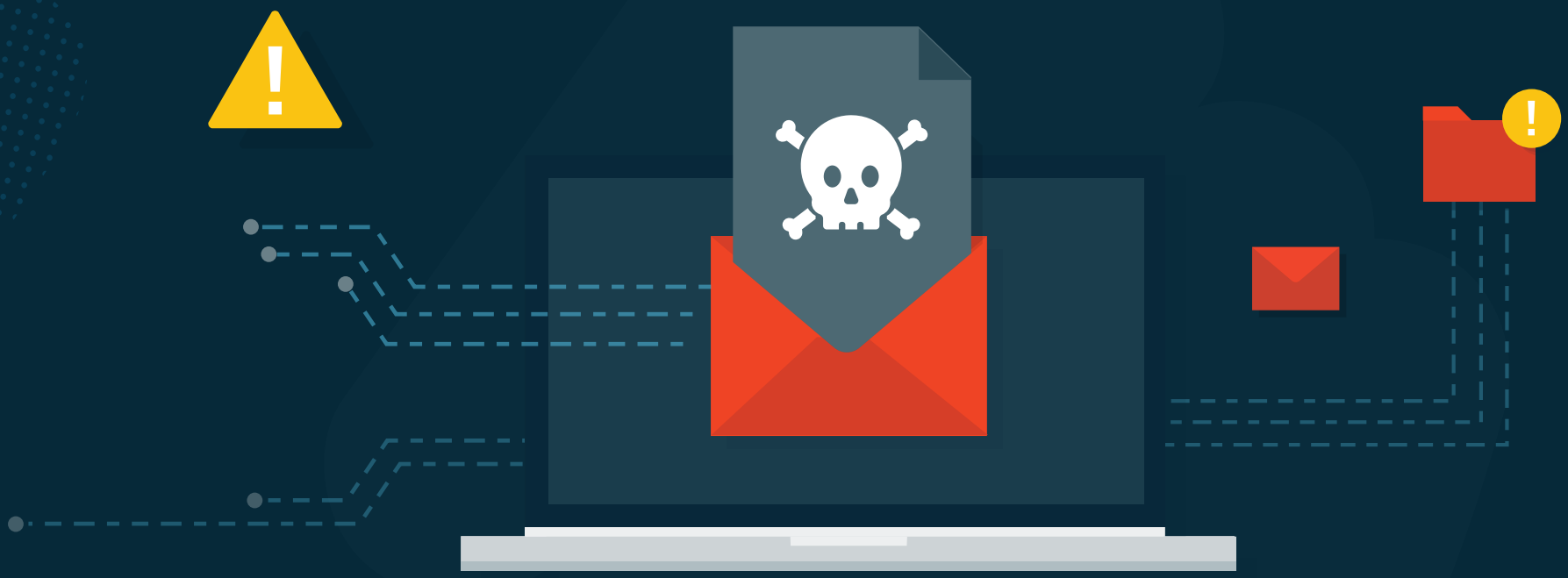
Report

datto



Datto's European State of the Channel

Ransomware Report

Follow us on Twitter: **@Datto**

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

About the Report

Datto's State of the Channel Ransomware Report is comprised of statistics pulled from a survey of nearly 300 managed service providers (MSPs), our partners and customers, across Europe. 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, 84% of MSPs report ransomware attacks against customers, which is higher than all other continents.
- **The average managed service providers (MSPs) report ~5 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 from 22%, year-over-year), which is higher than the global average of 35%.
- **The problem is bigger than we know, as a startling number of attacks go unreported.** MSPs report that only 16% of ransomware attacks are reported to the authorities.
- **SMBs are largely in the dark about the frequency and severity of ransomware attacks.** Nearly 86% of MSPs are "highly concerned" about the ransomware threat and 24% report their SMB clients feel the same.
- **Lack of cyber security 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, 67% of MSPs report victimised clients experienced a loss of business productivity. More than half report clients experienced business-threatening downtime.
- **The cost of business downtime is over 12X greater than the cost of the ransom requested.** MSPs report the average requested ransom for SMBs is ~$2,600 while the average cost of downtime related to a ransomware attack is ~$33,200. This exceeds the global rate where the cost of downtime is 10x greater than the average ransom requested.
- **European MSPs report Windows as the most targeted system by hackers.** They are also seeing a rise in attacks on Apple and Android systems.
- **Ransomware infections in the cloud continue to increase year-over-year.** Of MSPs that report cloud-based malware infections, 49% 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 91% 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 24% of MSPs
report SMBs "highly concerned" about ransomware.

86% 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)

84% of MSPs report clients struck by ransomware

58% of MSPs report clients struck by viruses

51% of MSPs report clients struck by adware

44% of MSPs report clients struck by spyware

43% of MSPs report clients struck by trojan horses

26% of MSPs report clients struck by cryptojacking

22% of MSPs report clients struck by rootkits

18% of MSPs report clients struck by worms

9% of MSPs report clients struck by keyloggers

Ransomware Attacks Continue to Climb Highest in Europe

From Q2 2016 - Q2 2018

84% of MSPs

report ransomware attacks against SMB customers. In the first 6 months of 2018 alone, **58% report ransomware attacks against clients.**

