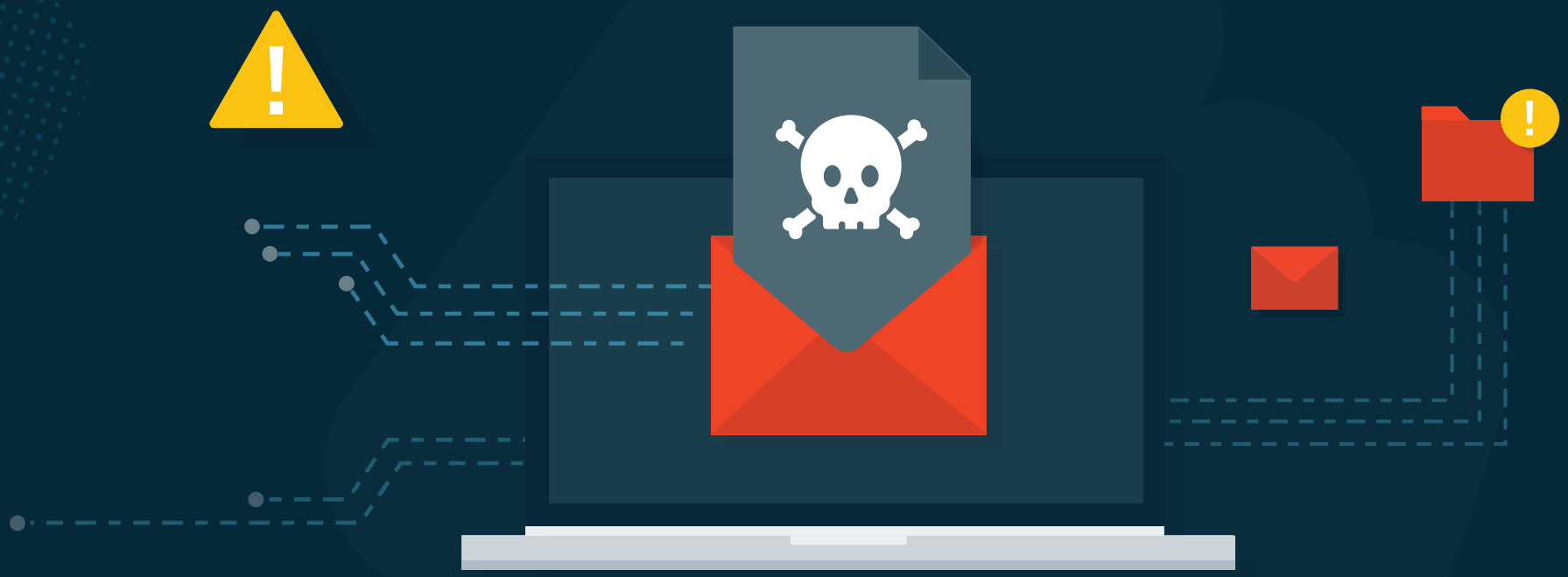
Report

SWK
NETWORK SERVICES



Datto's State of the Channel
Ransomware Report

About the Report

The State of the Channel Ransomware Report is comprised of statistics pulled from a survey of 2,400+ managed service providers (MSPs), Datto partners and customers, 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.

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

Key Findings

- **Ransomware remains a massive threat to small-to-mid-sized businesses (SMBs).** From Q2 2016 - Q2 2018, 79% of MSPs report ransomware attacks against customers. In the first 6 months of 2018 alone, 55% 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 5 of these attacks within their client base per year.** In the first half of 2018, an alarming 35% of MSPs report clients suffered multiple attacks in a single day (up from 26%, 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 4 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 36% 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, 67% of MSPs report victimized clients experienced a loss of business productivity. More than half report clients experienced business-threatening downtime.
- **The cost of business downtime is 10X greater than the cost of the ransom requested.** MSPs report the average requested ransom for SMBs is ~$4,300 while the average cost of downtime related to a ransomware attack is ~$46,800.
- **Having an Apple operating system isn't a silver bullet.** In the first 6 months of 2018, the number of MSPs reporting OS/iOS attacks increased by nearly 500% year-over-year.
- **Ransomware infections in the cloud continue to increase year-over-year.** Of MSPs that report cloud-based malware infections, nearly 50% 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 90% report that victimized clients with Datto BCDR in place fully recovered from the attack in 24 hours, or less.

Most SMBs Unaware of Ransomware Risk

Only 36% 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)

79% of MSPs report clients struck by ransomware

63% of MSPs report clients struck by viruses

58% of MSPs report clients struck by adware

58% of MSPs report clients struck by spyware

38% of MSPs report clients struck by trojan horses

28% of MSPs report clients struck by cryptojacking

26% of MSPs report clients struck by rootkits

20% of MSPs report clients struck by worms

14% of MSPs report clients struck by keyloggers

Ransomware Attacks Continue to Climb

From Q2 2016 - Q2 2018

79% of MSPs

report ransomware attacks against SMBs. In the first half of 2018 alone, **55% report attacks against clients.**

