REPORT

pch technologies

Datto's State of the Channel
Ransomware Report

ABOUT THIS REPORT

With survey findings gathered from 1,700+ Managed Service Providers (MSPs) serving 100,000+ small-to-mid-sized businesses (SMBs) around the globe, Datto's State of the Channel Ransomware 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.

This report covers the evolution of ransomware from Q2 2016 to Q2 2017.

KEY FINDINGS

- **Global ransomware attacks against small-to-mid-sized businesses (SMBs) soar.** An estimated 5 percent of global SMBs fell victim to a ransomware attack from Q2 2016-Q2 2017. According to 97 percent of managed service providers (MSPs), ransomware attacks are more frequent in 2017. Eighty-six percent cite SMB clients recently victimized by ransomware, 21 percent report six or more SMB attacks in the first half of 2017 alone.
- **Ransomware attacks will continue to thrive over the next two years.** According to 99 percent of MSPs, the frequency of SMB targeted attacks will continue to increase over the next two years.
- **More SMBs are reporting attacks to the authorities and less are paying the ransom.** Less than one in three ransomware attacks are reported by SMB victims to the authorities, a marked improvement from one in four incidents reported in 2016. Additionally, 35 percent report SMBs paid the ransom, down from 41% in 2016. The total cost of ransom paid to ransomware hackers in 2017 is $301M. Of those victims that pay up, 15 percent still never recover the data.
- **The ransom isn't what breaks the bank. The downtime and data loss cut the deepest.** As a result of a ransomware attack, 75% of MSPs report clients experienced business-threatening downtime.
- **Today's ransomware hackers are ruthless and greedy.** Nearly 30 percent of MSPs report a ransomware virus remained on an SMB's system after the first attack and struck again at a later time. One in three MSPs report ransomware encrypted an SMB's backup, making recovery even more complex.
- **CryptoLocker is still the most common variant attacking SMBs, but new and aggressive strains pop up every single day.** Nearly 85 percent of MSPs who've dealt with ransomware report seeing CryptoLocker. Additional common variants include CryptoWall, Locky and WannaCry, which is a new addition to the list.
- **No industry, operating system, cloud or device is safe from these attacks.** Among those industry verticals who are targeted most by ransomware attacks are Construction, Manufacturing and Professional Services. SaaS applications continue to be a growing target for ransomware attacks with Dropbox, Office 365 and G Suite most at risk. Mobile and tablet attacks are also on the rise.
- **When it comes to ransomware awareness, the majority are still in the dark.** While 90 percent of MSP respondents cited they are "highly concerned" about the business threat of ransomware, only 38 percent of SMB clients felt the same. This could be due to the lack of mandatory cybersecurity training across SMBs, which MSPs cite as the leading cause of ransomware infections.
- **Ransomware outsmarts today's top security solutions, so backup is essential.** MSPs are reporting successful infections despite SMBs having Anti-Virus Software, Email/Spam Filters, Ad Blockers, and regularly updated applications. The #1 most effective means for business protection from ransomware is a backup and disaster recovery (BDR) solution followed by cybersecurity training.
- **With a reliable backup and disaster recovery solution in place, the majority of SMBs will fully recover from a ransomware infection.** With a reliable backup and recovery solution (BDR) in place, 96% of MSPs report clients fully recover from ransomware attacks.

THE #1 CYBERSECURITY THREAT FOR BUSINESSES TODAY: RANSOMWARE

ACROSS THE GLOBE, AN ESTIMATED

5% OF SMALL-TO-MID-SIZED BUSINESSES (SMBs)

FELL VICTIM TO RANSOMWARE FROM 2016–2017

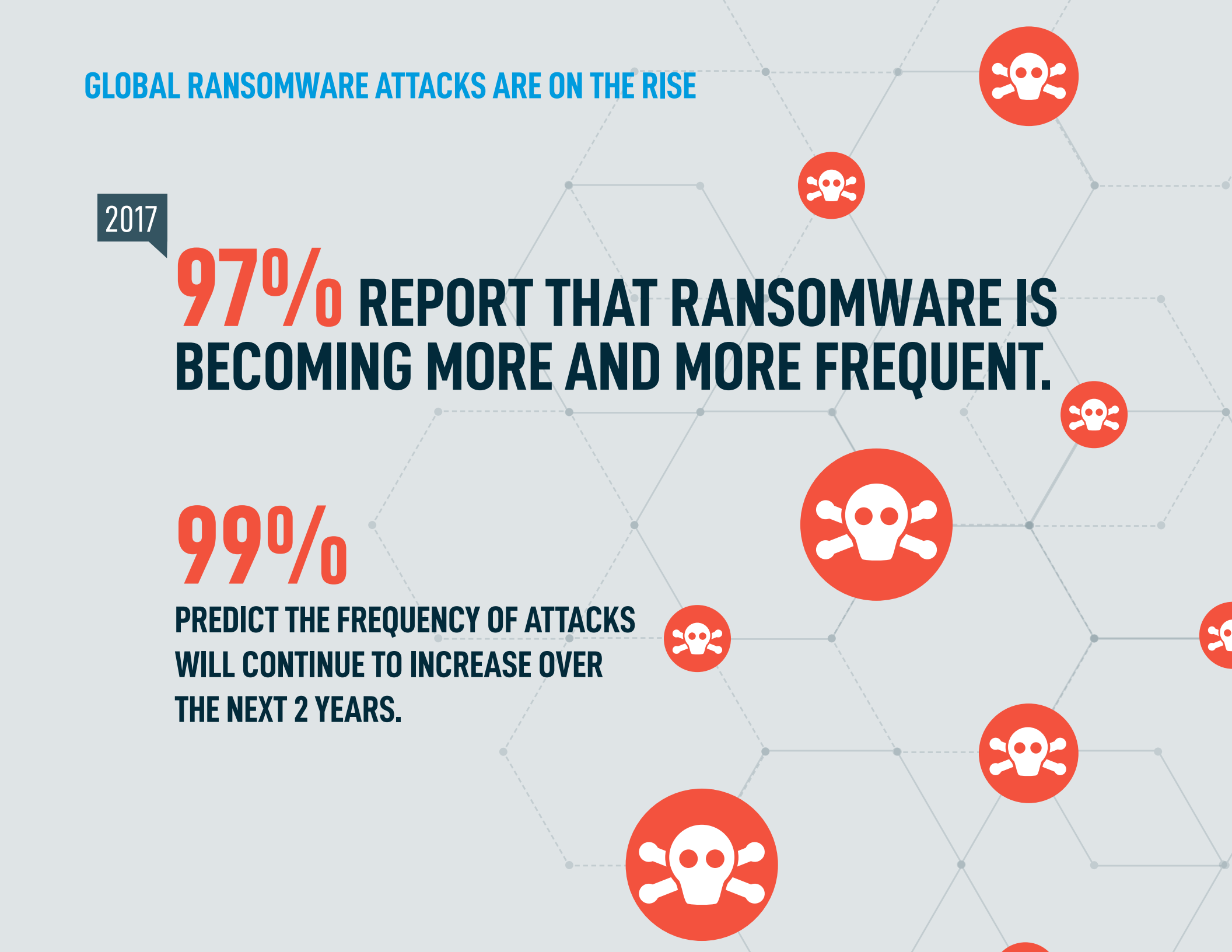
GLOBAL RANSOMWARE ATTACKS ARE ON THE RISE