92% of MSPs

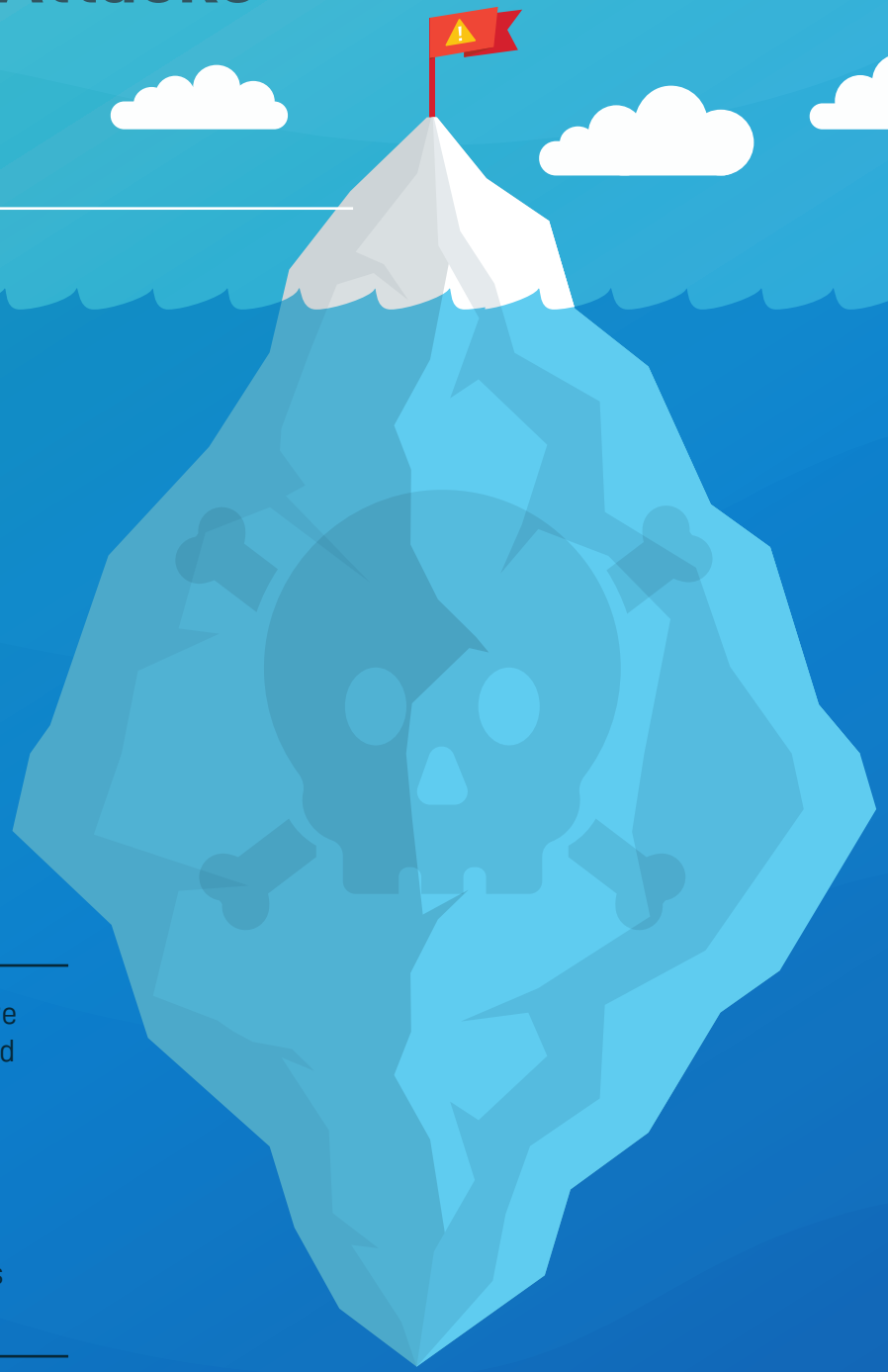
predict the number of **ransomware attacks will continue at current, or worse, rates.**

42% of MSPs

report clients suffered **multiple attacks** in the same day **(up from 22% in the previous year).**

Geo Trend: In Europe, 84% of MSPs report ransomware attacks against SMB customers from Q2 2016-Q2 2018, which is higher than all other continents. Additionally, 42% of European MSPs report multiple attacks against clients in a single day, which is higher than the global average of 35%.

On Average, MSPs Report ~5 Attacks Against Clients Per Year



But only about

16%

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

Geo Trend: Many countries and regions are passing laws to require companies to report data breaches to the 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

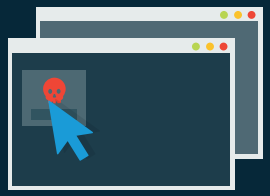
It's likely that the number of reported attacks will increase as laws like these are adopted around the world.

End User Error is the Common Denominator

Top Ransomware Delivery Methods:

50% of MSPs
Report Phishing Emails

44% of MSPs
Report Malicious Websites/Web Ads



16% of MSPs
Report Clickbait

Top Cyber Security Vulnerabilities:

42% of MSPs
Report Lack of End User Cyber Security Training

34% of MSPs
Report Poor User Practices/Gullibility

19% of MSPs
Report Weak Passwords/Access Management

From human error, to disgruntled employees, to lack of sophisticated protection, there are countless avenues ransomware can take to infiltrate small businesses around Europe. It's critical that those businesses recognize this imminent threat and face it head on with user education, investment in a layered preventative approach, and a reliable business continuity solution to recover data quickly, should the business become infected.

- Tim Walker, Managing Director, Aura Technology

Ransomware Attacks Are Costly

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

67% of MSPs report loss of business productivity

54% of MSPs report business-threatening downtime

46% of MSPs report data and/or device was lost

46% of MSPs report infection spread to other devices on the network

29% of MSPs report decreased customer profitability

28% of MSPs report damaged reputations

23% of MSPs report stolen data

22% of MSPs report paid a ransom and recovered the data

15% of MSPs report failure to meet SLA requirements

13% of MSPs report ransomware remained on system, struck again!

9% of MSPs report paid a ransom, data was never released

8% of MSPs report failure to achieve regulatory compliance

NHS Crippled by WannaCry Ransomware Attack

In 2017, the WannaCry ransomware attack hit 150 countries worldwide. In the United Kingdom, the National Health Service (NHS) suffered the biggest impact, with over 86 trusts, 603 primary care, and 565 general practitioner offices affected. Vital medical machinery was unable to be used and systems were locked, resulting in thousands of cancelled appointments and staff unable to perform daily duties. In just seven days, losses reached roughly £19m. In October of 2018, these costs were estimated to have reached £92m. Over the next three years, the government has committed to spending £150 million on new technology systems, along with a newly signed deal to upgrade local NHS computers to Microsoft 10.

May 12th 2017

WannaCry outbreak begins

NHS suffers biggest impact in the U.K.

