

REPORT

datto

Datto's State of the Channel **Ransomware Report** **EUROPE**

Follow us on Twitter: @DattoEMEA

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





ABOUT THIS REPORT

With survey findings gathered from 150 Managed Service Providers (MSPs) serving nearly 1.1M small-to-mid-sized businesses (SMBs) across Europe, Datto's State of the Channel Ransomware Report provides unique visibility into the state of ransomware from the perspective of the European IT Channel and their 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 recovery and continuity in the face of the growing threat.

To learn more about this report, please reach out to [Katie Thornton](#), Senior Content Marketing Manager at Datto, Inc.

KEY FINDINGS

- **Spike in ransomware attacks lead to millions in downtime-related costs for SMBs.** In Europe, an estimated 4.5 percent of small to medium-sized businesses (SMBs) fell victim to the malware from 2016 to 2017. The total amount of ransom paid from these attacks: \$98 Million.
- **For SMBs, it's no longer a question of if, but when.** Ransomware incidents are more frequent in 2017 according to 97% of MSPs. Eighty-nine percent of MSPs cite SMB clients recently victimised by ransomware, 59% reported SMB clients attacked in the first half of 2017 alone. Twenty-two percent of MSPs cite multiple attacks against clients in a single day.
- **Ransomware attacks will continue to thrive over the next two years.** According to 99% 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 fewer are paying the ransom.** Less than 33% of ransomware attacks are reported by SMB victims to the authorities. Additionally, 21 percent of SMBs pay the ransom. Of those that pay the ransom, 18 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, 78% of MSPs report clients experienced business-threatening downtime.
- **Today's ransomware hackers are ruthless and greedy.** Eleven percent of MSPs report a ransomware virus remained on an SMB's system after the first attack and struck again at a later time. Thirty-one percent of 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 81% of MSPs who've dealt with ransomware report seeing CryptoLocker. Additional common variants include CryptoWall, Locky and WannaCry.
- **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, Finance, 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 91% of MSP respondents cited they are "highly concerned" about the business threat of ransomware, only 35% of SMB clients felt the same. This could be due to the lack of mandatory cyber security 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 cyber security 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, 93% of MSPs report clients fully recover from ransomware attacks.



**4.5% OF SMBs FELL VICTIM
TO A RANSOMWARE ATTACK.**
FROM 2016-2017

SMB RANSOMWARE ATTACKS ARE ON THE RISE

97% REPORT THAT RANSOMWARE
ATTACKS ARE MORE FREQUENT THIS YEAR.

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

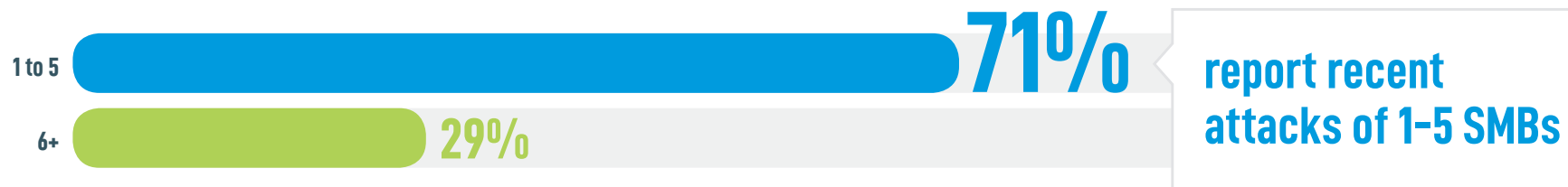
89% REPORT CLIENTS
HAVE SUFFERED FROM
RANSOMWARE ATTACKS
IN THE PAST 2 YEARS.

59% REPORT ATTACKS IN
THE 1ST HALF OF 2017 ALONE.

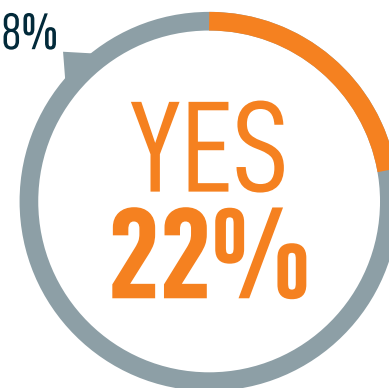


FOR SMBS, RANSOMWARE IS A FULL-BLOWN EPIDEMIC

Q: How many clients experienced a ransomware attack in the last 12 months?



