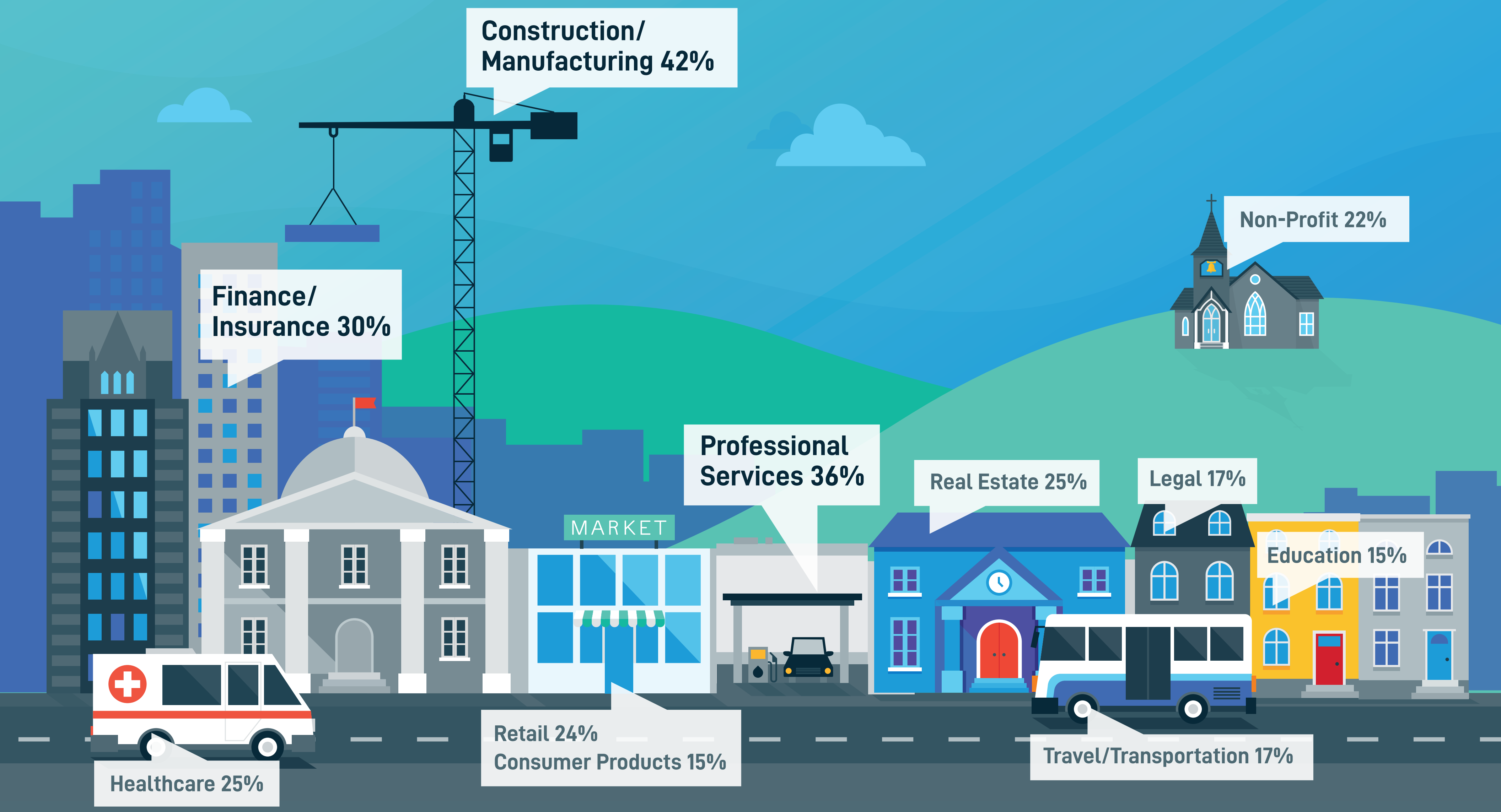
10x higher

than the ransom requested (per incident).

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

No Industry is Safe from Ransomware

Which industries have you seen victimised by ransomware? (Check all that apply)