92% of MSPs

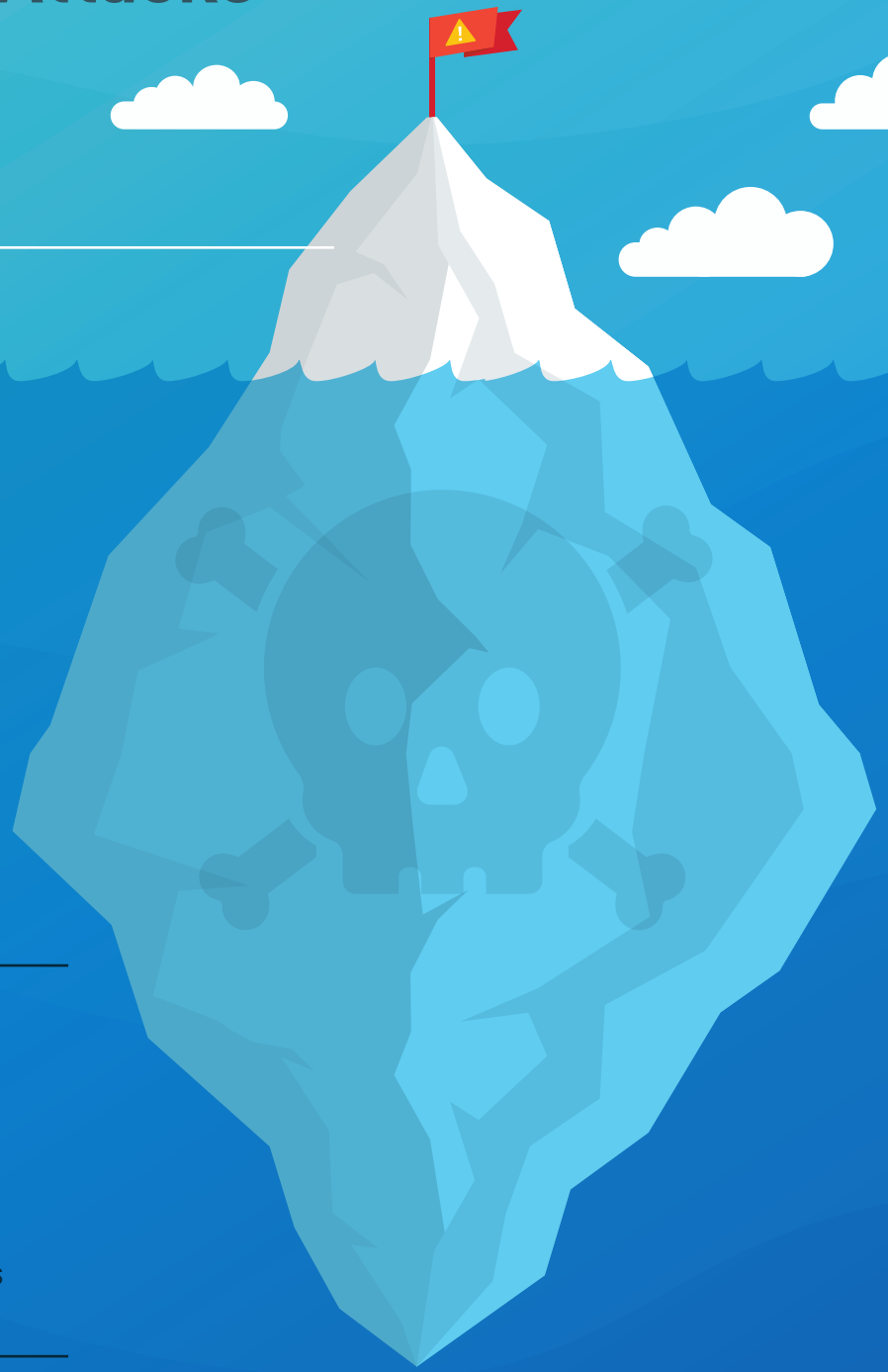
predict the number of **ransomware attacks will continue at current, or worse, rates.**

35% of MSPs

report clients suffered **multiple attacks** in the same day **(up from 26% 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 countries.

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



But only about

24%

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

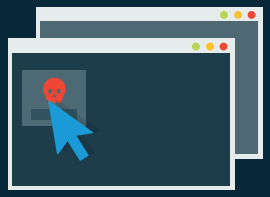
It's likely that the number of reported attacks will increase as laws like these are adopted around the world.

End User Error is the Common Denominator

Top Ransomware Delivery Methods:

66% of MSPs
Report Phishing Emails

24% of MSPs
Report Malicious Websites/Web Ads



21% of MSPs
Report Clickbait

Top Cybersecurity Vulnerabilities:

33% of MSPs
Report Lack of End User Cybersecurity Training

28% of MSPs
Report Poor User Practices/Gullibility

28% of MSPs
Report Weak Passwords/Access Management

The number one threat for SMB CEOs is thinking they are immune for some reason. They think they don't have anything the hackers want because it's not worth the price to protect themselves. Until something happens, then they're shocked by the cost to get everything back up and running. It's mind blowing.

- Michael Drake, CEO, masterIT

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

53% of MSPs report business-threatening downtime

43% of MSPs report data and/or device was lost

42% of MSPs report infection spread to other devices on the network

32% of MSPs report decreased customer profitability

30% of MSPs report clients paid a ransom and recovered the data

25% of MSPs report damaged reputations

22% of MSPs report stolen data

18% of MSPs report ransomware remained on system, struck again!

12% of MSPs report failure to meet SLA requirements

12% of MSPs report failure to achieve regulatory compliance

11% of MSPs report clients paid ransom but data was never released

City of Atlanta in the U.S. Paralyzed by Ransomware Attack

The city of Atlanta fell victim to a SamSam ransomware attack. For five days, numerous applications were crippled and city employees couldn't work from government issued devices. Systems affected included the ticketing system for the local police department and software used by the court system. The impact of the attack spanned far beyond government employees, impacting an estimated 6 million people who rely on city services.