86 trusts, 603 primary care and 565 general practitioner surgeries affected

Over 19,000 appointments cancelled

May 19th 2017

IT costs and

£19m loss

in NHS output services

July 2017

Technical support costs reach

£72m

October 2018

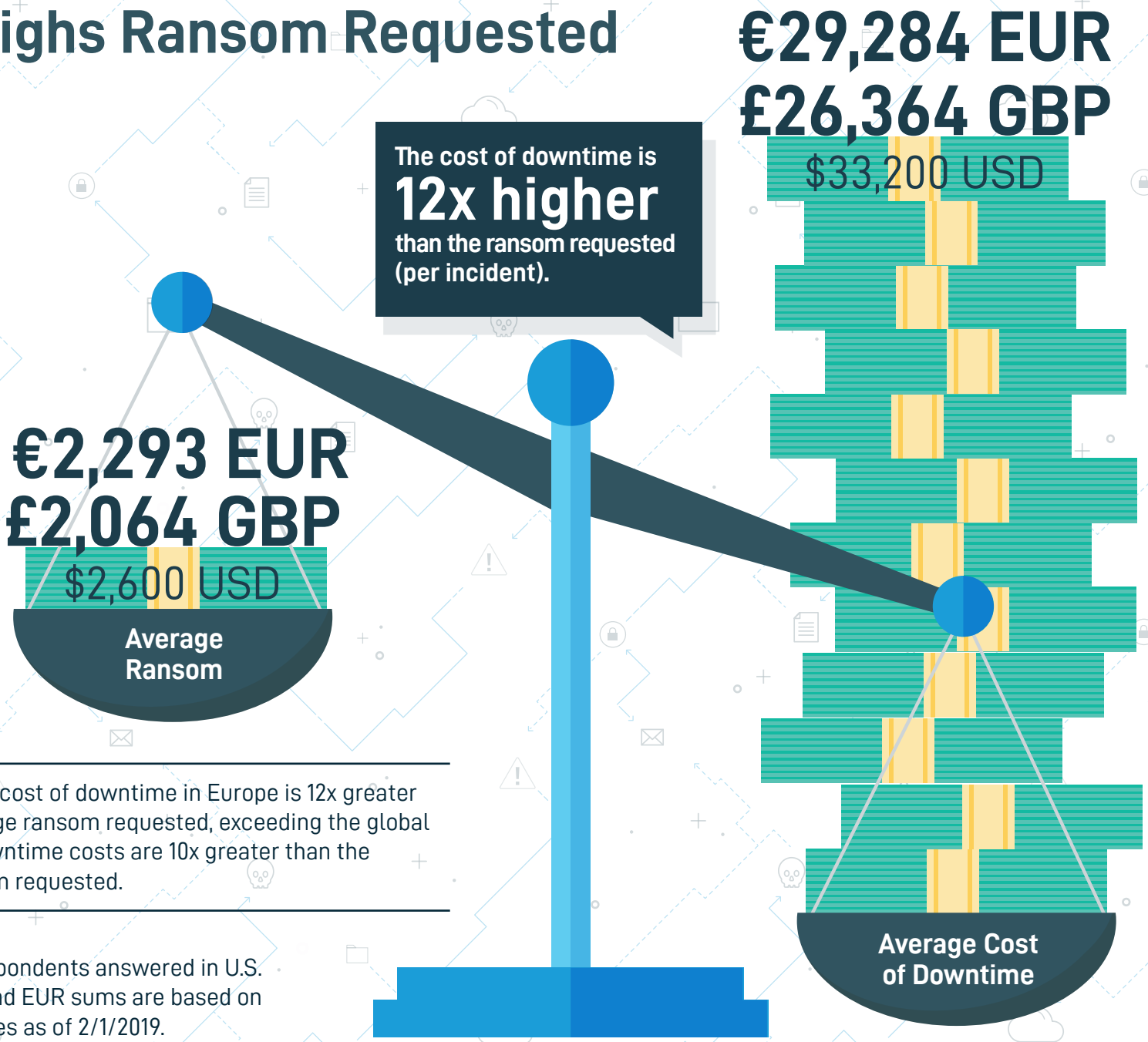
NHS estimated

£92m

in IT costs to restore data and systems from attack to date

Sources: Healthcare IT News, National Audit Office, BBC News, New Statesman, SKY News, Digital Health