2017

97% REPORT THAT RANSOMWARE IS BECOMING MORE AND MORE FREQUENT.

99%

PREDICT THE FREQUENCY OF ATTACKS WILL CONTINUE TO INCREASE OVER THE NEXT 2 YEARS.



FOR SMBs, IT'S NO LONGER A QUESTION OF IF, BUT WHEN

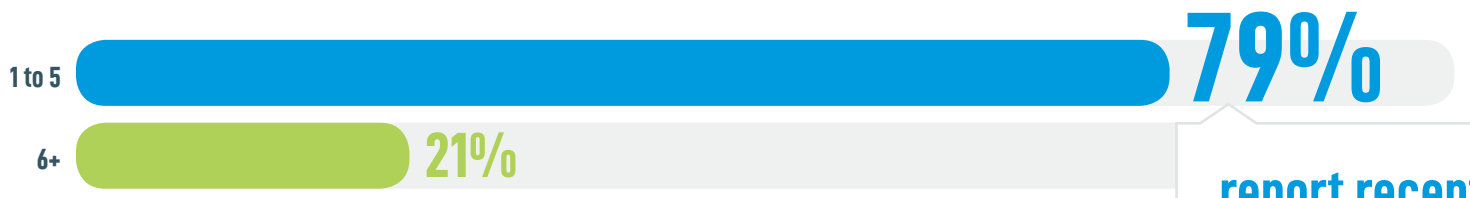
6 IN 7 REPORT SMBs VICTIMIZED BY RANSOMWARE FROM 2015–2017.

6 IN 10 REPORT ATTACKS IN THE 1ST HALF OF 2017 ALONE.

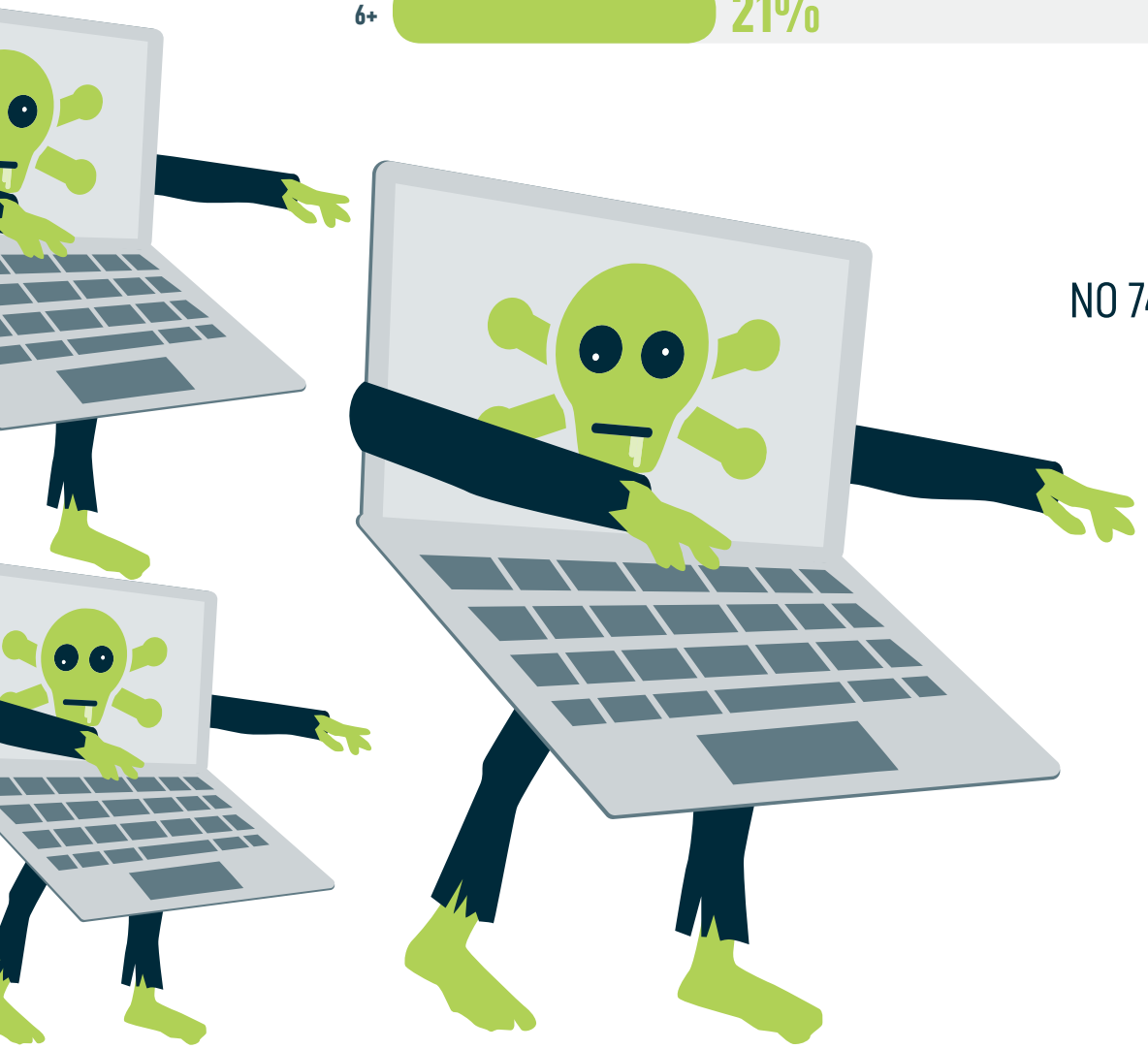
GEO TREND: In APAC, 93% of MSPs report attacks from 2015–2017 and 75% report attacks in H1 2017.