NO 78%



An unlucky **22%** report **multiple ransomware attacks** against SMB clients in a single day.

**RANSOMWARE ATTACKS
REPORTED TO AUTHORITIES BY SMBS**

**LESS THAN 33%
OF ATTACKS ARE
REPORTED TO
THE AUTHORITIES.**



PAYING THE RANSOM DOESN'T GUARANTEE DATA RECOVERY

IN 2017,

**21% OF MSPS REPORT
SMBs PAID THE RANSOM**



OF THOSE THAT PAID THE RANSOM,

**18% STILL NEVER
RECOVERED THE DATA.**

GEO TREND: Globally, 15% of SMBs who paid the ransom never recovered their data.

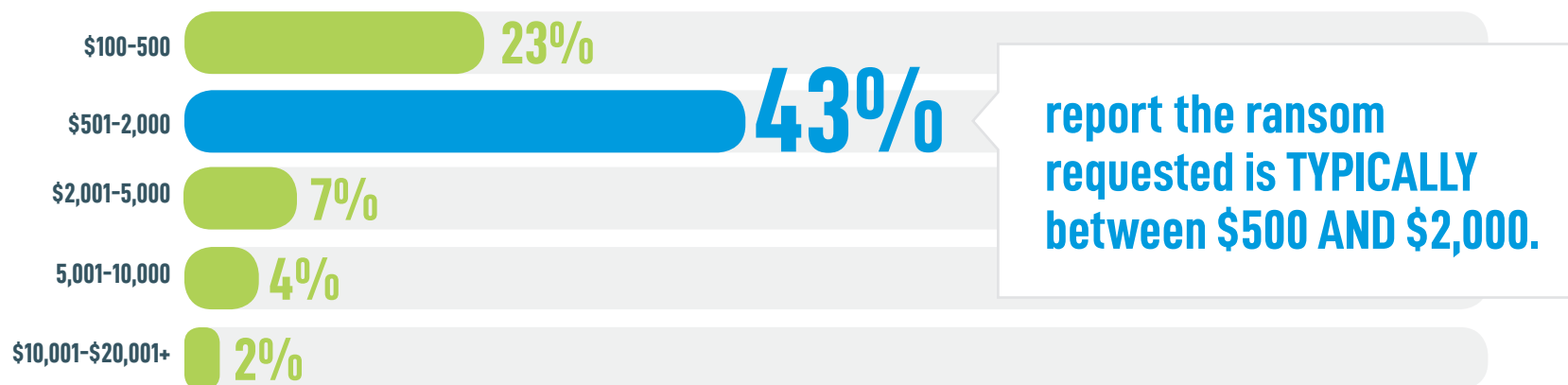
Q: How many of your clients have paid the ransom to hackers?

21%



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

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



**TOTAL RANSOM PAID BY EUROPEAN
SMBs TO RANSOMWARE HACKERS:
\$98 MILLION.**

*Between Q2 2016 and Q2 2017

Approx €79 million / £70 million
as per conversion rates on 12.2.2018

THE DOWNTIME CUTS THE DEEPEST

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



GEO TREND: Compared to the rest of the world the numbers in Europe are higher. Globally, 75% of MSPs report business-threatening downtime and 57% report lost/stolen devices.