Cost of Downtime Significantly Outweighs Ransom Requested



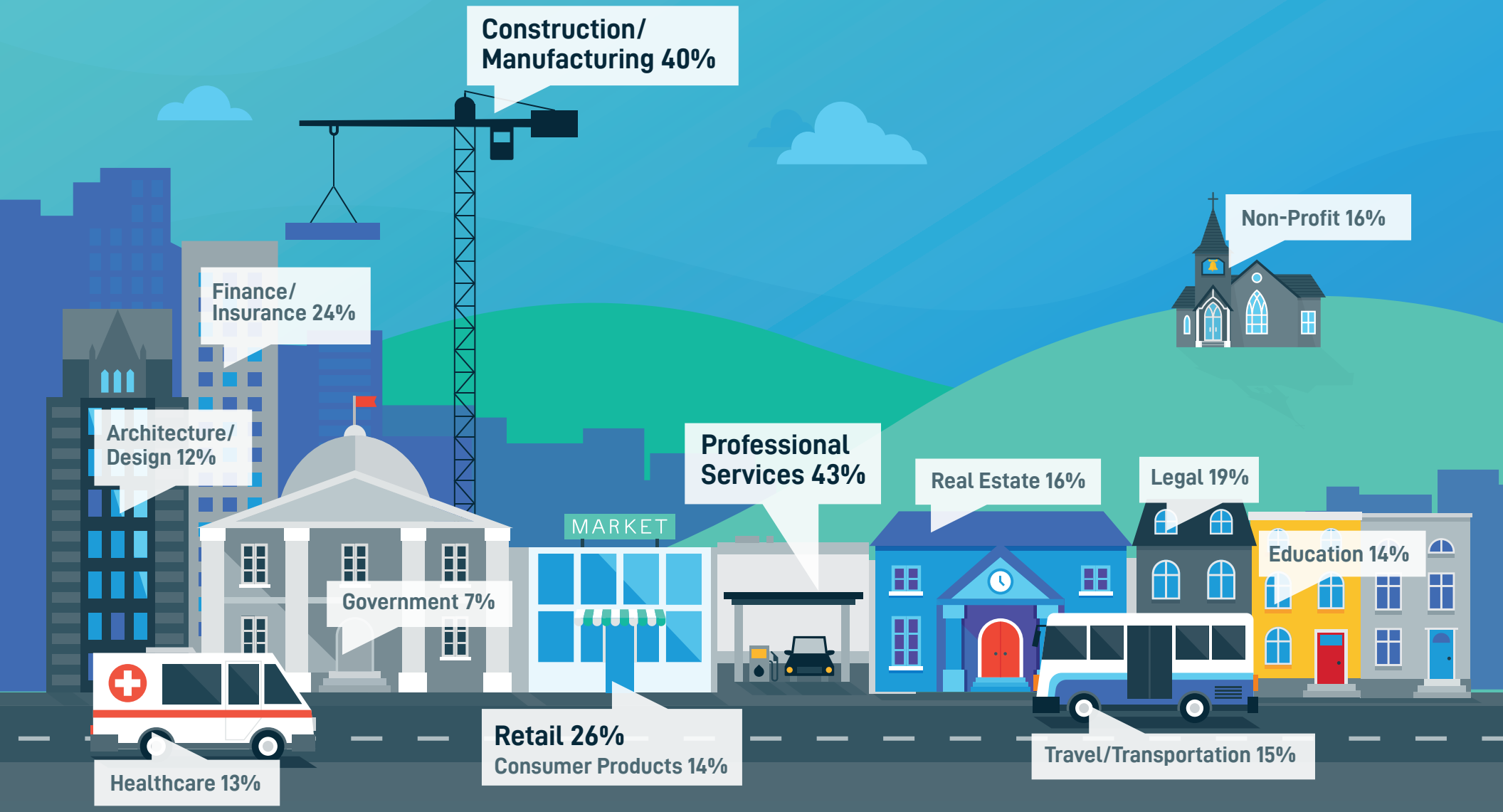
Geo Trend: The cost of downtime in Europe is 12x greater than the average ransom requested, exceeding the global rate where downtime costs are 10x greater than the average ransom requested.

*All survey respondents answered in U.S. dollars. GBP and EUR sums are based on conversion rates as of 2/1/2019.

.

No Industry is Safe from Ransomware

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



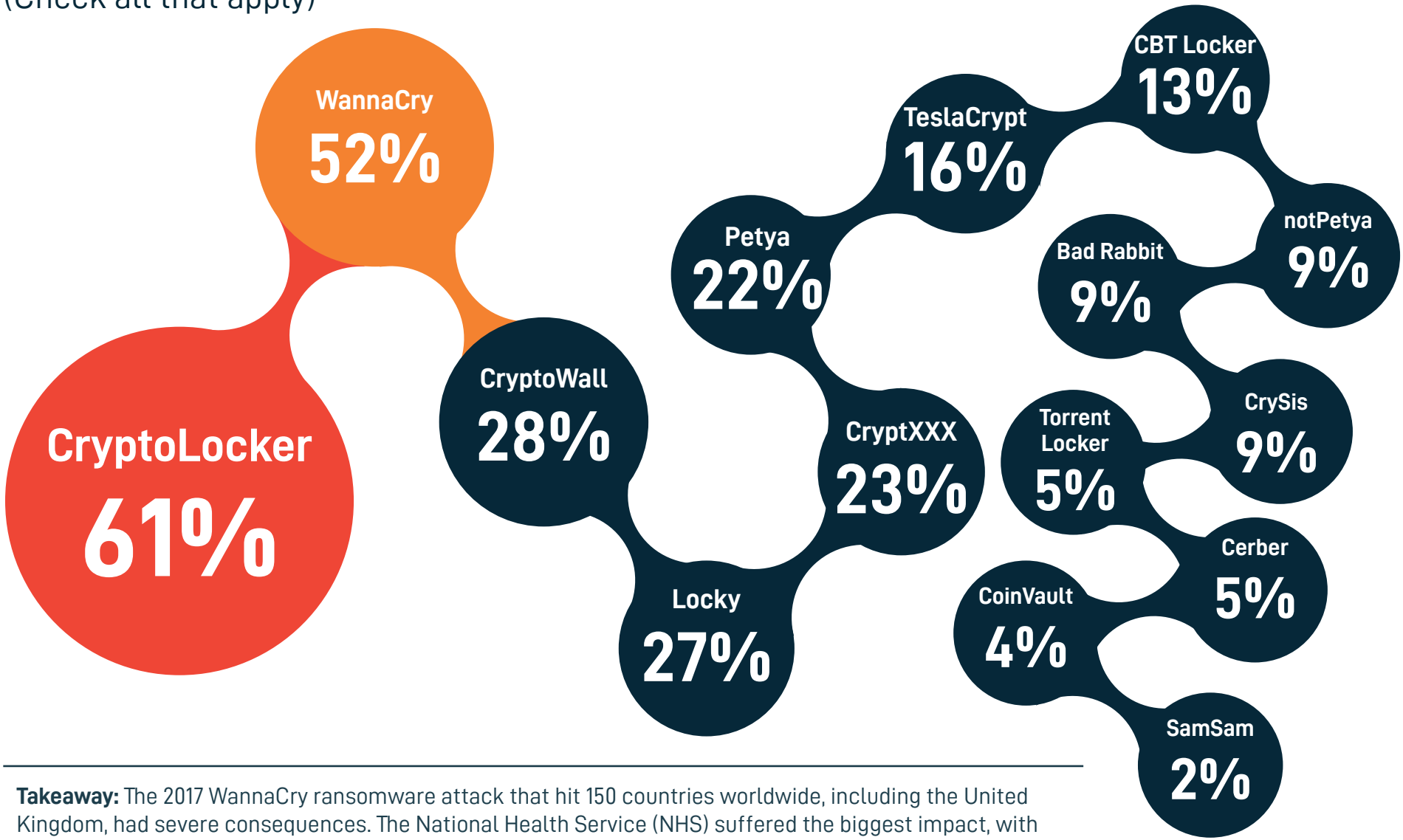
Media/Entertainment 8%
Government 7%

High Technology 7%
Energy/Utilities 5%

Telecom 5%

CryptoLocker and WannaCry Reign Supreme

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



Takeaway: The 2017 WannaCry ransomware attack that hit 150 countries worldwide, including the United Kingdom, had severe consequences. The National Health Service (NHS) suffered the biggest impact, with over 1000 trusts and NHS organisations affected. In just 7 days roughly £19m had been lost in output services and IT recovery costs. By October 2018, this number is believed to have escalated to £92m.