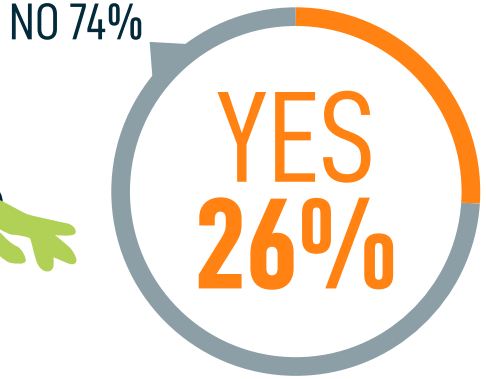
RANSOMWARE IS A FULL-BLOWN EPIDEMIC FOR GLOBAL SMBs

Q: How many clients have experienced a recent ransomware attack?



79% report recent attacks of 1-5 SMBs





An unlucky **26% report multiple attacks** against SMBs in a single day.

GEO TREND: In Canada, 31% of MSPs report multiple ransomware incidents in a single day.

MORE RANSOMWARE ATTACKS REPORTED TO AUTHORITIES BY SMBs

LESS THAN 1 IN 3 ATTACKS ARE REPORTED TO THE AUTHORITIES,

A MARKED IMPROVEMENT FROM 1 IN 4 ATTACKS REPORTED IN 2016.

LESS SMBs ARE PAYING CYBER CRIMINALS THE RANSOM

IN 2017,

35% REPORT SMBs PAID THE RANSOM,

WHICH IS SIGNIFICANTLY LESS THAN IN 2016.

2016:
41%

2017:
35%

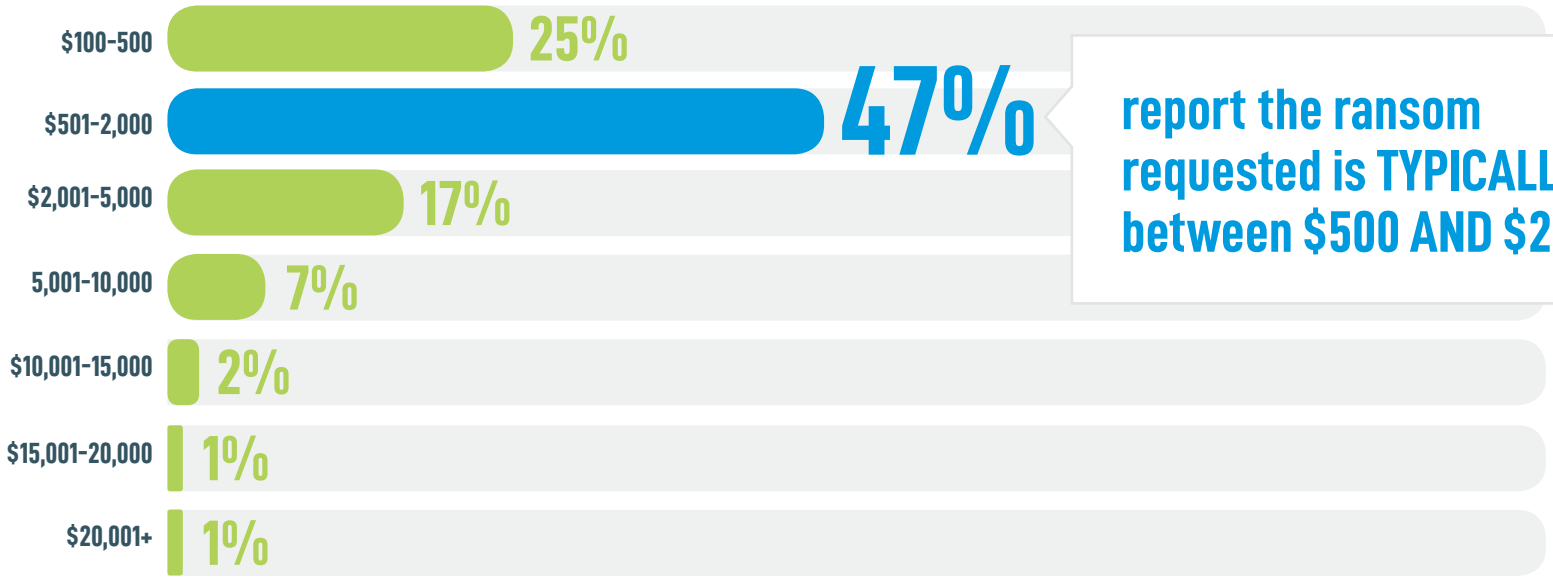
OF THOSE THAT PAID THE RANSOM,

15% NEVER RECOVERED THE DATA.

GEO TREND: In the UK alone, 21% of SMBs who paid the ransom never recovered the data.

FOR SMBs, THE RANSOM ISN'T WHAT BREAKS THE BANK

Q: If ransom was requested, how much (on average)?



47% report the ransom requested is TYPICALLY between $500 AND $2,000.

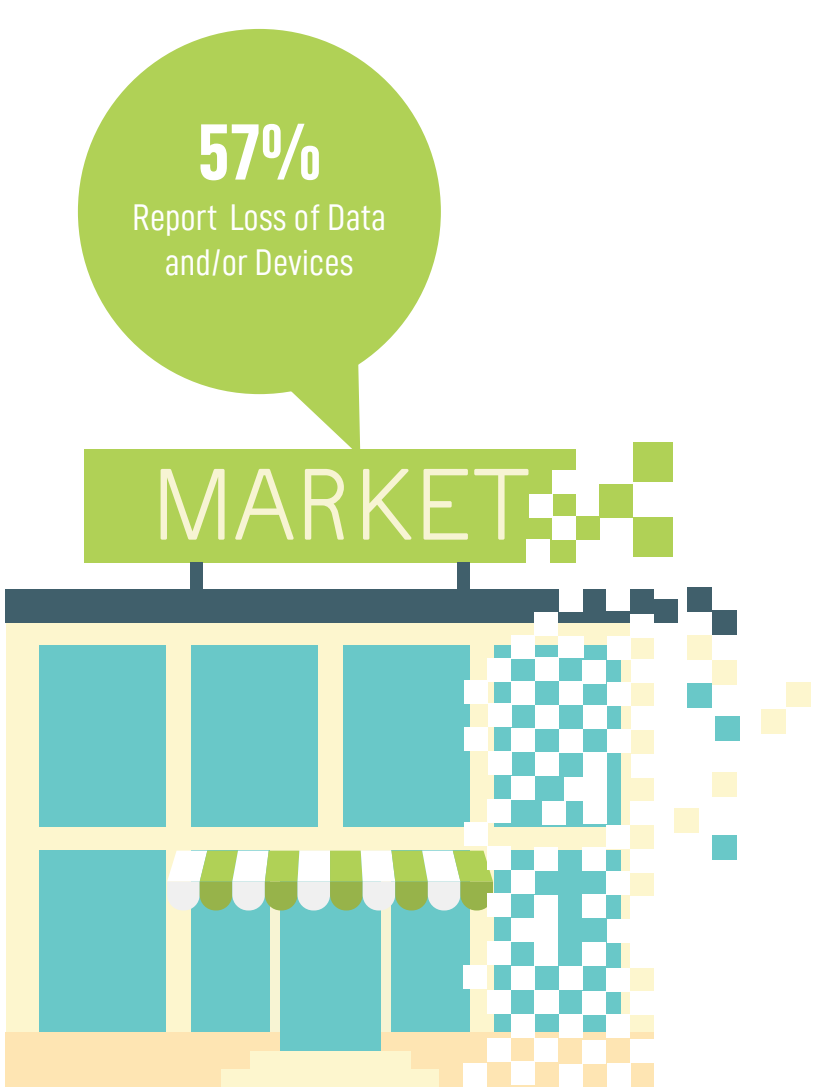
TOTAL RANSOM PAID BY SMBs TO RANSOMWARE HACKERS*:

$301 MILLION.

*Between Q2 2016 and Q2 2017

THE DOWNTIME CUTS THE DEEPEST

Q: Which of the following have clients experienced due to a ransomware attack?



TODAY'S CYBER CRIMINALS ARE MORE RUTHLESS THAN EVER

29% of MSPs REPORT

RANSOMWARE VIRUS REMAINED ON AN SMB'S SYSTEM AFTER THE FIRST ATTACK **AND STRUCK AGAIN AT A LATER TIME.**

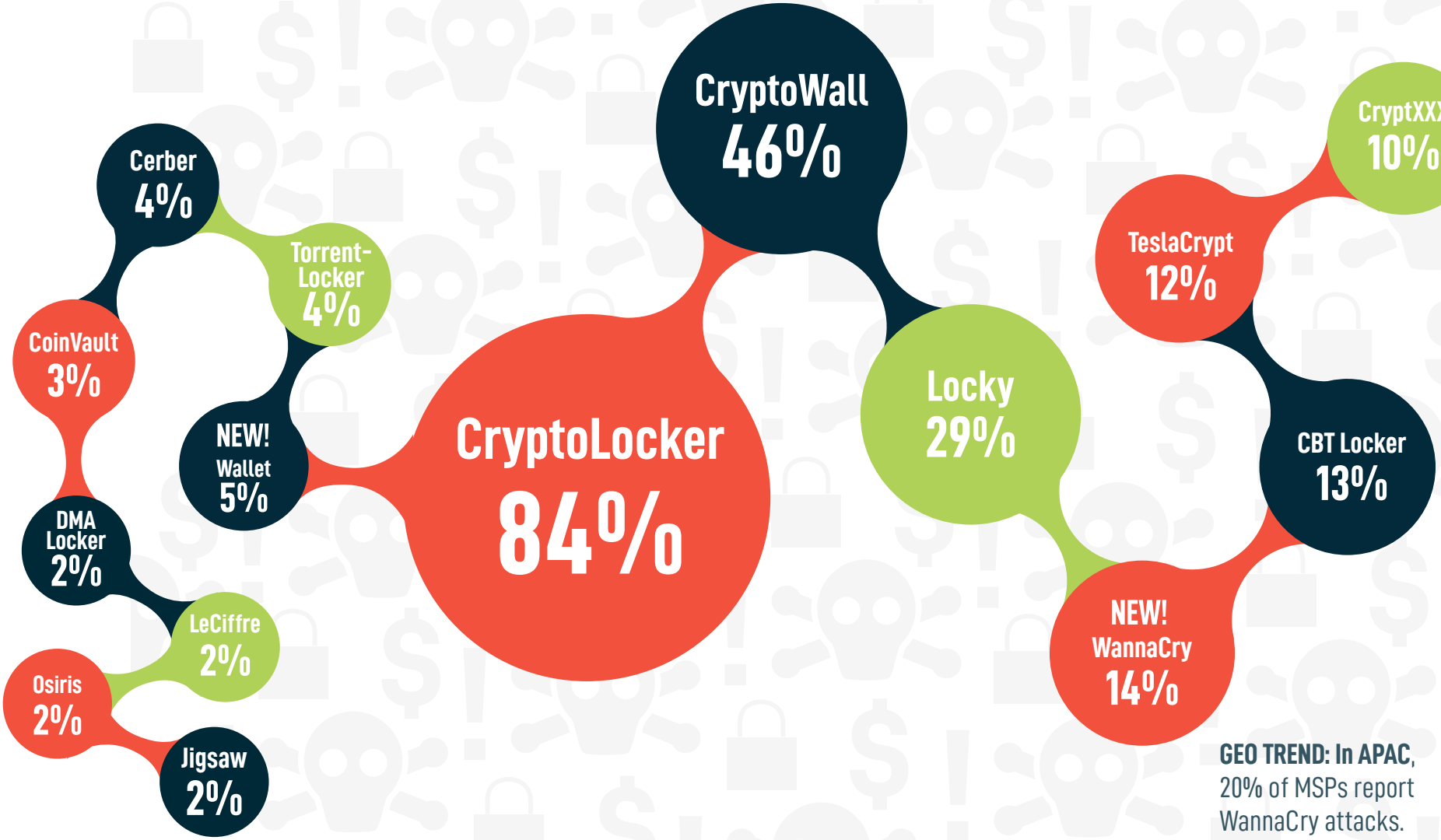
33% of MSPs REPORT

RANSOMWARE ENCRYPTED AN SMB'S BACKUP.

GEO TREND: IN APAC, 42% report ransomware encrypted SMB backups.