TODAY'S CYBER CRIMINALS ARE MORE RUTHLESS THAN EVER

11% of MSPs
REPORT

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

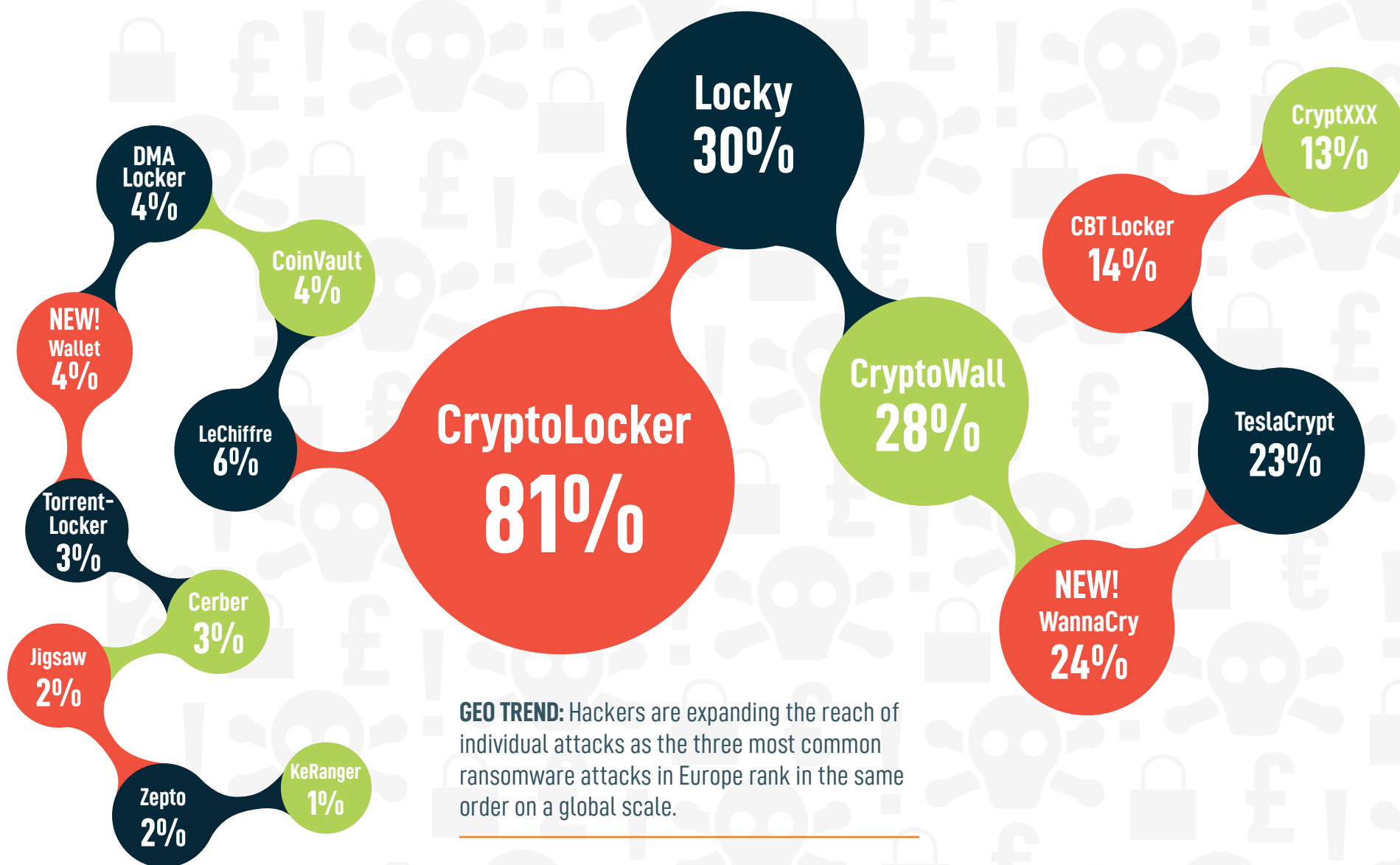
31% of MSPs
REPORT

**RANSOMWARE ENCRYPTING
A CLIENT'S BACKUP.**

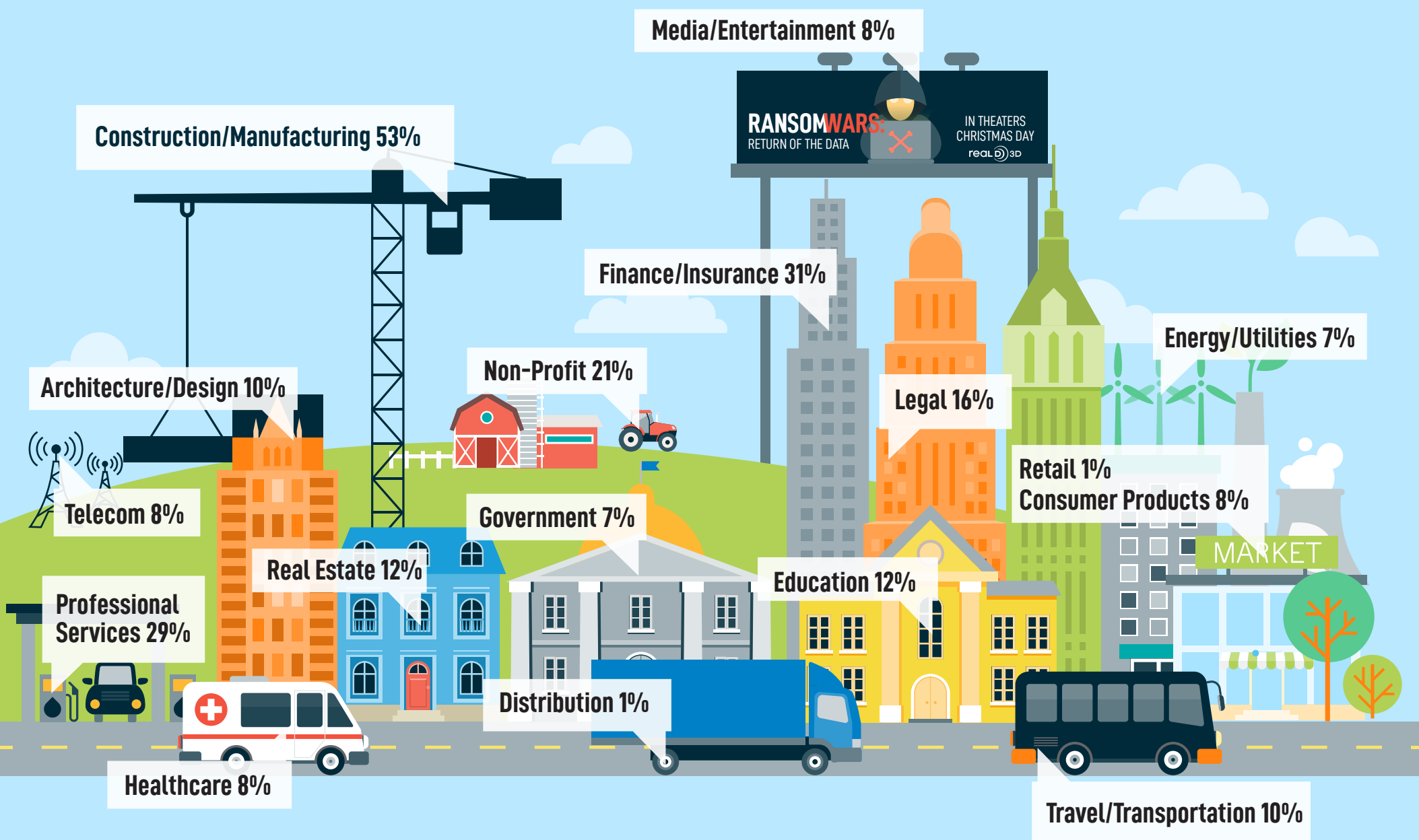


CRYPTOLOCKER STILL KING, BUT AGGRESSIVE STRAINS LAUNCH EVERY DAY