Construction/ Manufacturing 42%

Finance/ Insurance 30%

Professional Services 36%

Real Estate 25%

Legal 17%

Non-Profit 22%

Education 15%

Healthcare 25%

Retail 24%
Consumer Products 15%

Travel/Transportation 17%

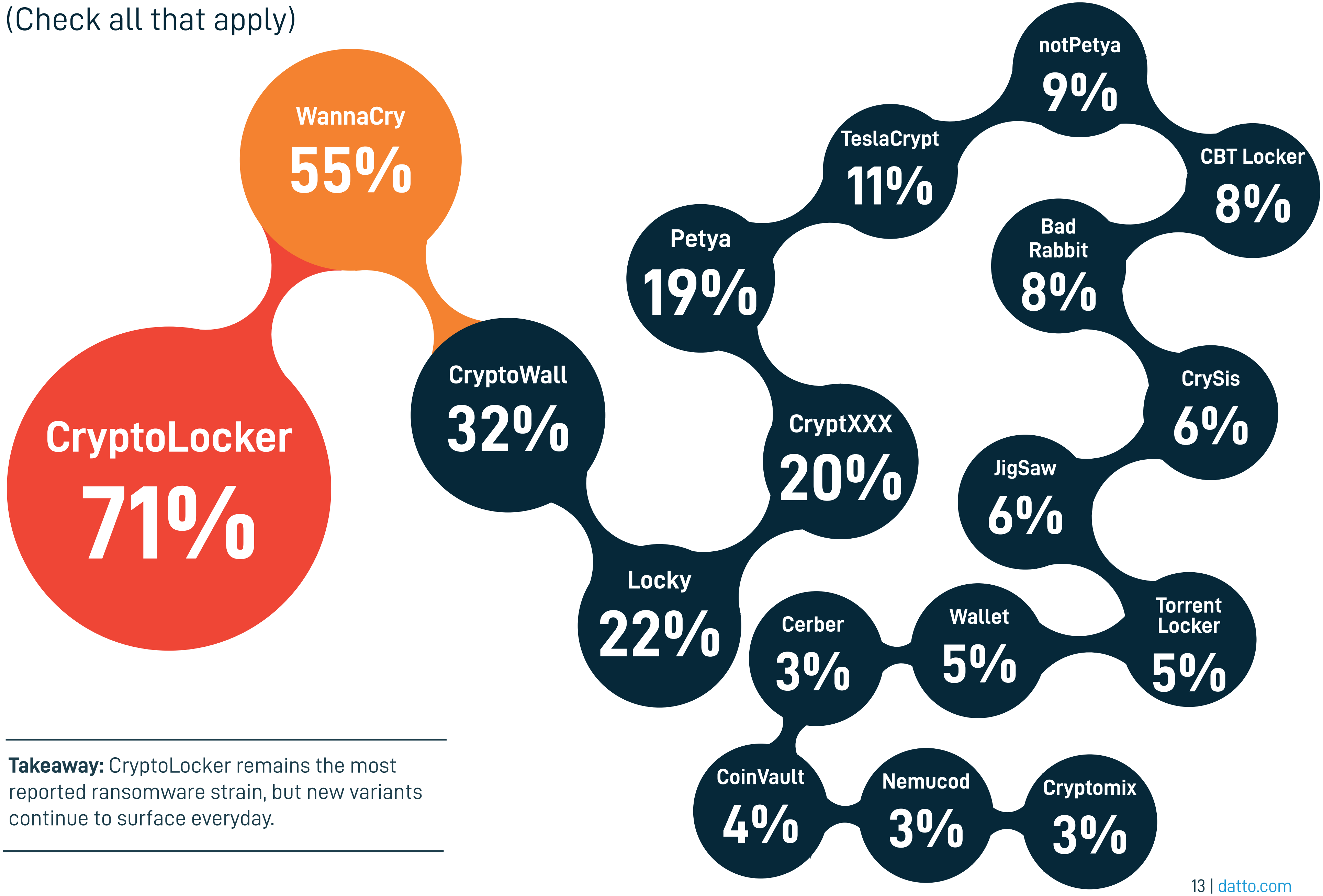
High Technology 11%
Architecture/Design 10%

Government 8%
Telecom 7%

Media/Entertainment 6%
Energy/Utilities 6%

CryptoLocker and WannaCry Reign Supreme

Have your clients been victimised by any the following ransomware attacks?
(Check all that apply)



Takeaway: CryptoLocker remains the most reported ransomware strain, but new variants continue to surface everyday.

ANZ Suffers the Highest Rate of Android Ransomware

11% of MSPs reporting infections in that system

Which systems have you seen infected by ransomware?
(Check all that apply)