CRYPTOLOCKER STILL KING, BUT AGGRESSIVE STRAINS LAUNCH EVERY SINGLE DAY

Q: Have any of your client's been victimized by any of the following?* (Check all that apply)

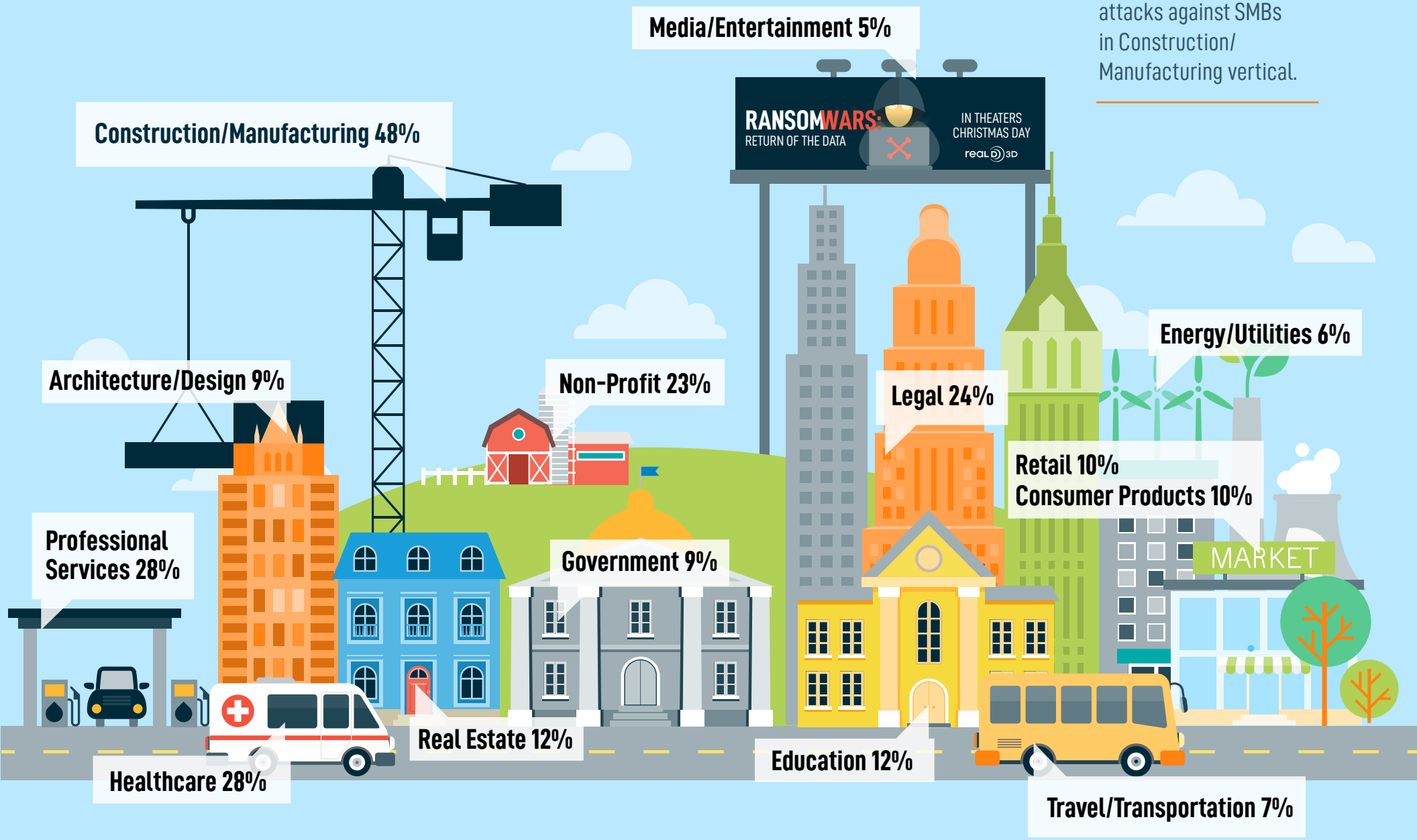


GEO TREND: In APAC, 20% of MSPs report WannaCry attacks.

**This survey was closed before 2017 NotPetya attacks.*

CONSTRUCTION/MANUFACTURING ARE HIGHLY TARGETED, BUT NO INDUSTRY IS SAFE

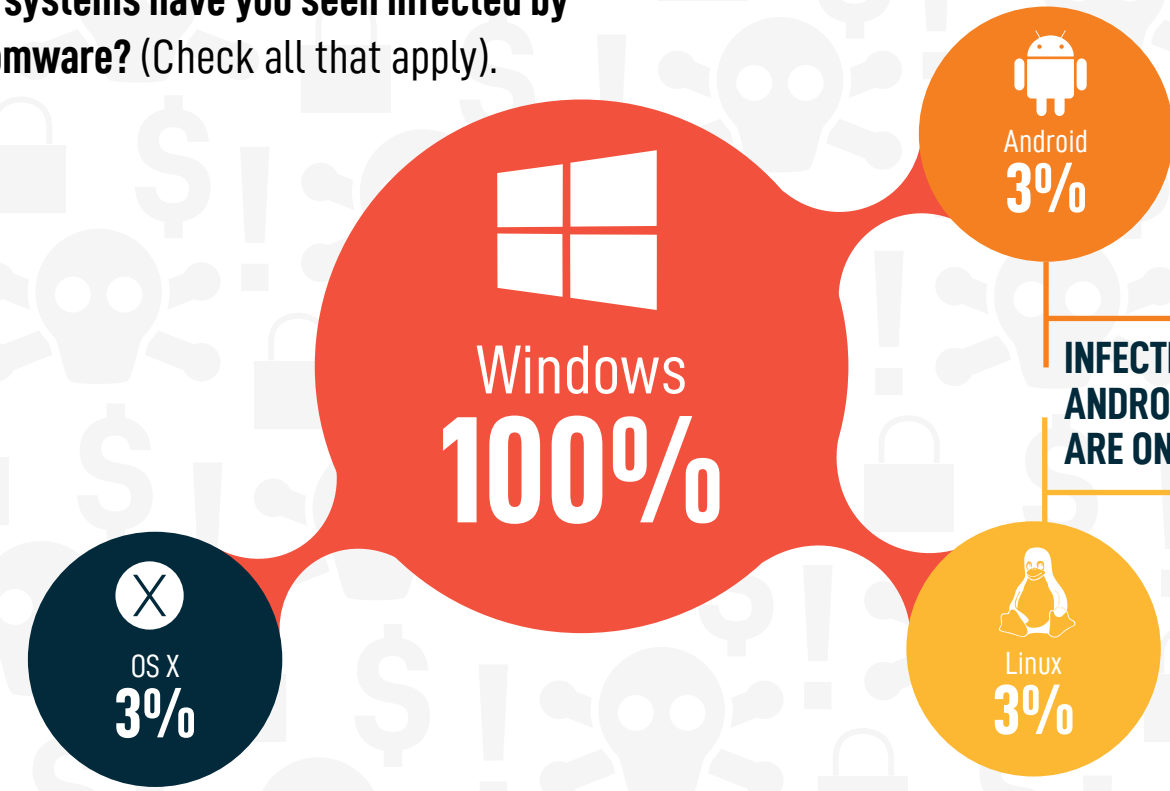
GEO TREND: In APAC, 62% report ransomware attacks against SMBs in Construction/ Manufacturing vertical.