March 22, 2018

SamSam Ransomware Hackers Demand

$51K Ransom

5 Days
Of Crippling Downtime

March 27, 2018

City Employees

Return to Work

June 6, 2018

Officials Request Additional

$9.5M

Recovery Budget
(Reuters)

August 6, 2018

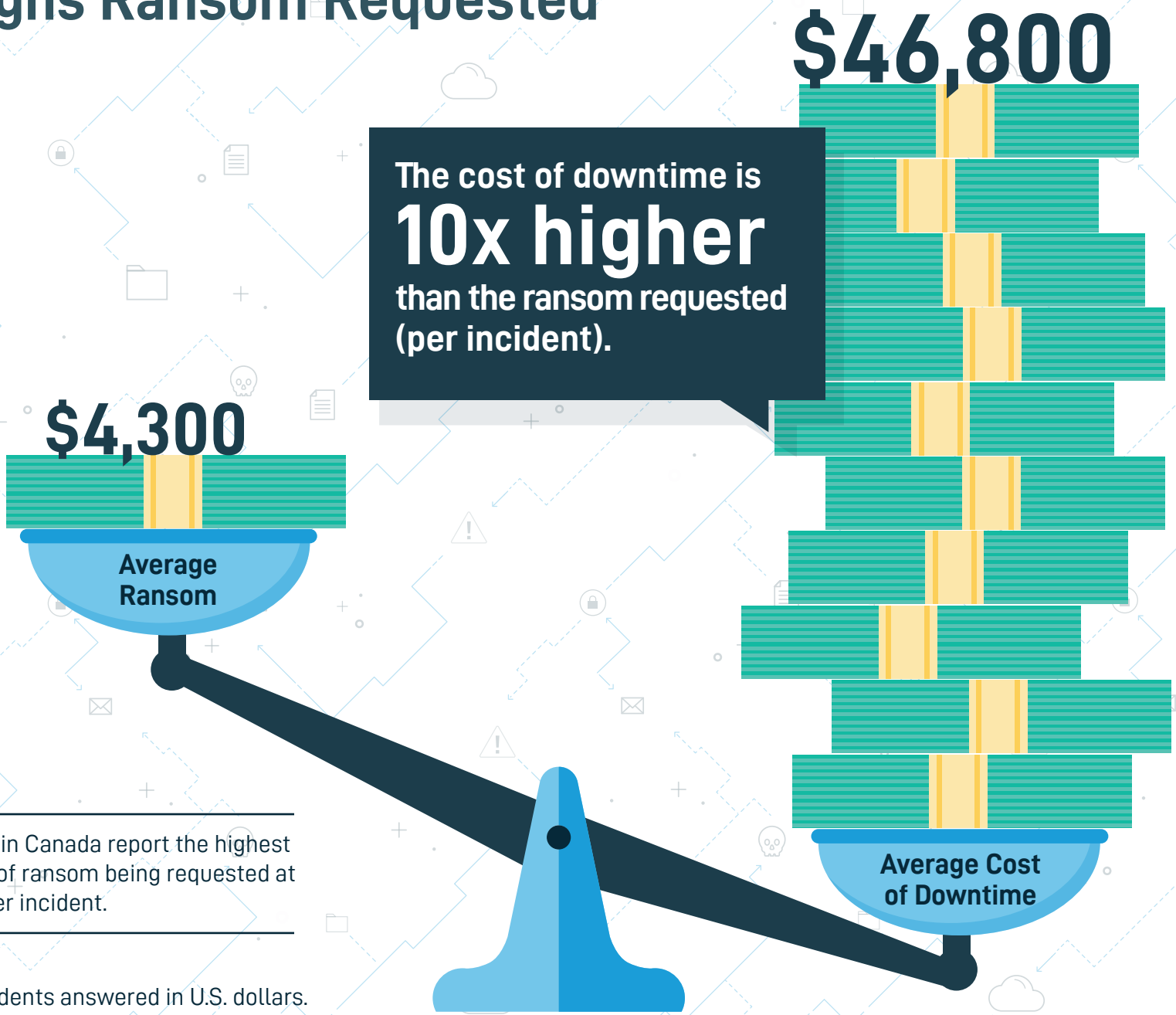
Total estimated cost of recovery reaches

$17M+

(AJC)