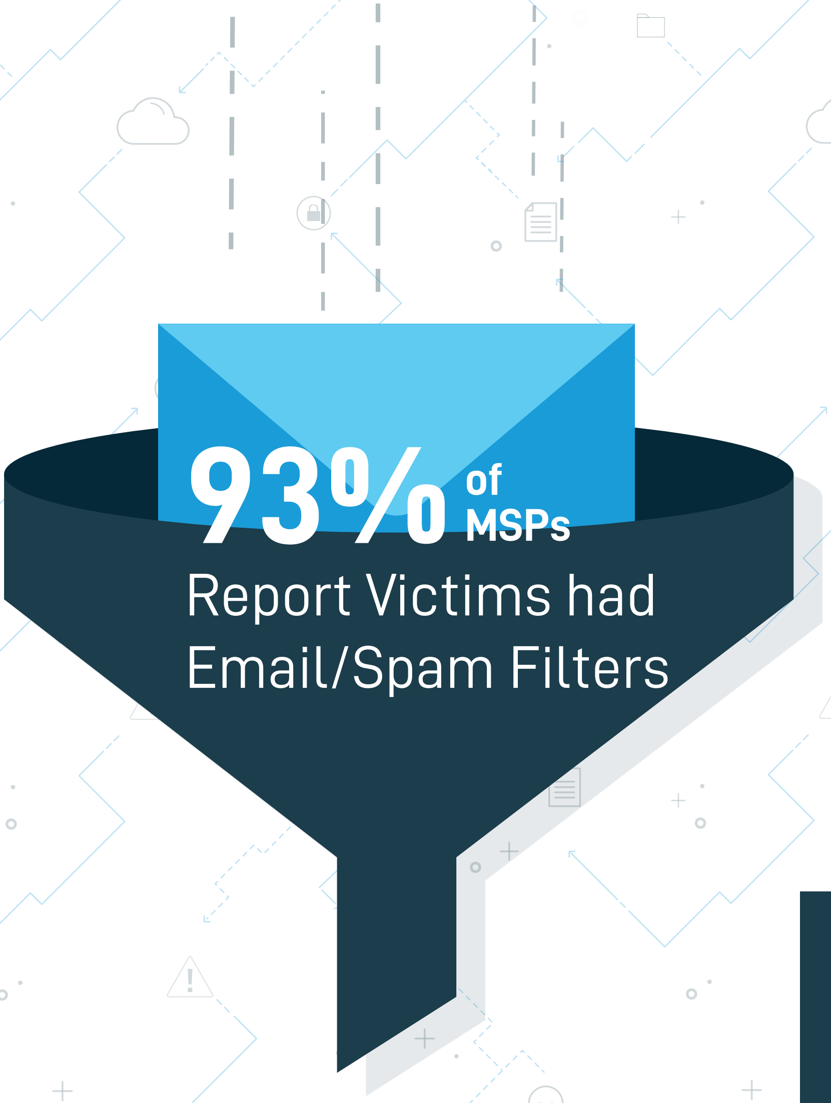
98%
Windows

5%
macOS

11%
Android

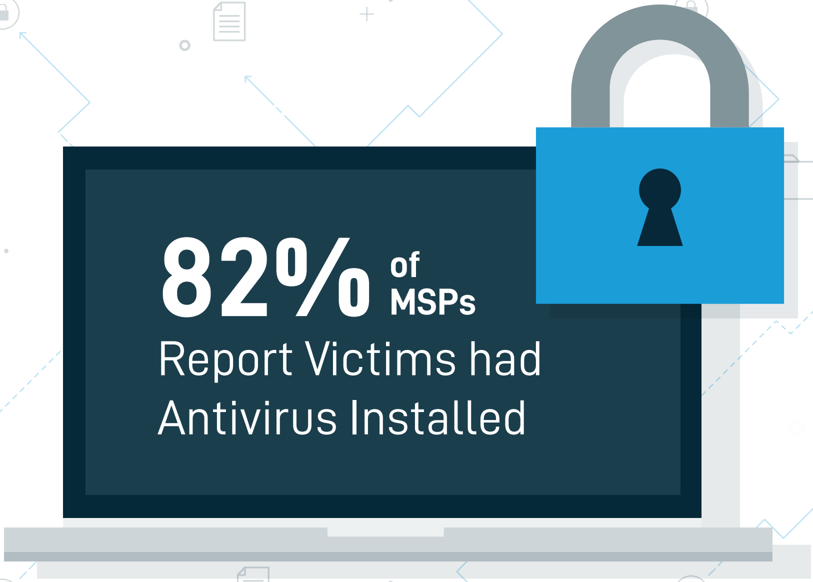
3%
iOS

Nothing Can Prevent Ransomware



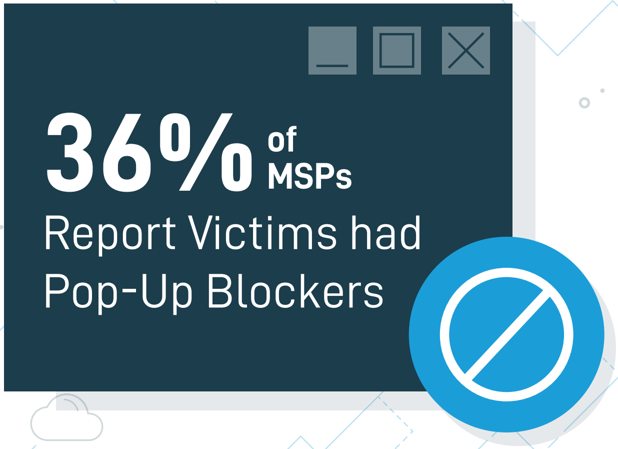
93% of MSPs

Report Victims had Email/Spam Filters



82% of MSPs

Report Victims had Antivirus Installed

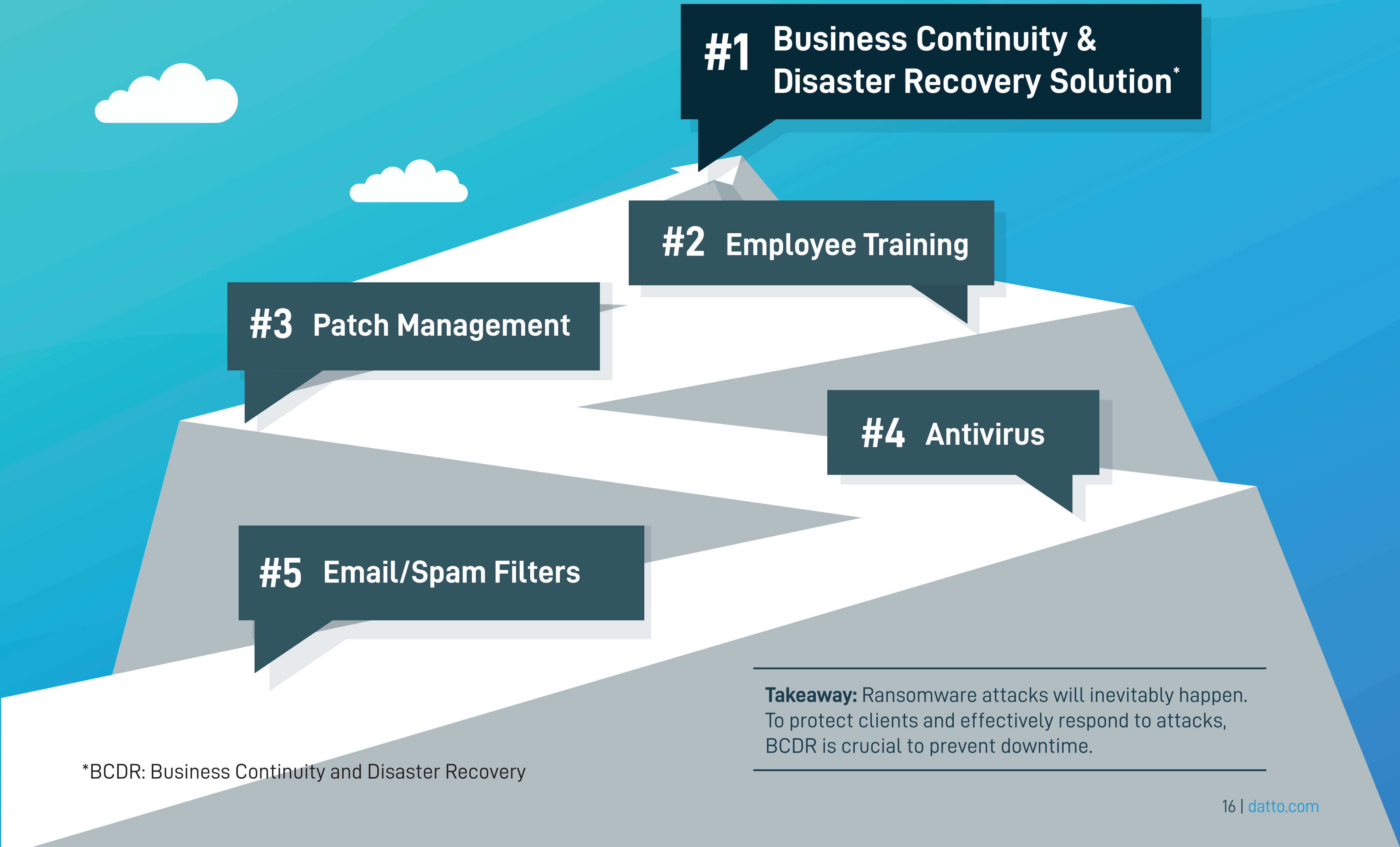


36% of MSPs

Report Victims had Pop-Up Blockers

Takeaway: As no single solution is guaranteed to prevent ransomware attacks, a multilayered portfolio is highly recommended.

MSPs Rank BCDR as Most Effective for Ransomware Protection Compared to Other Solutions



#1 Business Continuity & Disaster Recovery Solution*

#2 Employee Training

#3 Patch Management

#4 Antivirus

#5 Email/Spam Filters

Takeaway: Ransomware attacks will inevitably happen. To protect clients and effectively respond to attacks, BCDR is crucial to prevent downtime.

*BCDR: Business Continuity and Disaster Recovery

With Reliable BCDR, Costly Downtime is Avoided

With BCDR[*†], 84%

of MSPs report clients **fully recovered** from an attack in **24 hours, or less.**