MSPs Report Windows as Most Targeted System by Ransomware

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

97%
Windows

6%
macOS

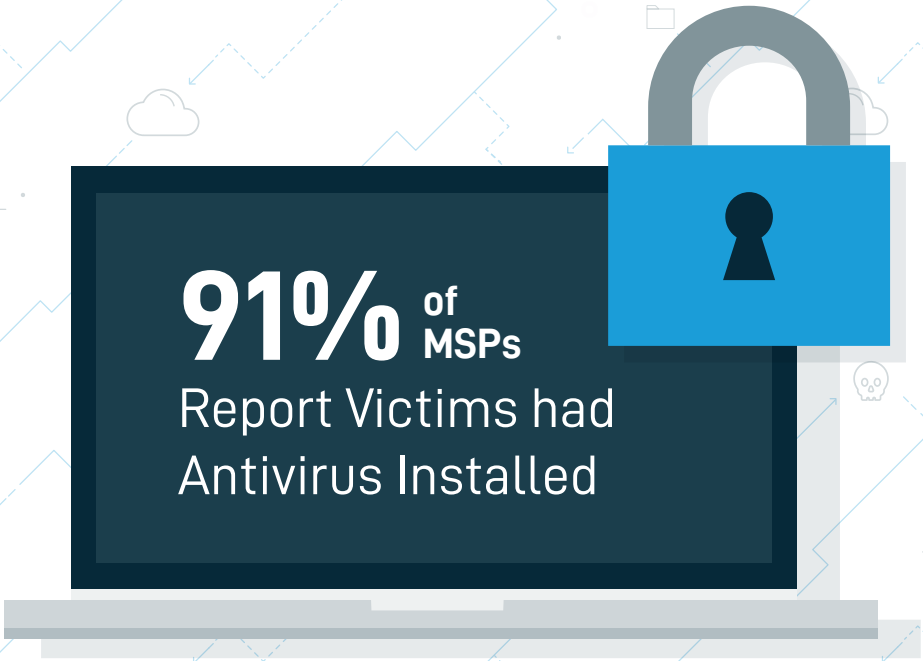
6%
Android

iOS

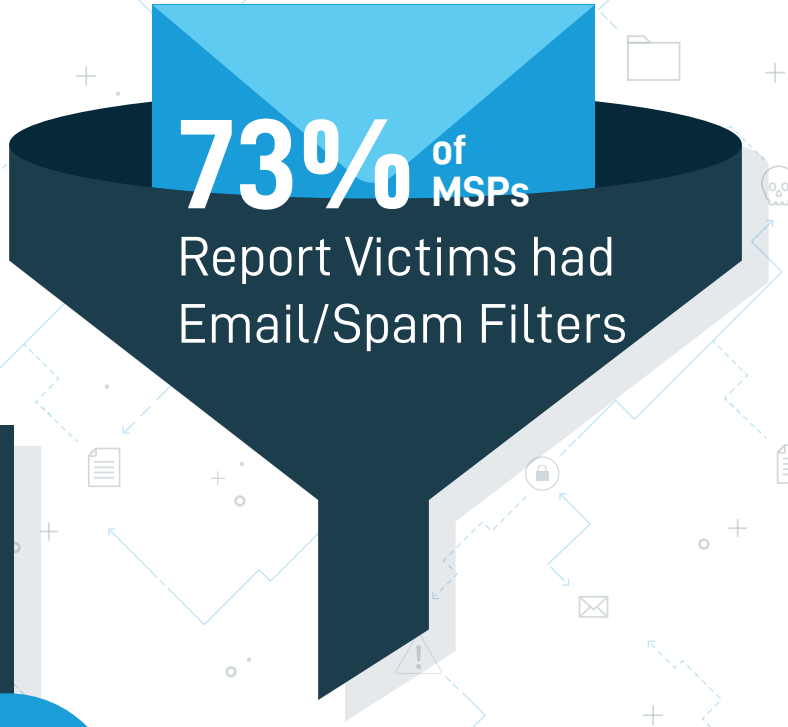
2%
iOS

Takeaway: European MSPs report Windows as the most targeted system by hackers, and are also seeing a rise in attacks on Apple and Android systems.