Sources: Reuters, The Atlanta Journal-Constitution

Cost of Downtime Significantly Outweighs Ransom Requested

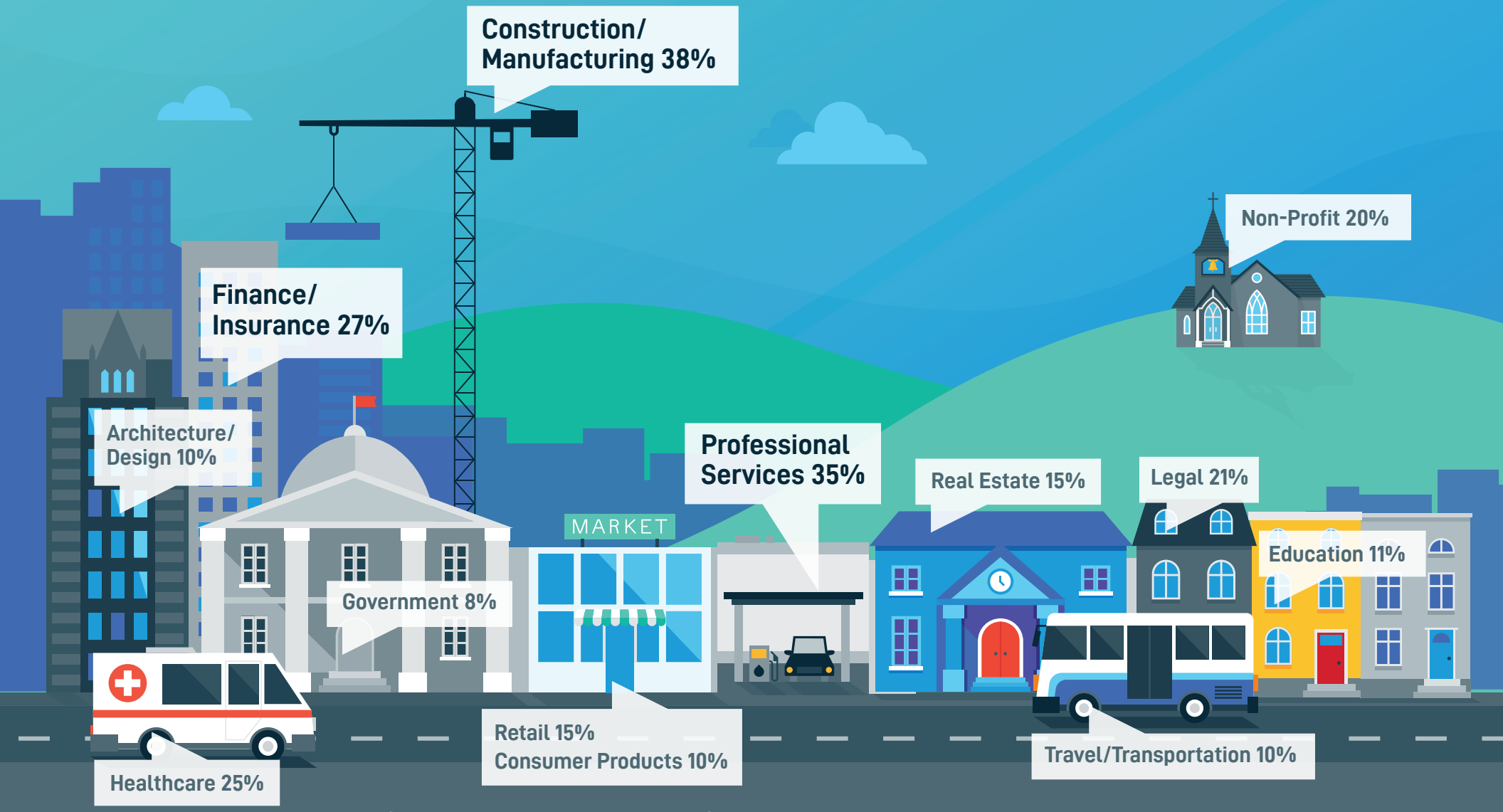


Geo Trend: MSPs in Canada report the highest average amount of ransom being requested at roughly $6,600, per incident.

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

No Industry is Safe from Ransomware

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



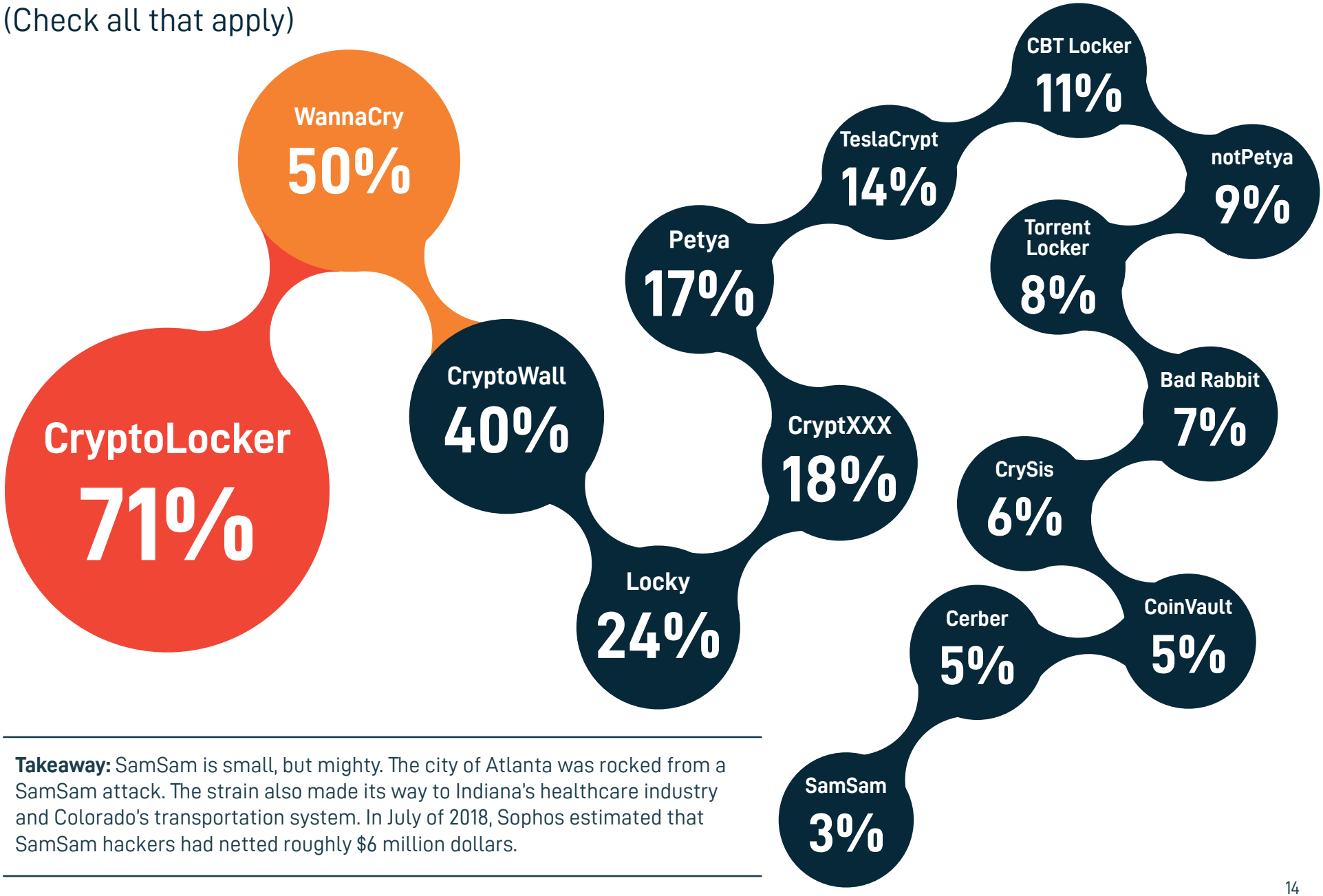
Media/Entertainment 6%
High Technology 5%

Energy/Utilities 5%
Telecom 3%

Agriculture 1%
Other 0.11%

CryptoLocker and WannaCry Reign Supreme

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



Takeaway: SamSam is small, but mighty. The city of Atlanta was rocked from a SamSam attack. The strain also made its way to Indiana's healthcare industry and Colorado's transportation system. In July of 2018, Sophos estimated that SamSam hackers had netted roughly $6 million dollars.