Without BCDR, Only 47%

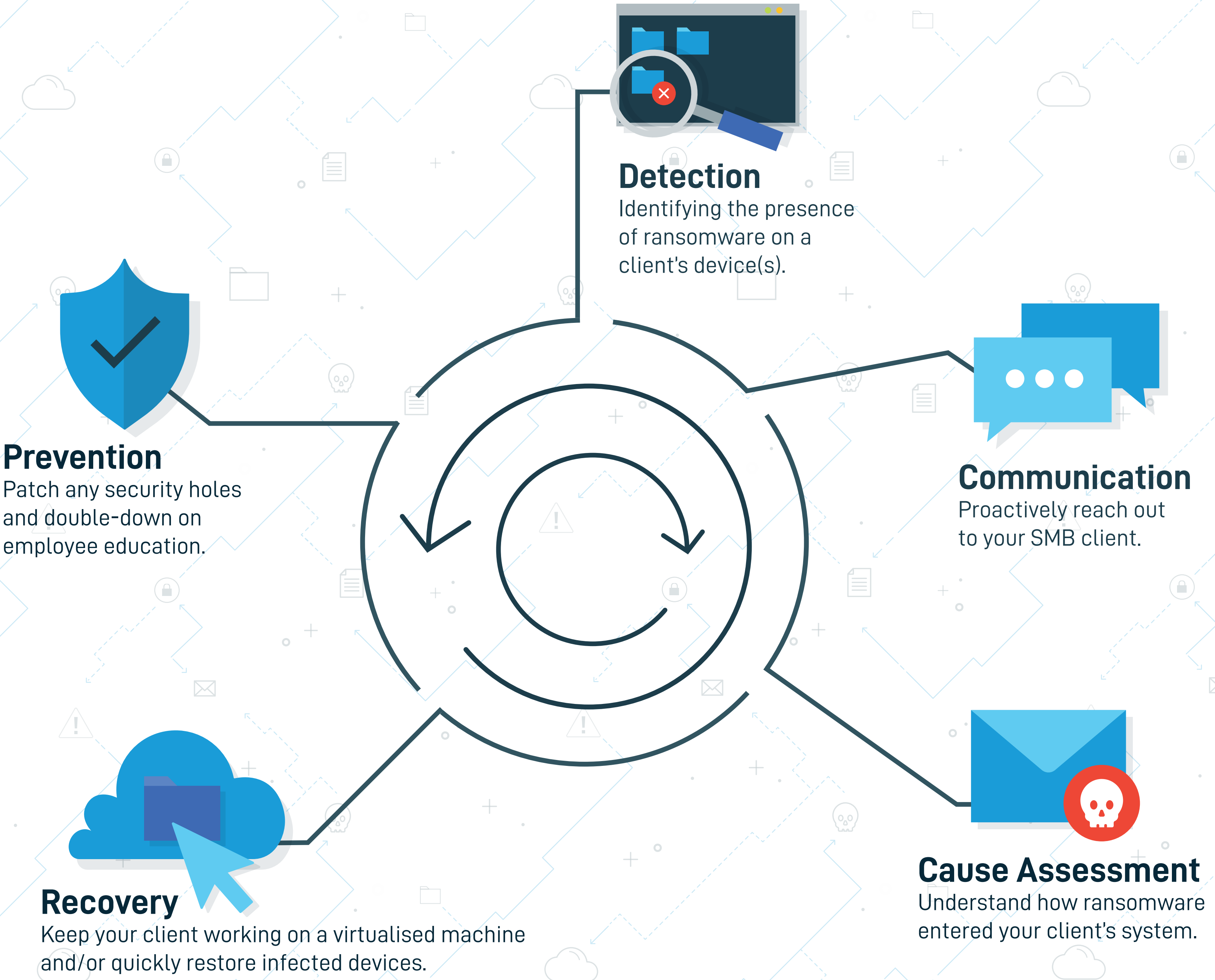
of MSPs report clients were able to do the same.

Not only does BCDR make recovery fast, MSPs rank it as the **#1 most cost effective ransomware solution.**

[*] BCDR: Business Continuity and Disaster Recovery

[†] Refers to Datto devices

A Ransomware Response Plan Needs More Than BCDR



Detection
Identifying the presence of ransomware on a client's device(s).