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



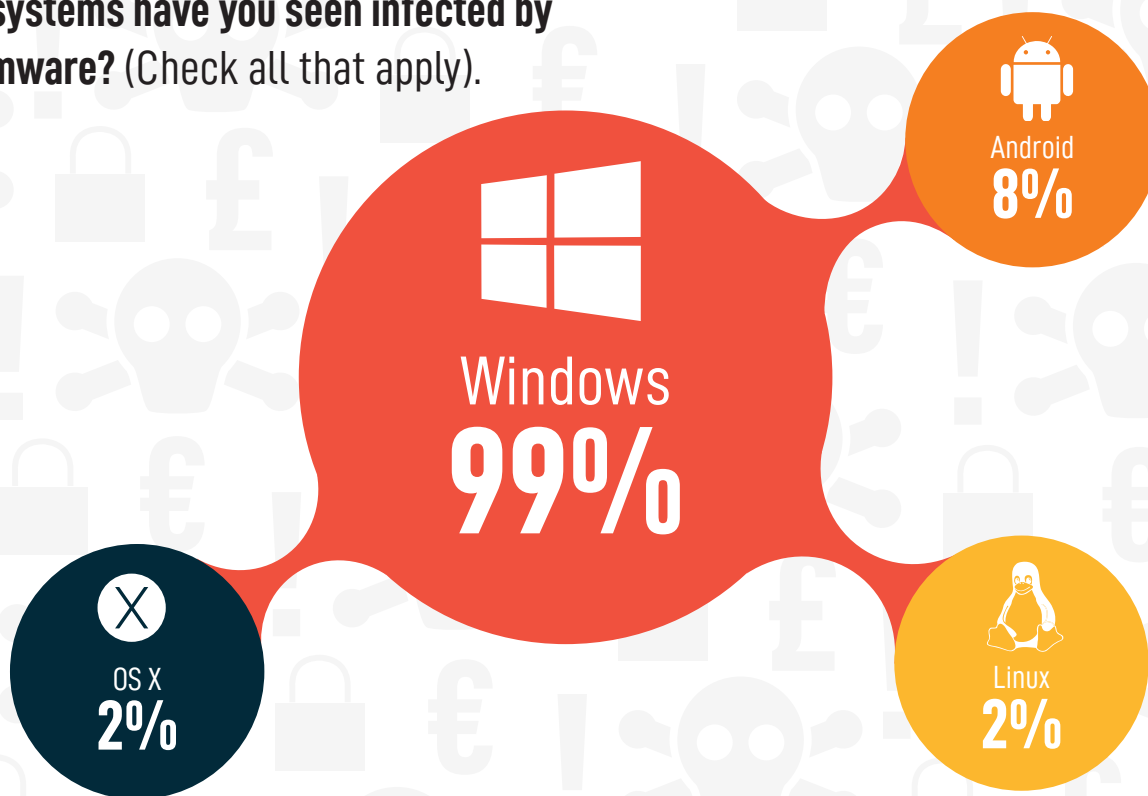
CONSTRUCTION & MANUFACTURING ARE HIGHLY TARGETED, BUT NO INDUSTRY IS SAFE



ALL OPERATING SYSTEMS ARE AT RISK TO RANSOMWARE

99% 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).