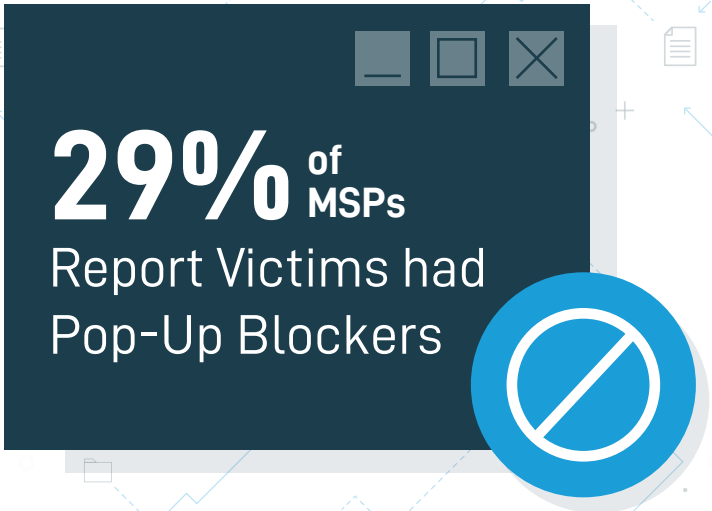
Nothing Can Prevent Ransomware



91% of MSPs
Report Victims had Antivirus Installed



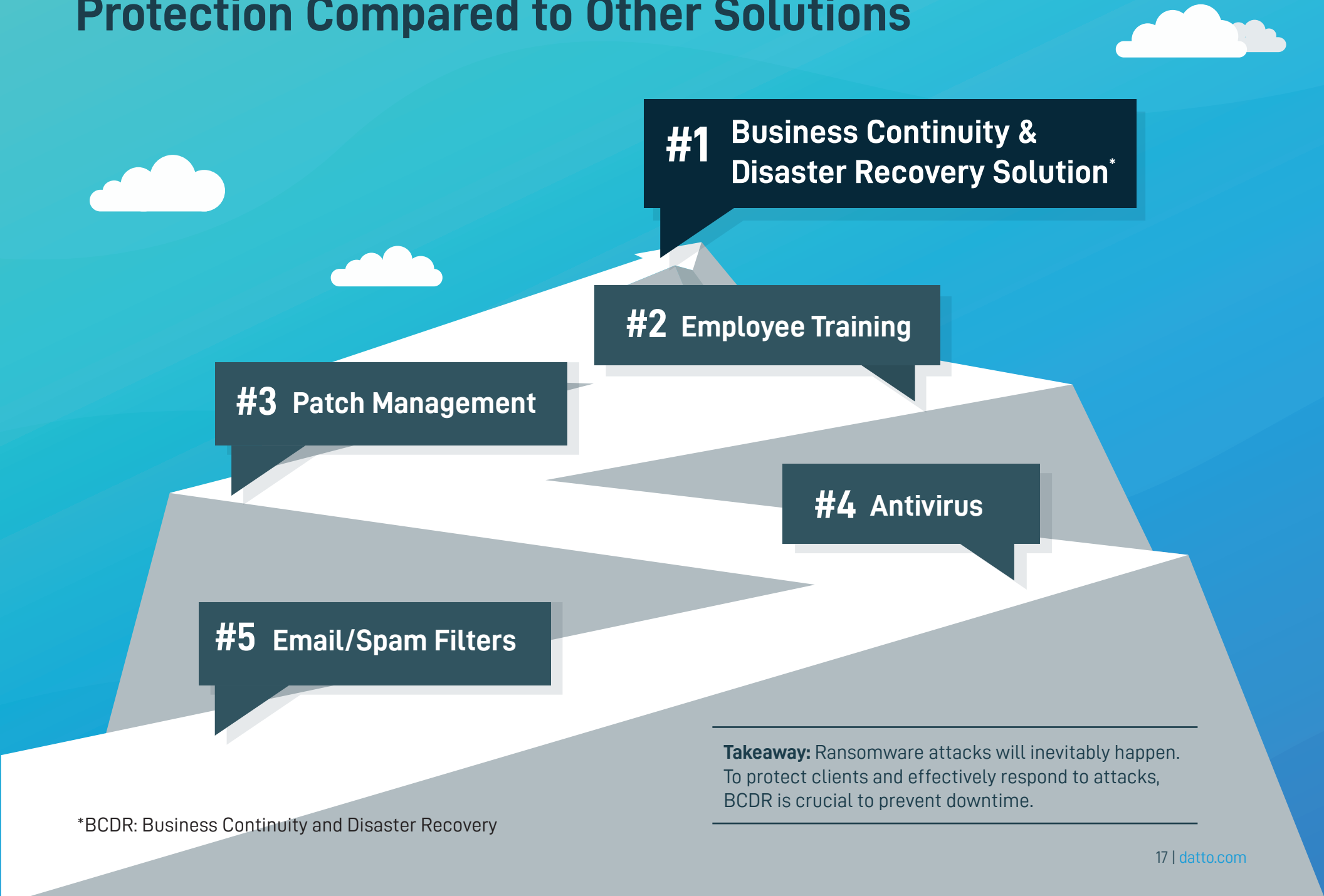
73% of MSPs
Report Victims had Email/Spam Filters



29% 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



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*†, 91%

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

Without BCDR, Only 50%

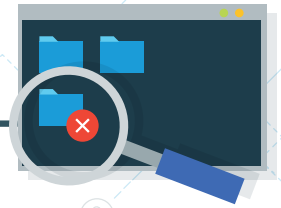
of MSPs report clients were able to do the same.

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.