ALL OPERATING SYSTEMS ARE AT RISK TO RANSOMWARE

100% OF MSPs REPORT WINDOWS RANSOMWARE INFECTIONS, BUT NO SINGLE OS IS SAFE.

Q: What systems have you seen infected by ransomware? (Check all that apply).



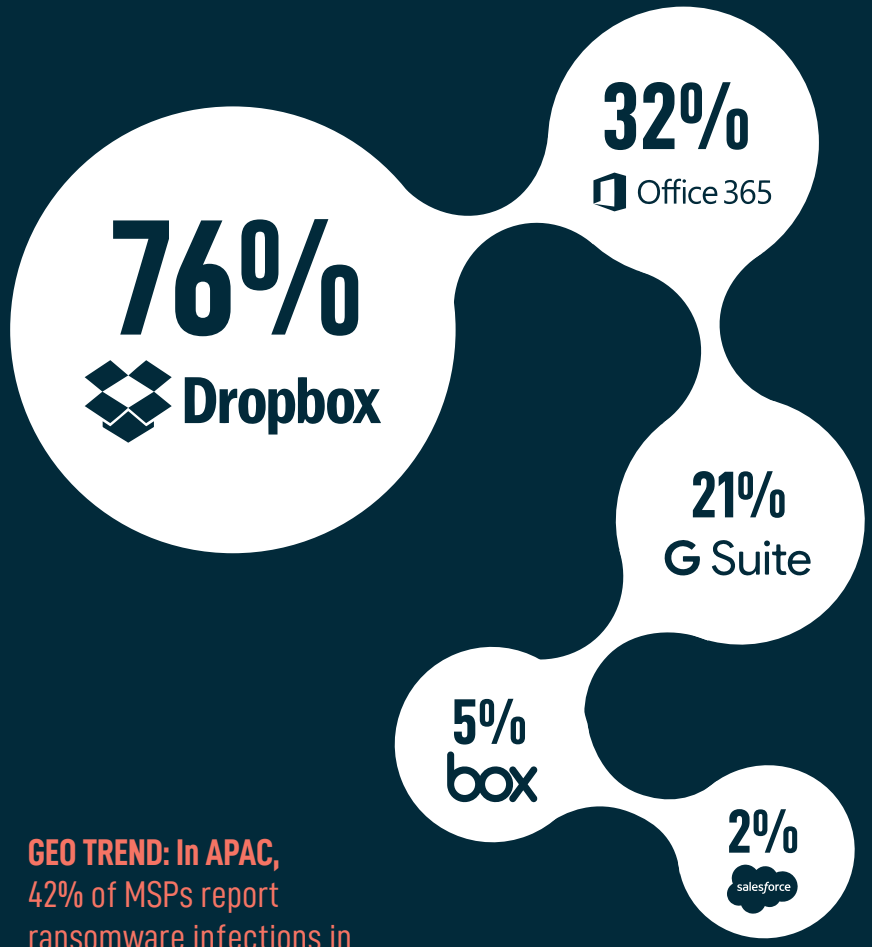
INFECTIONS OF ANDROID & LINUX ARE ON THE RISE.

GEO TREND: In EMEA, 7% of MSPs report Android ransomware infections.

MOBILE/TABLET RANSOMWARE ATTACKS ARE ON THE RISE

SAAS APPLICATIONS ARE NOT IMMUNE TO RANSOMWARE

Of MSPs who report ransomware in SaaS-based applications, the most common are:



GEO TREND: In APAC, 42% of MSPs report ransomware infections in cloud-based applications.

2017

26% REPORT RANSOMWARE INFECTIONS IN CLOUD APPLICATIONS

MAJORITY OF SMBs ARE IN THE DARK ABOUT RANSOMWARE THREAT

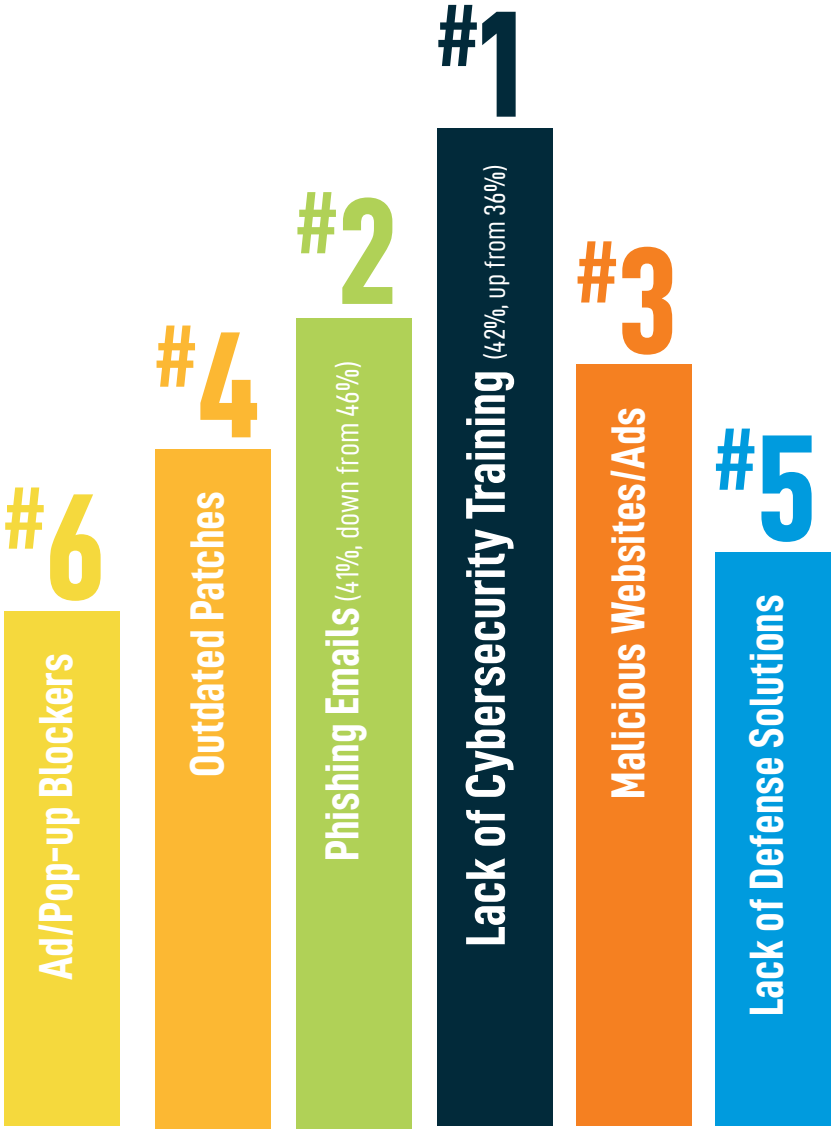
Who's "HIGHLY CONCERNED" about ransomware?