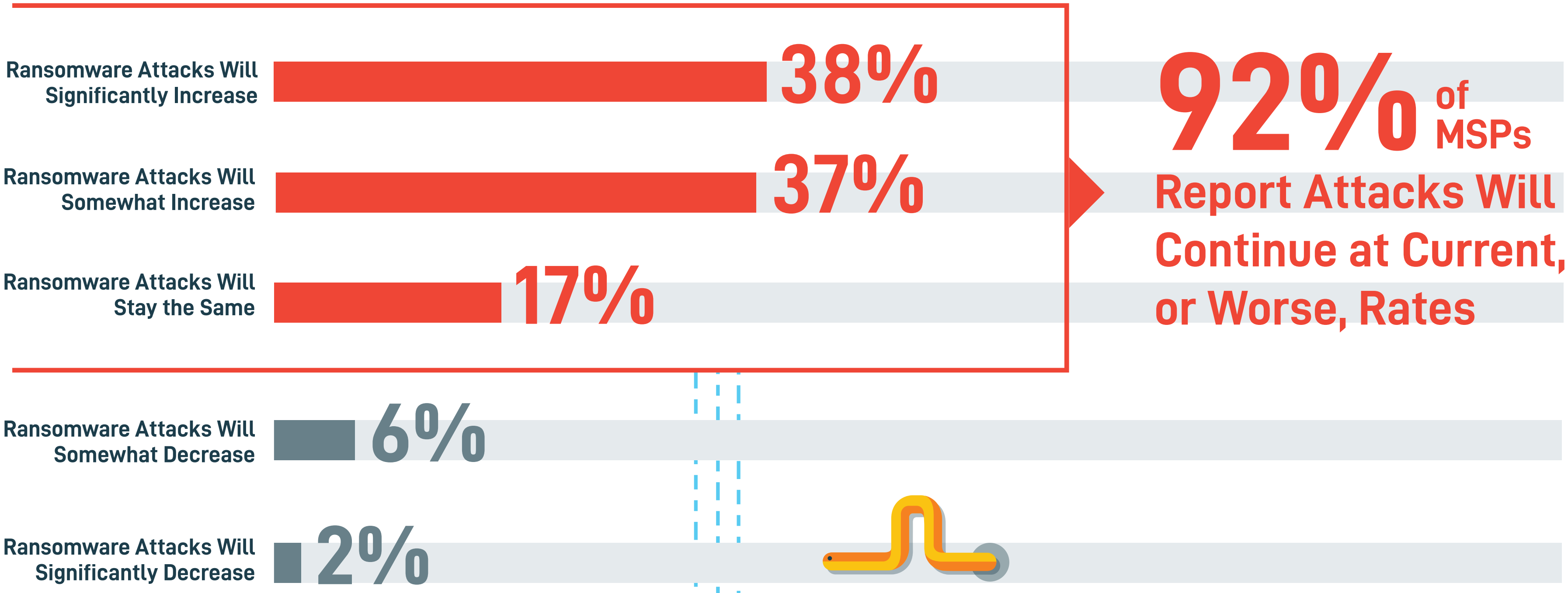
Prevention
Patch any security holes and double-down on employee education.

Communication
Proactively reach out to your SMB client.

Recovery
Keep your client working on a virtualised machine and/or quickly restore infected devices.

Cause Assessment
Understand how ransomware entered your client's system.