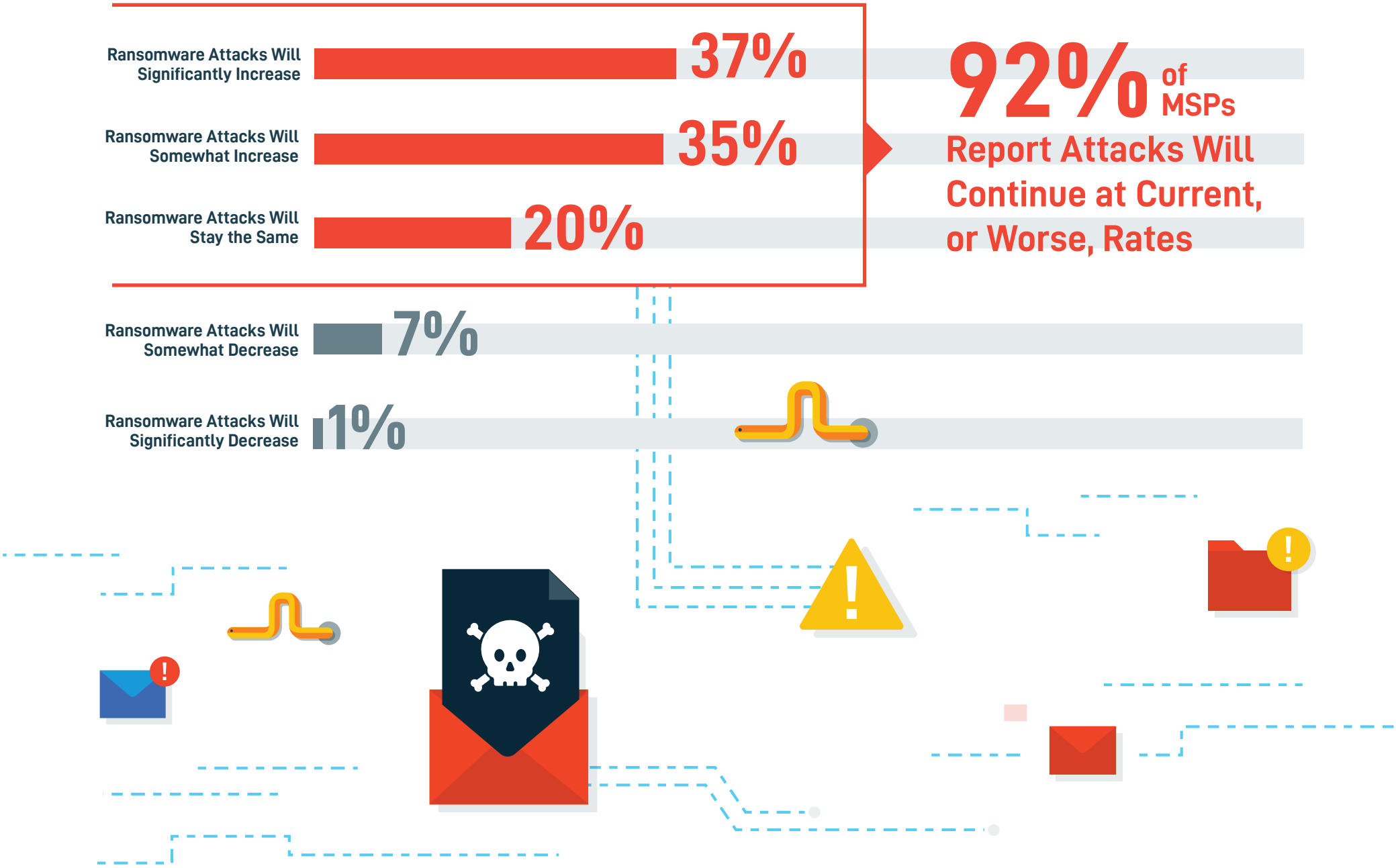
Cause Assessment

Understand how ransomware entered your client's system.

Recovery

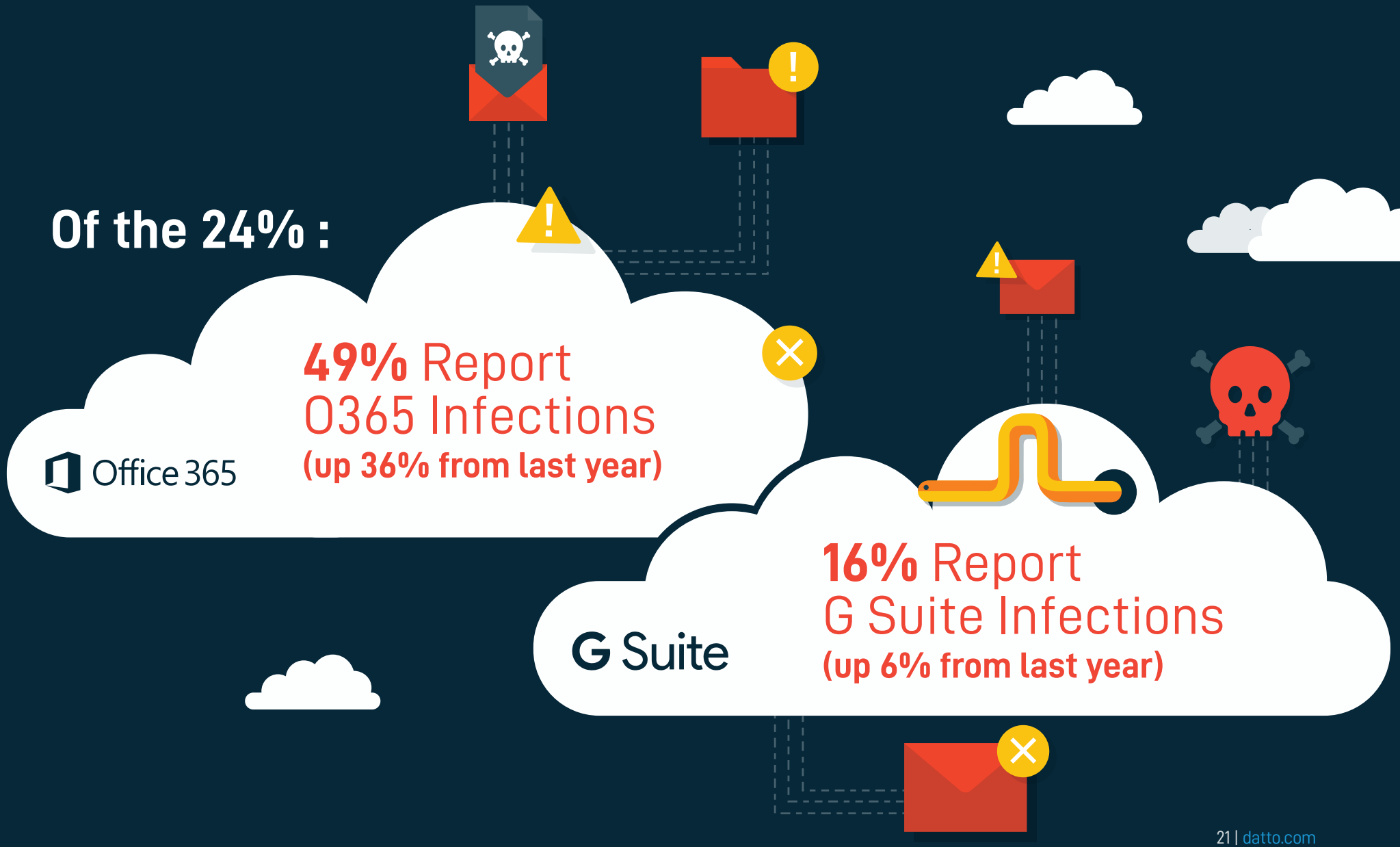
Keep your client working on a virtualised machine and/or quickly restore infected devices.