500% Increase in MSPs Reporting Apple OS Attacks

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

99%
Windows

Geo Trend: APAC suffers the highest rate of Android ransomware incidents globally, with 11% of MSPs reporting infections in that system.

9%
macOS

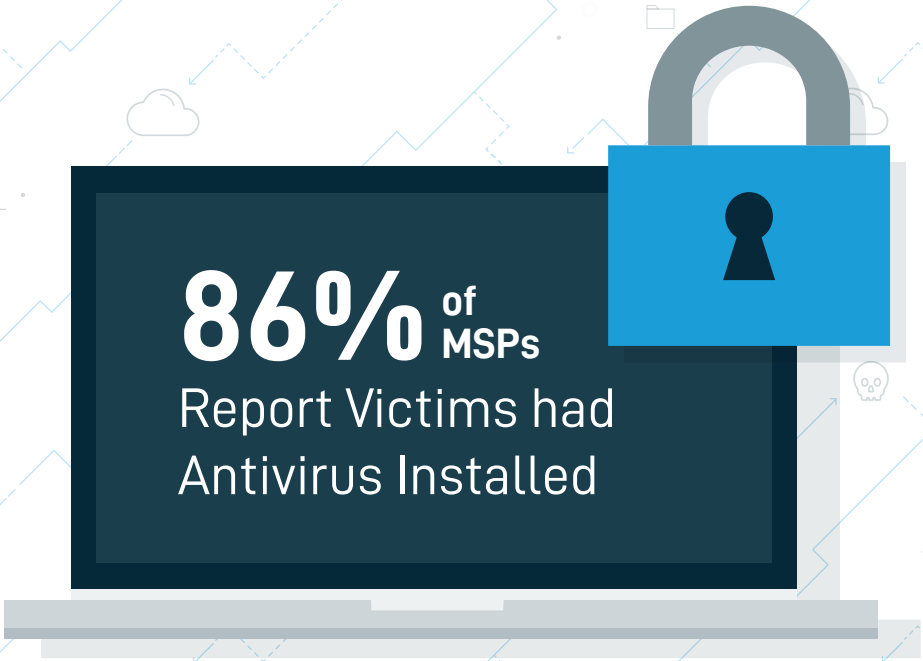
8%
Android

iOS

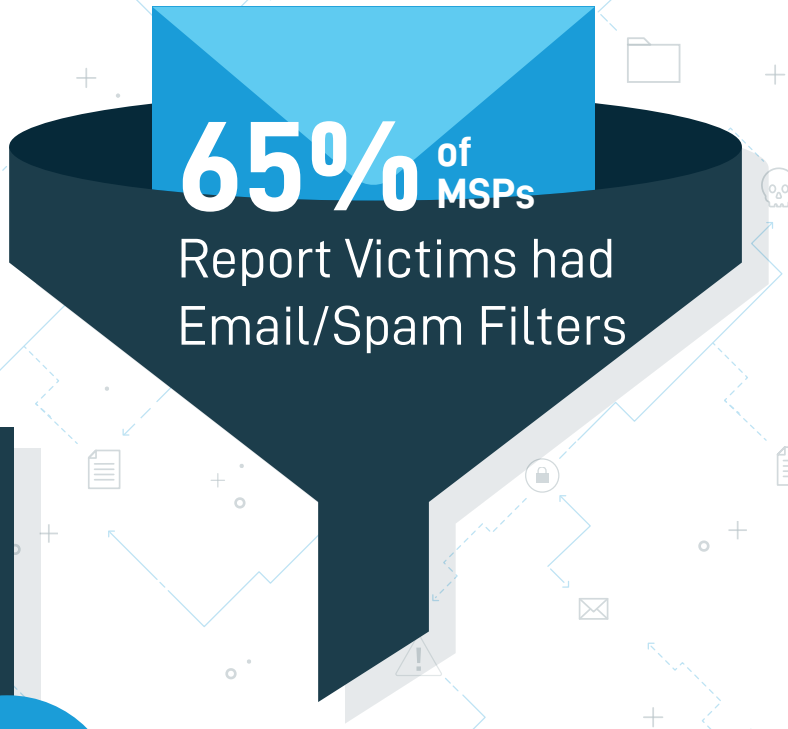
5%
iOS

Takeaway: Apple ransomware attacks are growing. The number of MSPs reporting OS/iOS attacks is **up nearly 500%** from last year.