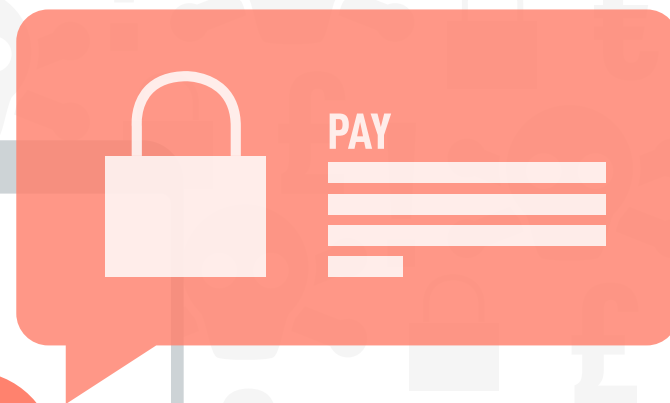


GEO TREND: European MSPs reported the highest percentage of Android devices affected at 8%; compared to the global percentage at 3%.

INFECTIONS OF OS X, ANDROID, LINUX ARE ON THE RISE.

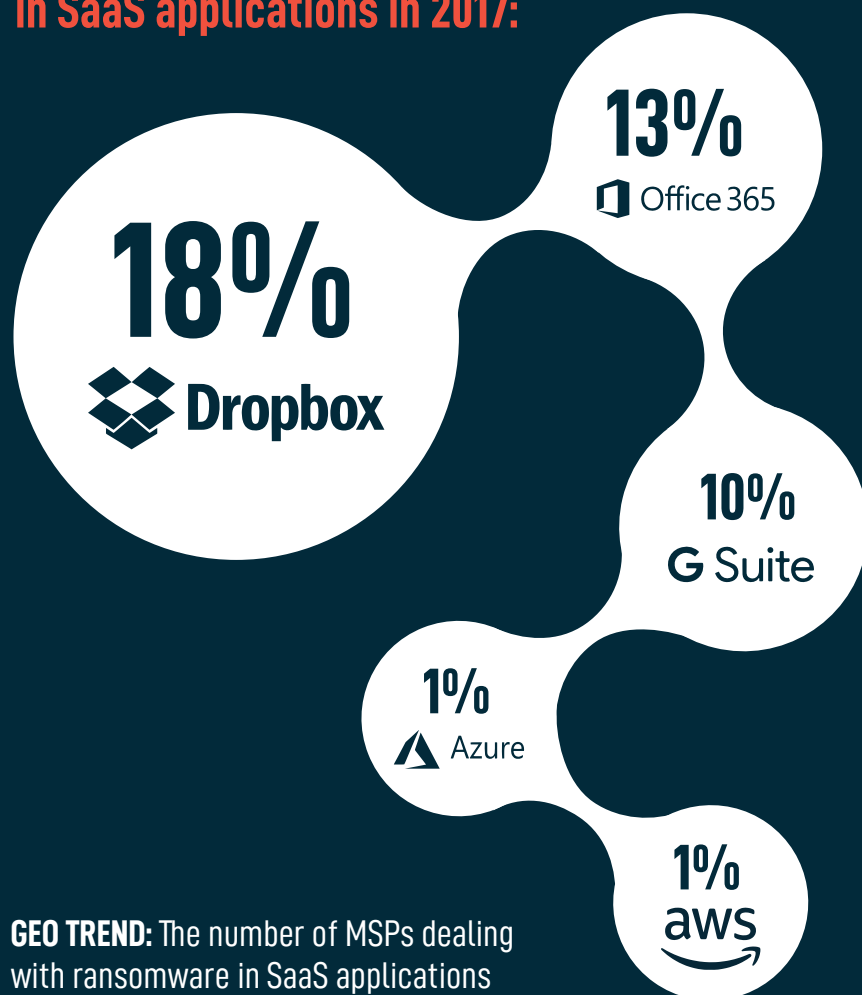
MOBILE/TABLET RANSOMWARE ATTACKS ARE ON THE RISE