90% of MSPs (up from 88% in 2016)

38% of SMBs (up from 34% in 2016)

IN 2017, **90% OF MSPs ARE "HIGHLY CONCERNED" ABOUT THE RANSOMWARE THREAT** WHILE ONLY 38% OF SMBs FEEL THE SAME.

LACK OF CYBERSECURITY TRAINING FUELS THE SUCCESS OF RANSOMWARE

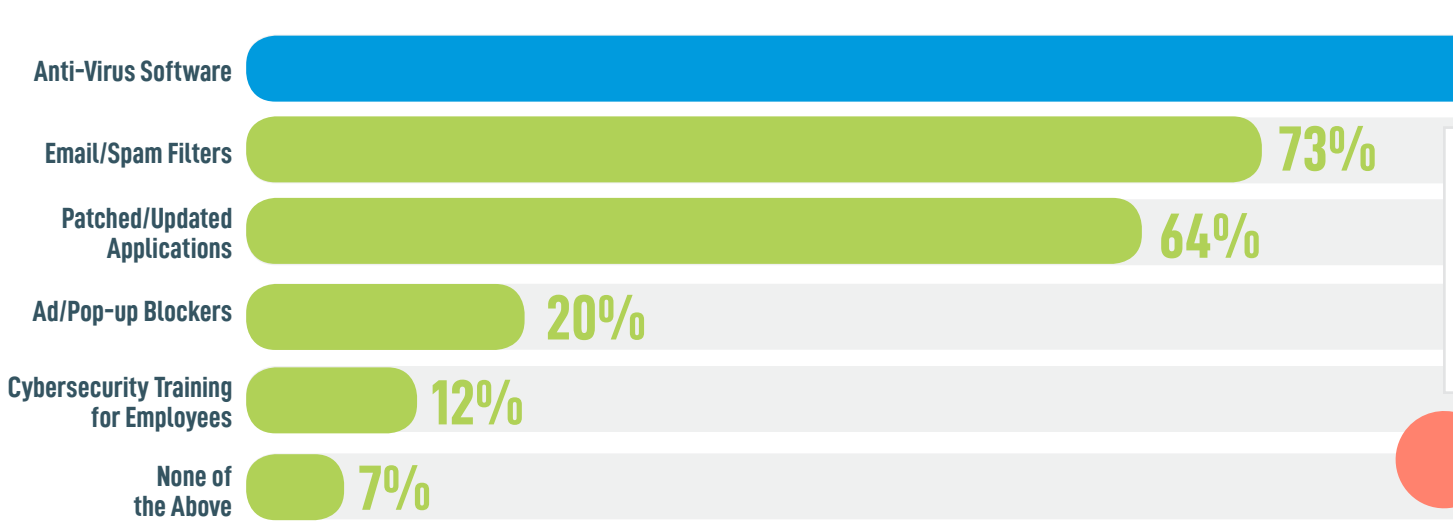


Q: What would you say is the leading of a ransomware infection?

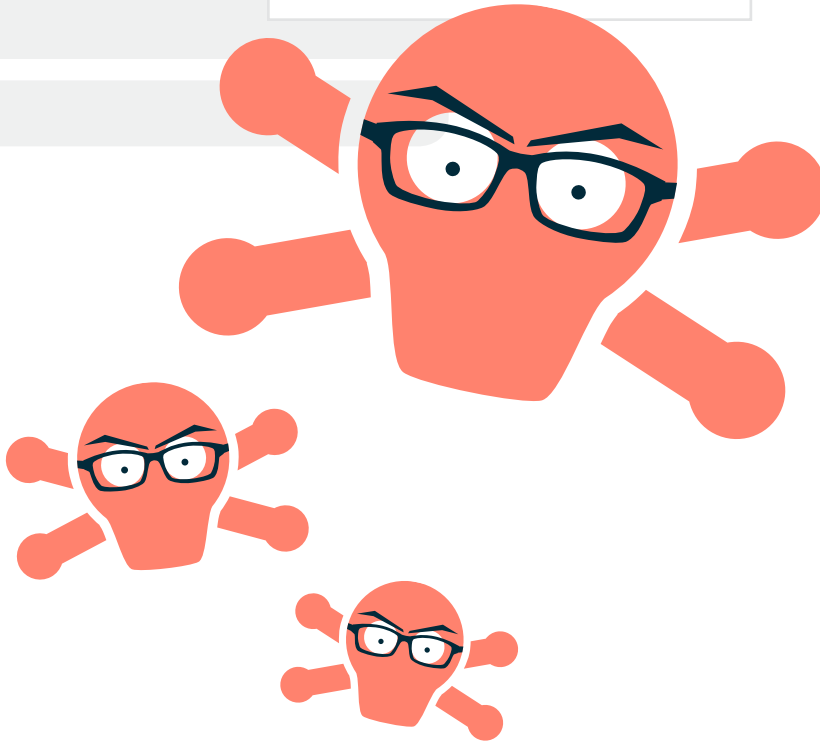
The majority of MSPs blame the **lack of cybersecurity training across SMBs.** Employees today are largely unprepared to defend themselves against these attacks.