Majority of MSPs Report: Ransomware is Here to Stay

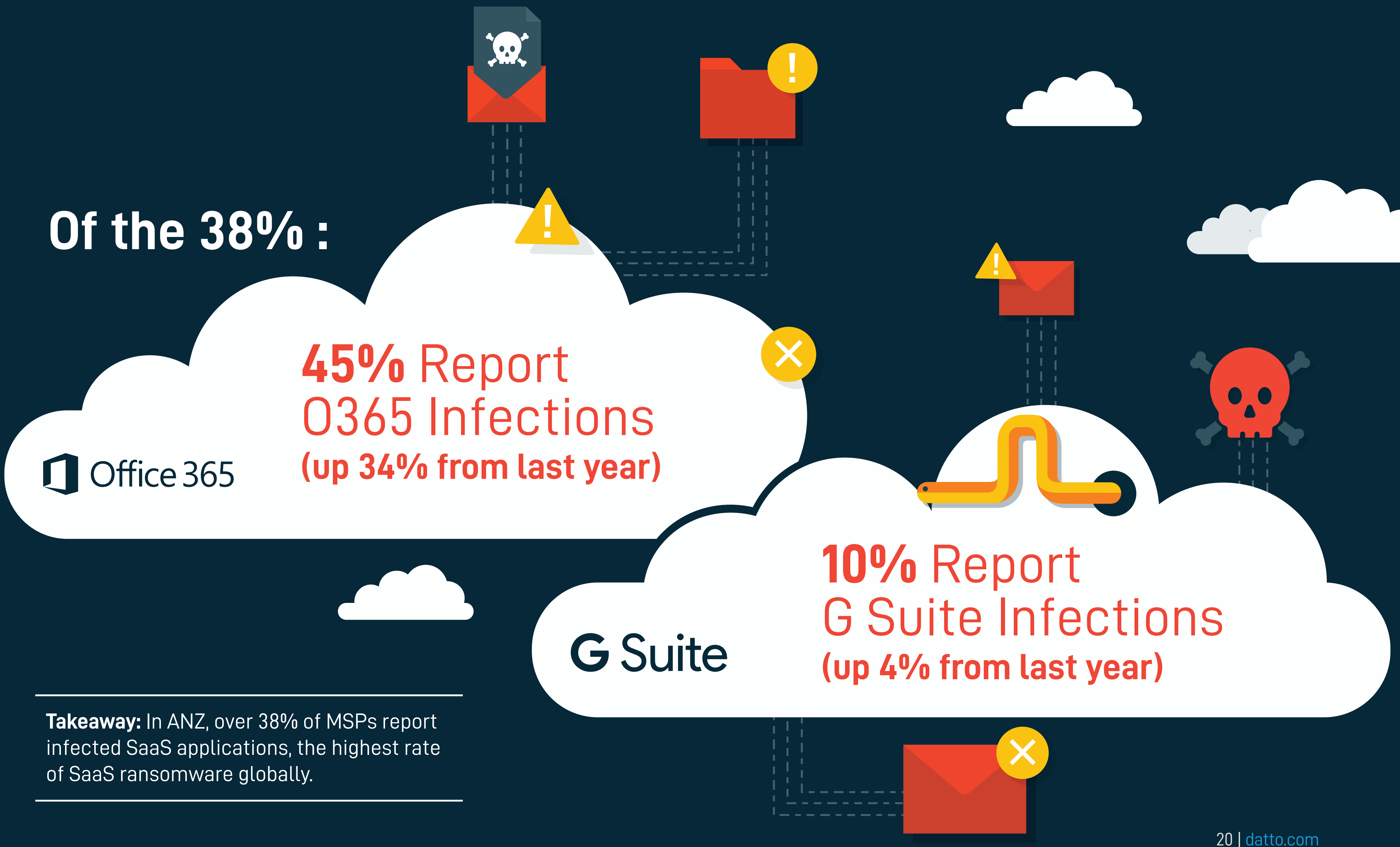


92% of MSPs Report Attacks Will Continue at Current, or Worse, Rates

Ransomware Will Creep into the Cloud

38% of MSPs have seen ransomware attacks in SaaS applications

Of the 38% :



Office 365

45% Report
O365 Infections
(up 34% from last year)

G Suite

10% Report
G Suite Infections
(up 4% from last year)

Takeaway: In ANZ, over 38% of MSPs report infected SaaS applications, the highest rate of SaaS ransomware globally.