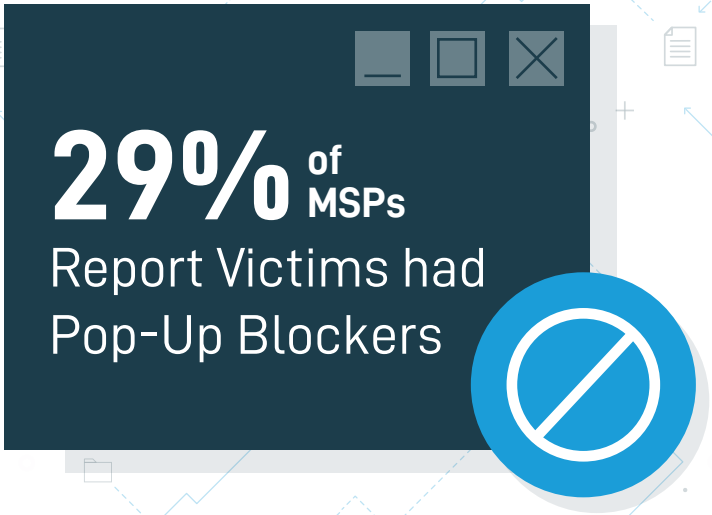
Nothing Can Prevent Ransomware



86% of MSPs Report Victims had Antivirus Installed



65% 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*†, 90%

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

Without BCDR, Only 60%

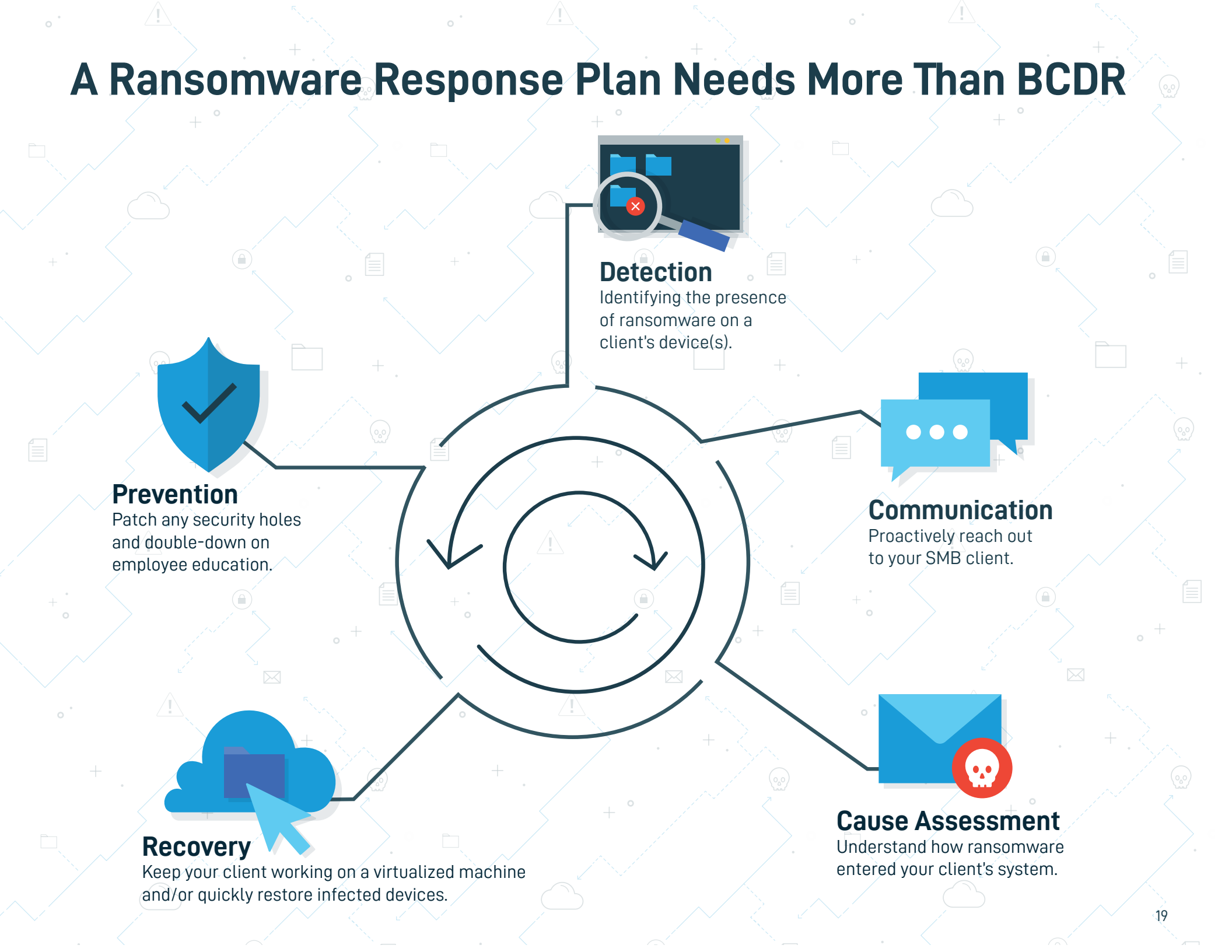
of MSPs report clients were able to do the same.

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).