TODAY'S TOP CYBERSECURITY SOLUTIONS ARE NO MATCH FOR RANSOMWARE

Q: Of the ransomware incidents you've encountered, had they implemented any of the following?
(Check all that apply)



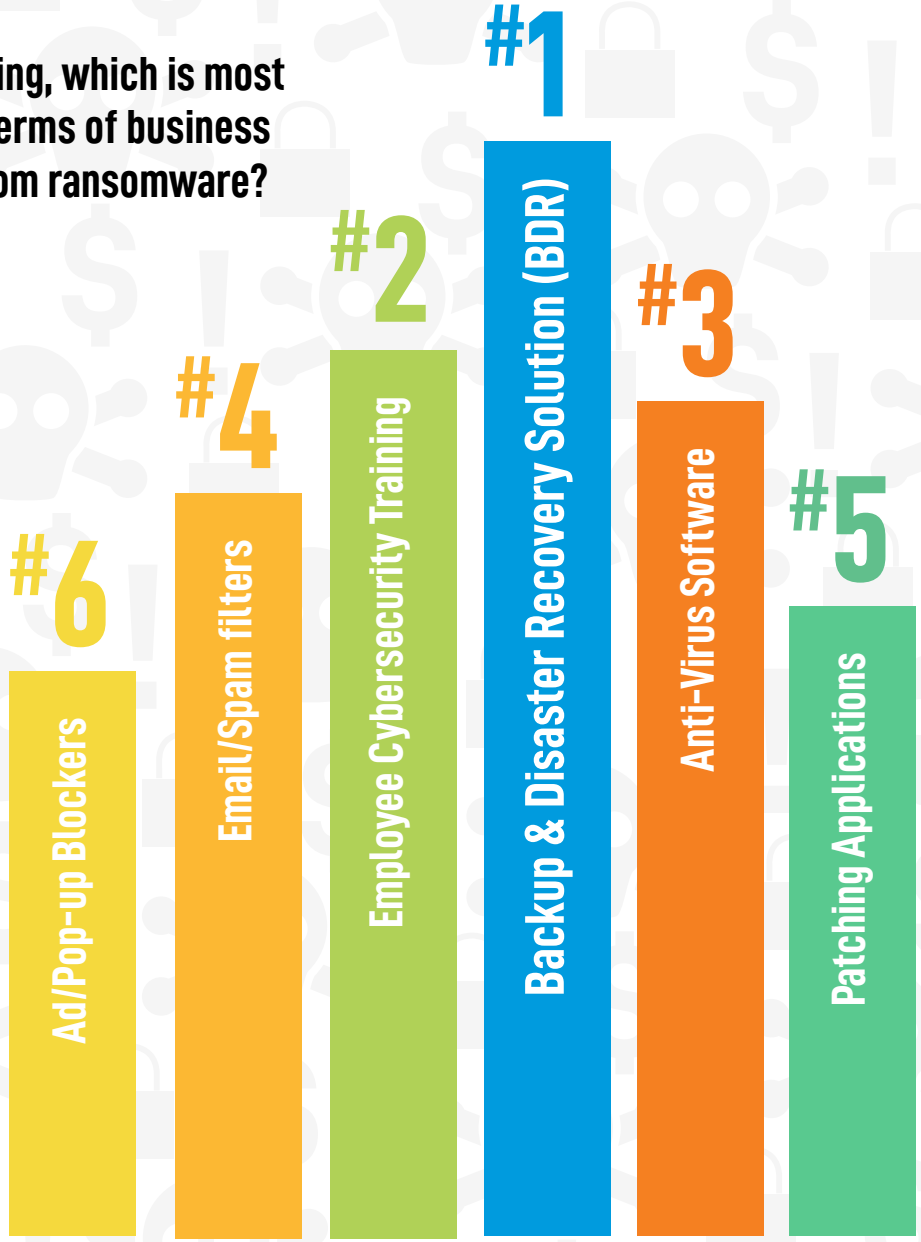
94% report ransomware successfully bypassed anti-virus software.



AS NO SINGLE SOLUTION IS GUARANTEED TO PREVENT RANSOMWARE ATTACKS, **A MULTILAYERED PORTFOLIO IS HIGHLY RECOMMENDED.**

BACKUP & DISASTER RECOVERY (BDR) MOST EFFECTIVE RANSOMWARE PROTECTION

Q: Of the following, which is most effective in terms of business protection from ransomware?



The #1 solution for SMB ransomware protection?

Backup & Disaster Recovery followed by cybersecurity training for all employees.

WITH RELIABLE BDR, MAJORITY OF SMBS WILL RECOVER FROM RANSOMWARE

WITH BDR in place,
96% REPORT SMBs
FULLY RECOVER
FROM RANSOMWARE

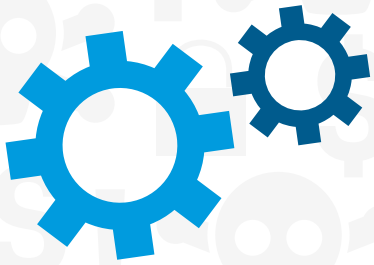
WITHOUT BDR in place,
40% REPORT SMBs
UNABLE TO RECOVER
QUICKLY AND FULLY
FROM RANSOMWARE

95% OF MSPS FEEL "MORE PREPARED"
to respond to an SMB ransomware infection if BDR is in place.

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 BDR. There is no sure fire way of preventing ransomware. Instead, businesses should focus on how to maintain operations despite a ransomware attack. There is only one way to do this: with a solid, fast and reliable backup and 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.

ABOUT DATTO RANSOMWARE DETECTION AND RECOVERY

With Datto Ransomware Detection, available on SIRIS and ALTO devices, MSPs can easily identify a ransomware attack and roll systems back to a point-in-time before the attack hit. Ransomware, like most illicit software, leaves an identifiable footprint as it takes over a server, PC or laptop. Datto's 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 NAS Information:** Traditionally deployed as a cloud-protected network attached storage (NAS) device, the device now includes NAS Guard, which allows customers to protect the device and other network storage with full image rollbacks under one umbrella.
- **Protect SaaS Information:** Subscribers can roll files and data stored in software-as-a-service (SaaS) applications, such as G Suite and Office 365, back to a known good state of health.
- **Protect FSS information:** Building on the ransomware lessons learned from Datto Saas Protection, Datto Drive now performs daily backups in the cloud and on customers' local appliances, protecting both from ransomware.
- **Protect backup data itself:** While backups are happening they exist as a network share that ransomware could encrypt. In the event that does happen, Datto can roll the backup data back to a healthy point and continue on incrementally as if nothing happened.
- **Get back to production quickly:** Whether you have virtual servers or physical servers, Datto reduces your Failback Time Objective (FTO) to the time of a reboot. Restoring back to production with virtual servers is really easy, we leverage your hypervisor environment to handle the cutover. Physical servers have always been a pain but we introduced Fast Failback to reduce your failback time down to a reboot.
- **Restore only the information you need:** Use Backup Insights to compare what changed and restore only what is needed.

For more information, visit: www.datto.com/ransomware

ABOUT THE SURVEY

Datto's Global State of the Channel Ransomware Report is comprised of statistics pulled from a survey of 1,700+ managed services providers in the US, Canada, Australia, the UK and around the world.