Majority of MSPs Report: Ransomware is Here to Stay



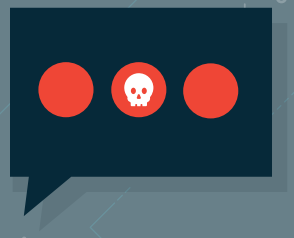
Ransomware Will Creep into the Cloud

24% of MSPs have seen ransomware attacks in SaaS applications

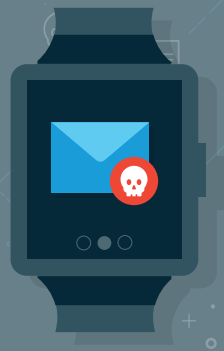


Ransomware of the Future Gets Personal

57% of MSPs
Predict Ransomware Will Target
IOT Devices



56% of MSPs
Predict Ransomware Will Target
Social Media Accounts

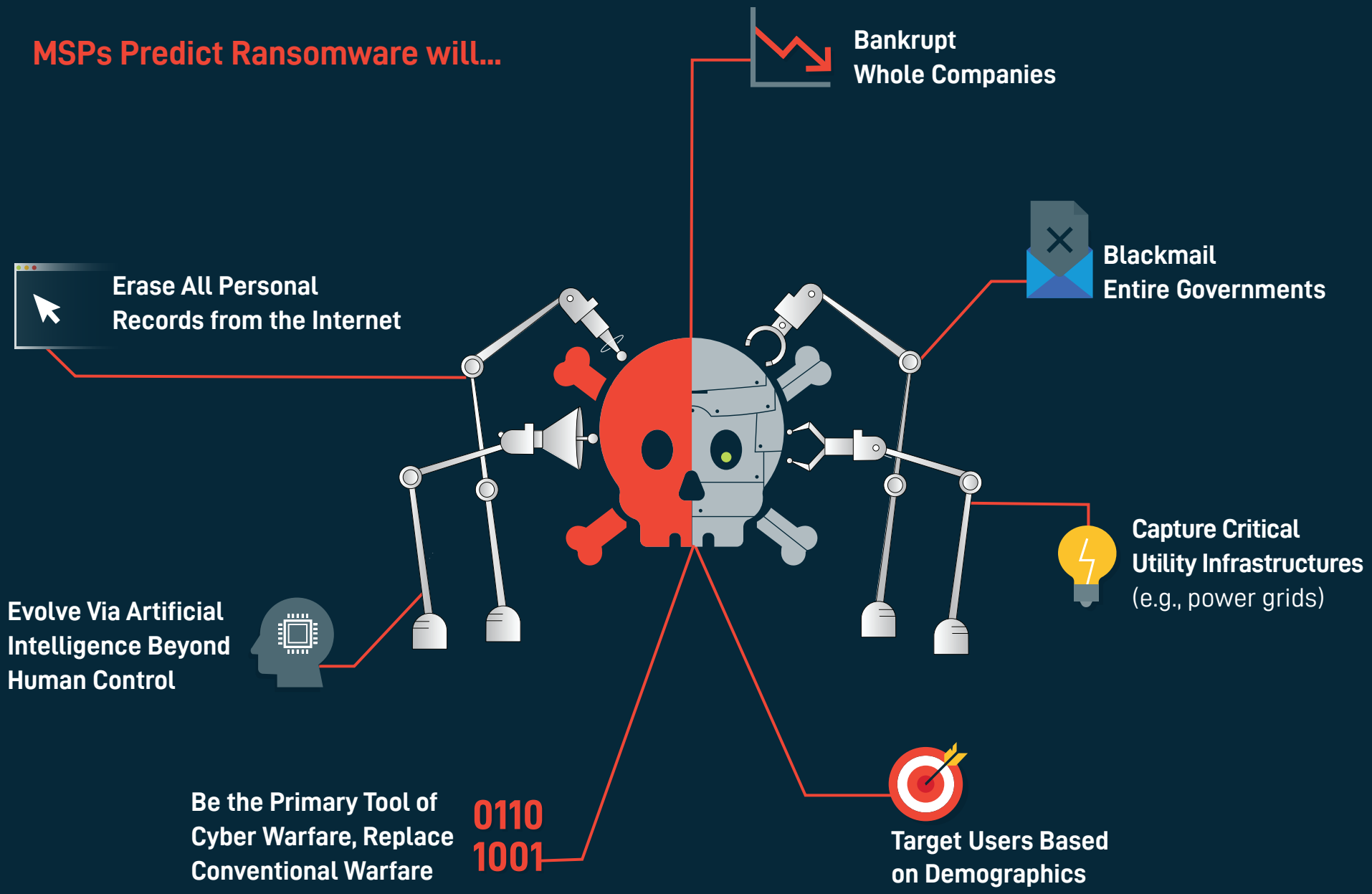


51% of MSPs
Predict Ransomware Will Target
Wearables
(e.g., smartwatches)

39% of MSPs
Predict Ransomware Will Target
Self Driving Cars

34% of MSPs
Predict Ransomware Will Target
Medical Devices
(e.g., insulin pumps, pacemakers)

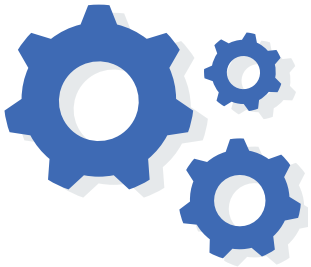
Ransomware Will Wreak Havoc Everywhere



Final Takeaways

Businesses must prepare the front line of defense: your employees. Today's companies must provide regular and mandatory cyber security 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.



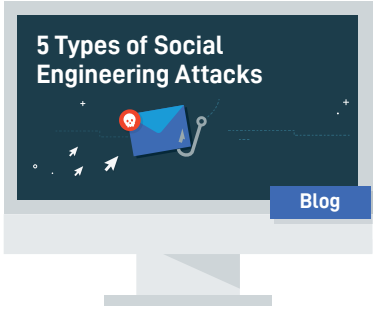
Businesses must ensure business continuity with BCDR. There is no sure fire way of preventing ransomware. Instead, businesses should focus on how to maintain operations despite a ransomware attack. One way to do this is a solid, fast and reliable business continuity and disaster recovery solution.

Businesses need a dedicated 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 a Managed Service Provider (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 Employee



Ransomware Survivor Stories

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 defense 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.