Ransomware of the Future Gets Personal

53% of MSPs

Predict Ransomware Will Target

Social Media Accounts

54% of MSPs

Predict Ransomware Will Target

IoT Devices

48% of MSPs

Predict Ransomware Will

Bankrupt Whole Companies

44% of MSPs

Predict Ransomware Will Target

Critical Utility Infrastructure

34% of MSPs

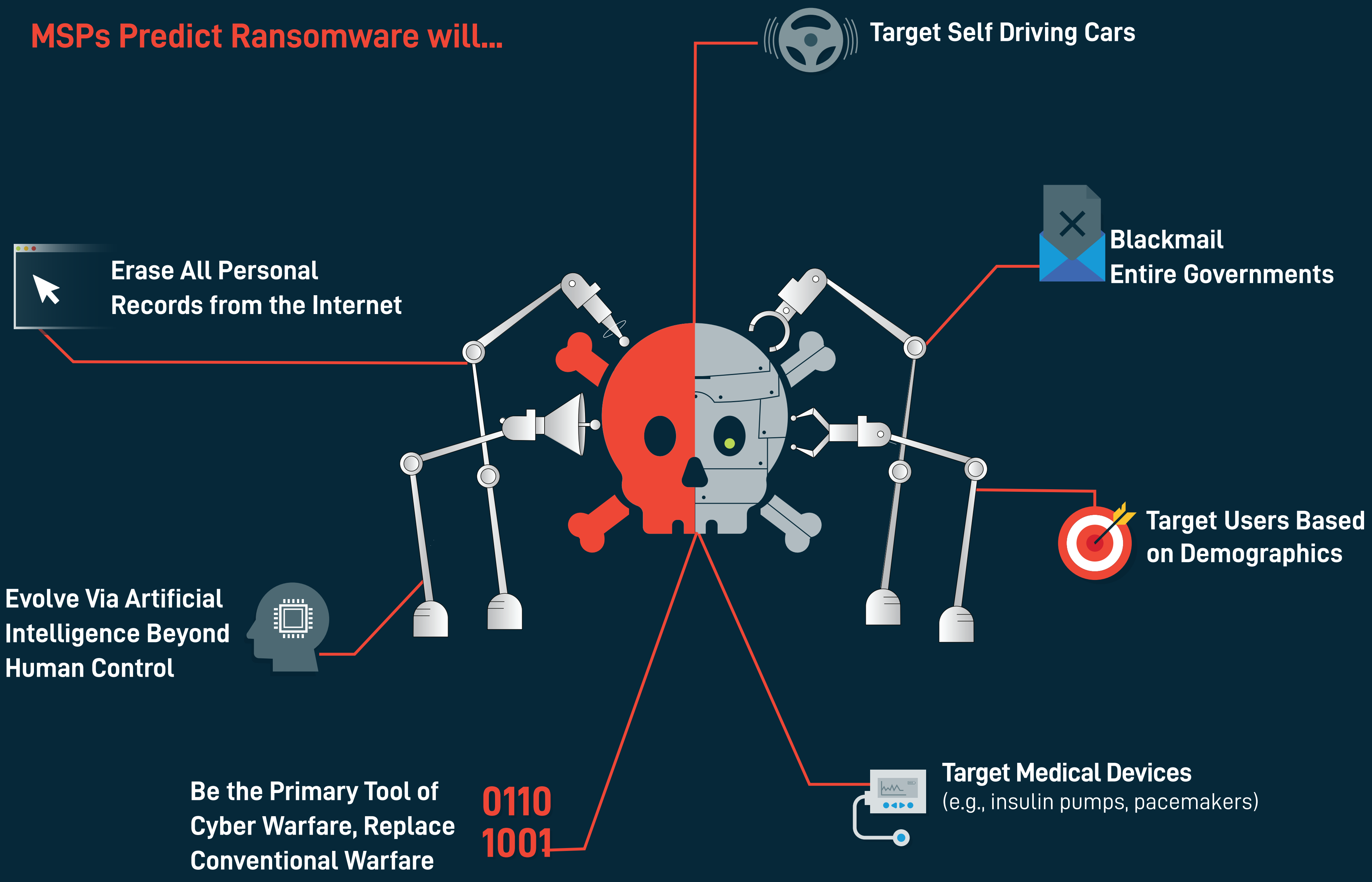
Predict Ransomware Will Target

Wearables

(e.g. smartwatches)

Ransomware Will Wreak Havoc Everywhere

MSPs Predict Ransomware will...



Target Self Driving Cars

Blackmail
Entire Governments

Target Users Based
on Demographics

Target Medical Devices
(e.g., insulin pumps, pacemakers)

Be the Primary Tool of
Cyber Warfare, Replace
Conventional Warfare

Evolve Via Artificial
Intelligence Beyond
Human Control

Erase All Personal
Records from the Internet

Final Takeaways

Businesses must prepare the front line of defence: 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 organisations in multiple ways. Reducing the risk of infections requires a multilayered approach rather than a single product.

Businesses must ensure business continuity with BCDR. There is no sure fire way of preventing ransomware. Instead, businesses should focus on how to maintain operations despite a ransomware attack. One way to do this is a solid, fast and reliable business continuity and disaster recovery solution.

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.

Additional Resources

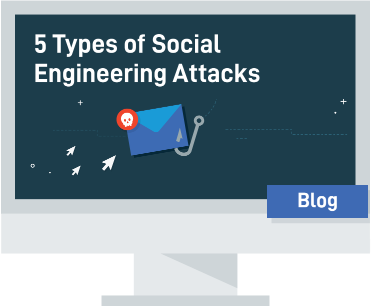
You Also Might Be Interested In:

eBook
datto
Cybersecurity Made MSPeasy Toolkit

MSPeasy Series
datto
Ransomware Made MSPeasy
The MSPs Guide to Saving the Day

eBook
datto
Defending Office 365 Data from Ransomware

Knowledge is Power: Ransomware Education for Employees


5 Types of Social Engineering Attacks
Blog

Common Types of Ransomware to Keep and Eye Out For
Slideshare

7 Steps to Ransomware Recovery
Slideshare

Ransomware Survivor Stories

datto
SUCCESS STORY
300K Files Locked by Ransomware? No Problem for PCS and Datto
datto

datto
SUCCESS STORY
MSP Recovers 85K Files from a Ransomware Attack
datto

Cole Informatics Saves Vick Insurance from Ransomware Disaster

Stay Up-To-Date on All Things Ransomware:

Subscribe

To the Datto blog

Visit the Datto Website

Learn more about ransomware

Become a Datto Partner

About Datto Ransomware Protection

With Datto, MSPs can easily identify a ransomware attack and roll systems back across devices and SaaS applications to a point-in-time before the attack occurred. Ransomware, like most illicit software, leaves an identifiable footprint as it takes over a server, PC or laptop. Datto devices, which actively monitor backups, can detect a ransomware footprint and instantly notify admins that they have a ransomware attack on their hands. After that, recovery is simply a matter of restoring from a previous known (good) backup.

Datto protects all of your business data, no matter where it lives:

Protect backup data itself: While backups are happening, they exist as a network share that ransomware could encrypt and subsequently compromise other backups in the chain. Datto's patented Inverse Chain Technology protects existing backups, and in the event of an attack, Datto can roll the data back to a healthy, protected point and continue on as if nothing happened.

Get back to production quickly: Datto offers restore options for any scenario - ranging from granular restore of specific files to restoring an entire system. No matter what the scope of the ransomware attack is, Datto gets you back to production quickly, reducing your Failback Time Objective (FTO) to the time of a reboot.

Protect Office 365 and G Suite data: SaaS Protection takes point-in-time backups daily across client SaaS apps, so MSPs can roll files and data back to a known good state of health.

Protect NAS information: Every Datto NAS device includes NAS Guard, which allows customers to protect the device and other network storage with full image rollbacks under one umbrella.

Restore only the information you need: Use Backup Insights to compare what changed and restore only what is needed.

Patch systems to protect against ransomware: A proactive patch management strategy using Datto RMM is the best first line of defence for MSP clients. MSPs can quickly pinpoint devices operating with outdated software, or those that have yet to receive the latest patch and can systematically deploy updates to mitigate the number of vulnerabilities exploited by ransomware.

For more information, visit: https://www.datto.com/continuity.