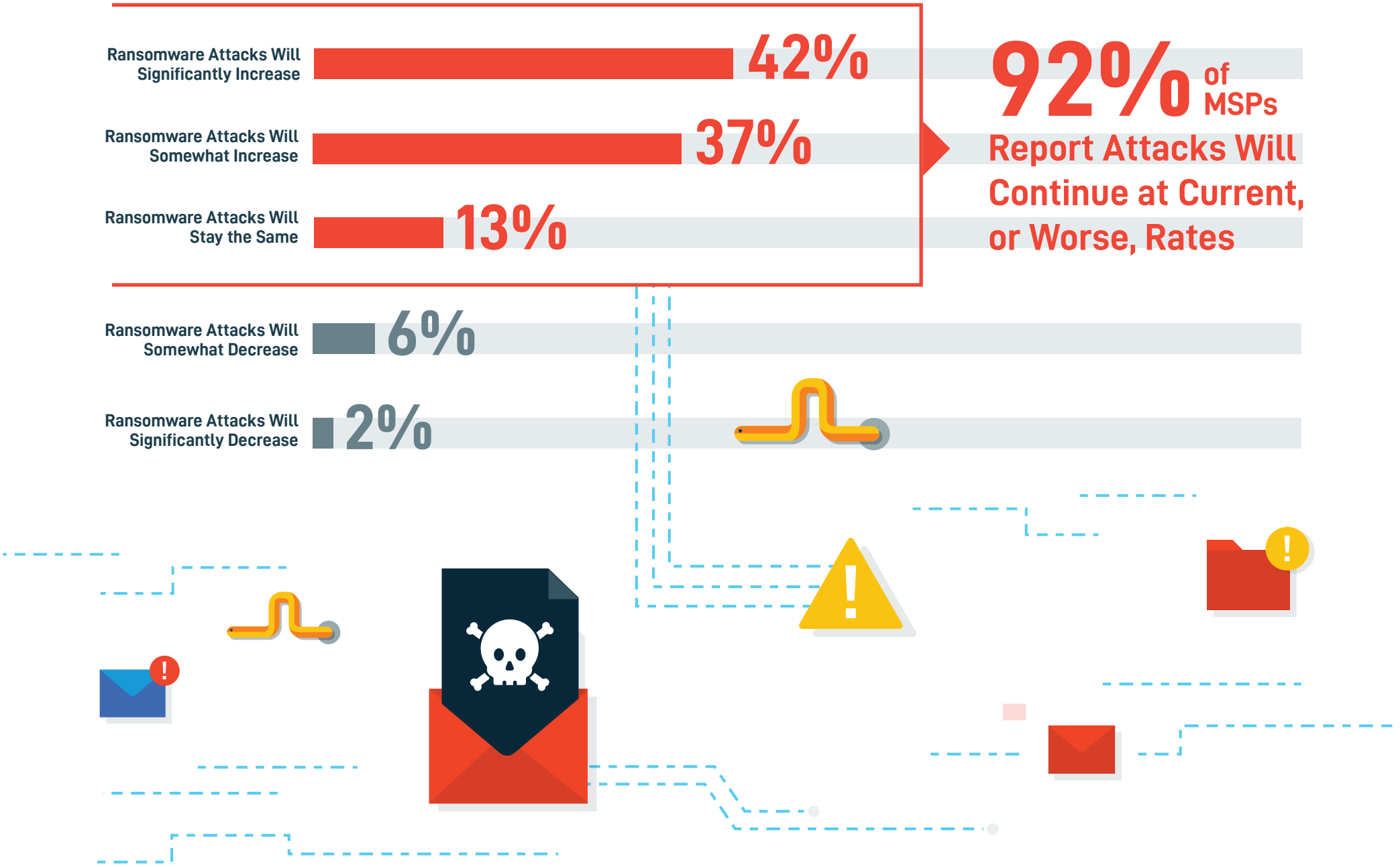
Communication
Proactively reach out to your SMB client.

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

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

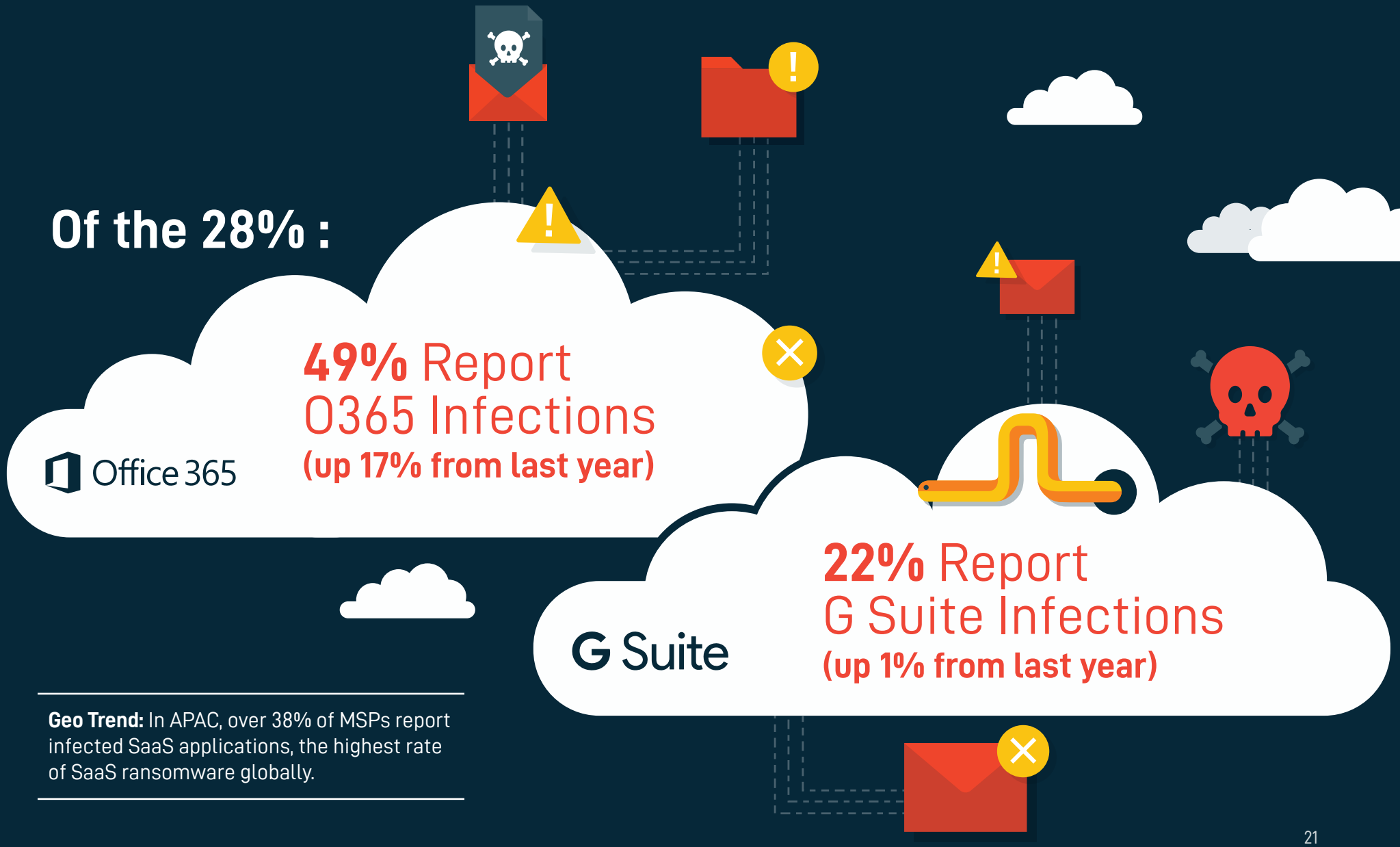
Prevention
Patch any security holes and double-down on employee education.

Majority of MSPs Report: Ransomware is Here to Stay



Ransomware Will Creep into the Cloud

28% of MSPs have seen ransomware attacks in SaaS applications (up 2% from last year)



Of the 28% :

Office 365

49% Report
O365 Infections
(up 17% from last year)

G Suite

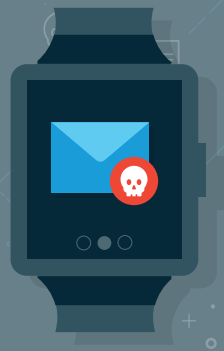
22% Report
G Suite Infections
(up 1% from last year)

Geo Trend: In APAC, over 38% of MSPs report infected SaaS applications, the highest rate of SaaS ransomware globally.

Ransomware of the Future Gets Personal

57% of MSPs
Predict Ransomware Will Target **Social Media Accounts**

54% of MSPs
Predict Ransomware Will Target
IOT Devices

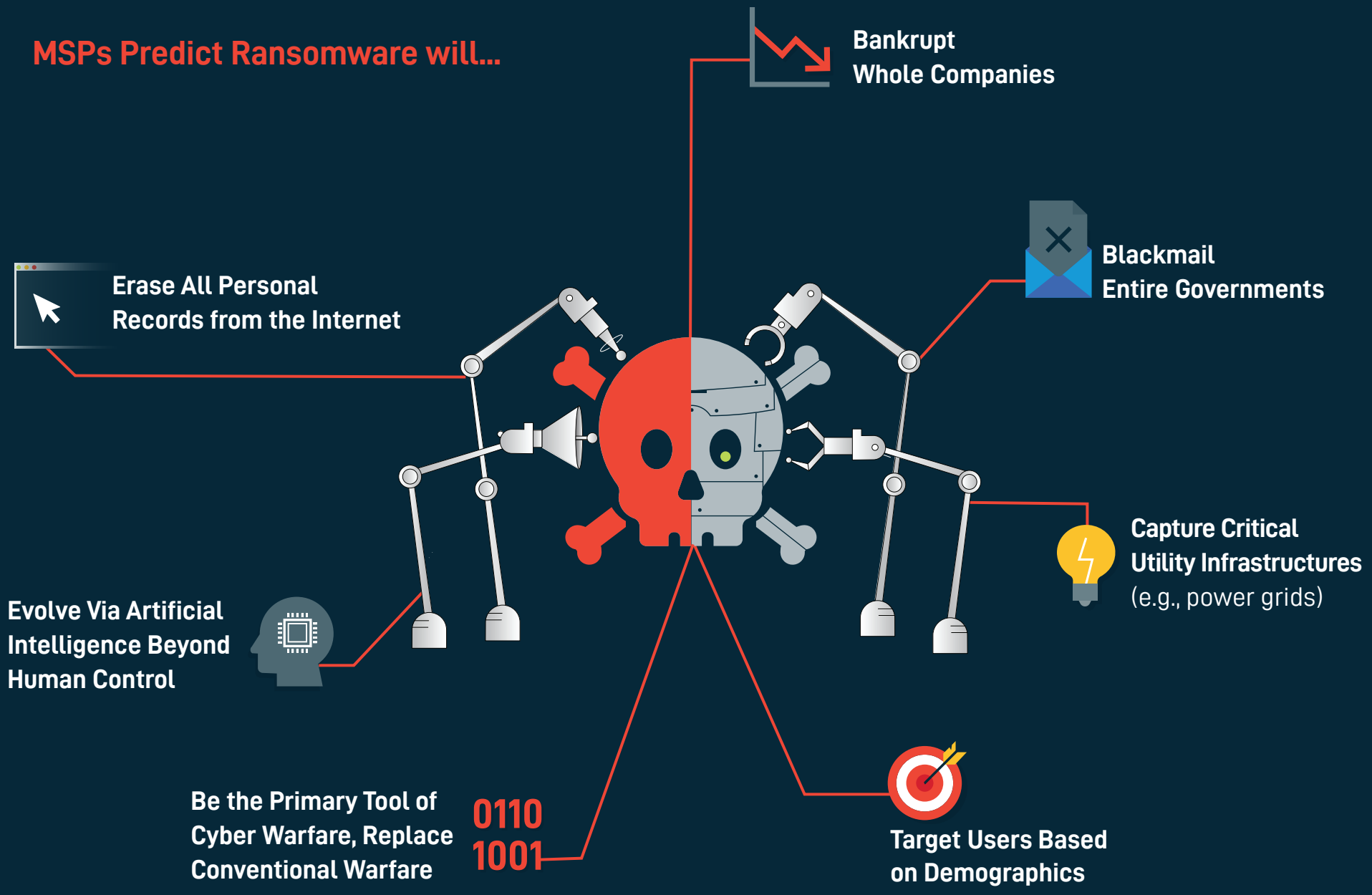


43% of MSPs
Predict Ransomware Will Target
Wearables
(e.g., smartwatches)

39% of MSPs
Predict Ransomware Will Target
Self Driving Cars

37% of MSPs
Predict Ransomware Will Target
Medical Devices
(e.g., insulin pumps, pacemakers)

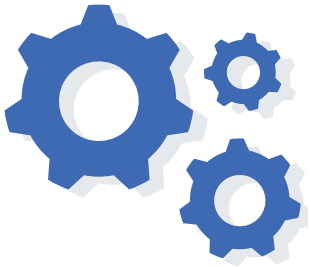
Ransomware Will Wreak Havoc Everywhere



Final Takeaways

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

For more information please contact:
SWK Network Services
Phone: 856-956-5800
Email: nwsinfo@swktech.com
SWK Technologies, Inc. | http://www.swknetworkservices.com
120 Eagle Rock Ave., Suite 330 East Hanover, NJ, 07936