4⁰% OF MSPs REPORT
**MOBILE
RANSOMWARE
ATTACKS
IN 2017.**



DROPBOX, OFFICE 365, G SUITE: MOST AT RISK TO RANSOMWARE

Of the MSPs who've reported ransomware in SaaS applications in 2017:



GEO TREND: The number of MSPs dealing with ransomware in SaaS applications in Europe is almost double the global average of 26%.

2017

44% REPORTED RANSOMWARE INFECTIONS IN SAAS APPLICATIONS, MOST COMMONLY IN DROPBOX, OFFICE 365 AND G SUITE

WHEN IT COMES TO RANSOMWARE AWARENESS, THE MAJORITY ARE IN THE DARK

Who's "HIGHLY CONCERNED" about ransomware?

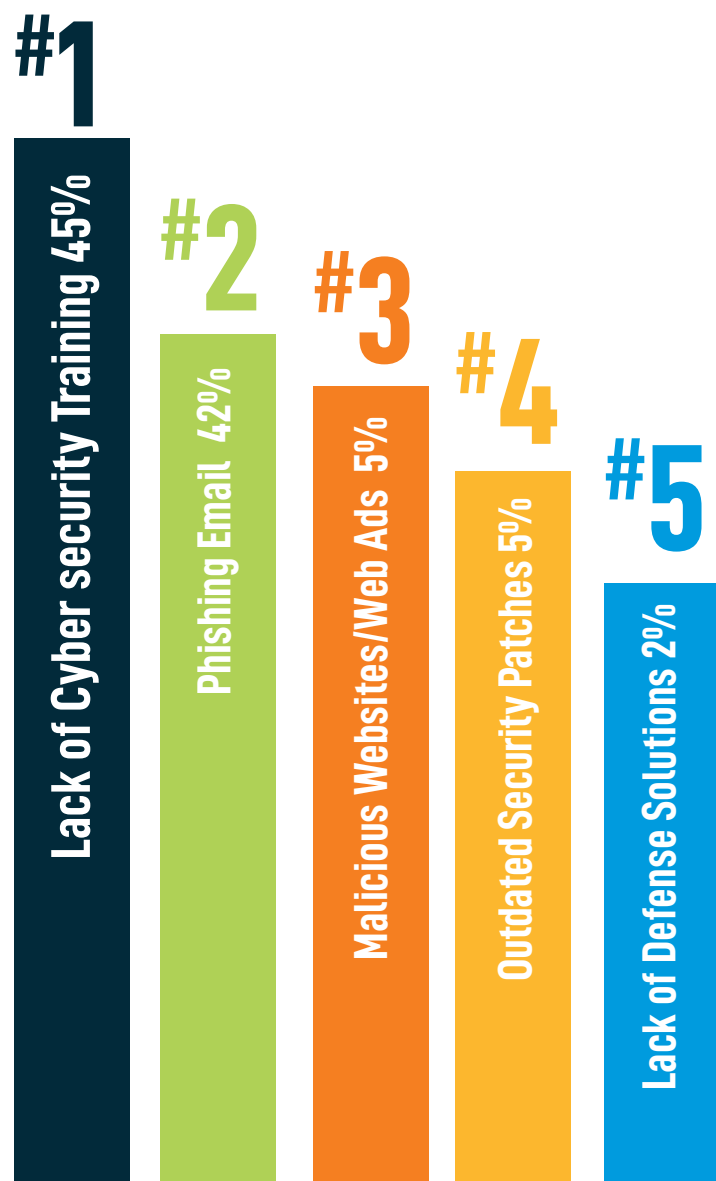


IN 2017, **91% OF MSPs ARE "HIGHLY CONCERNED" ABOUT RANSOMWARE** WHILE ONLY 35% OF SMBS FEEL THE SAME.

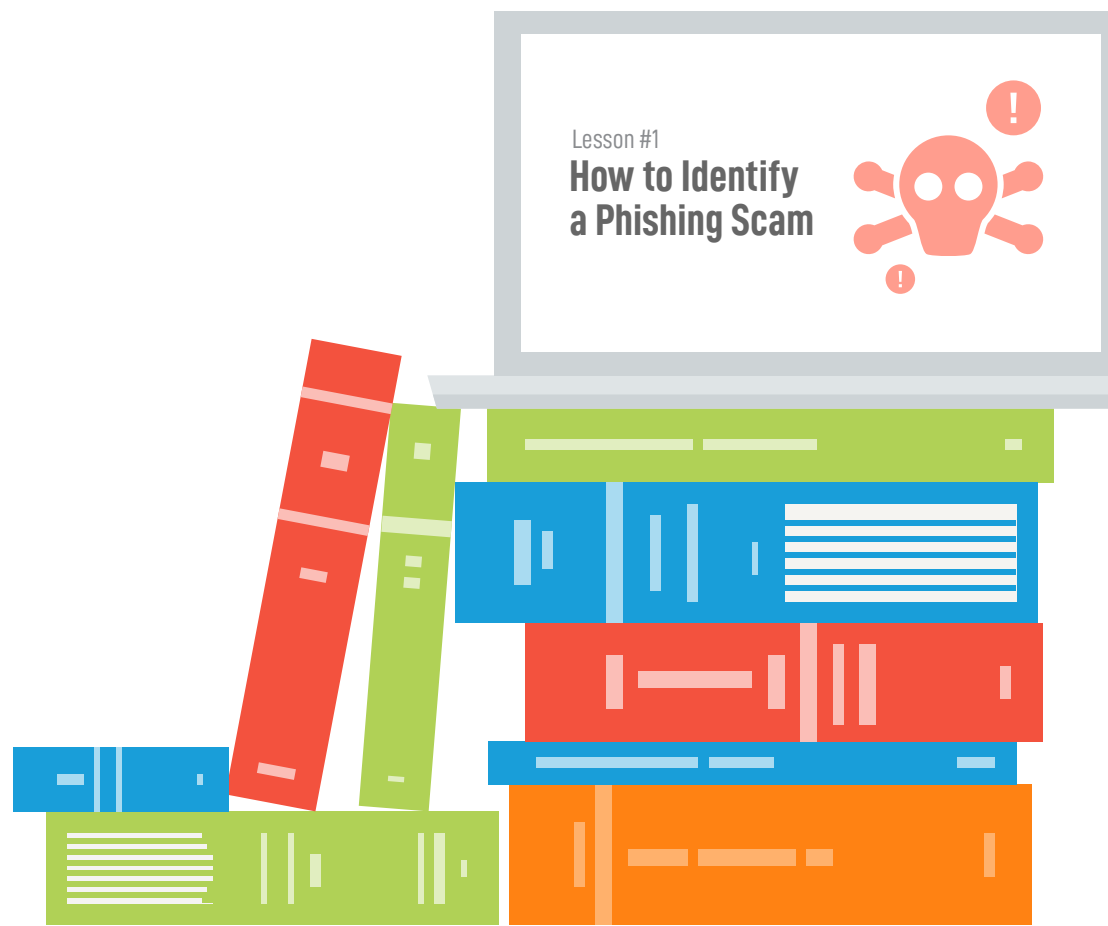


PHISHING IS #1 CULPRIT BEHIND RANSOMWARE SUCCESS

Q: From your experience, what would you say is the leading cause of a ransomware infection?

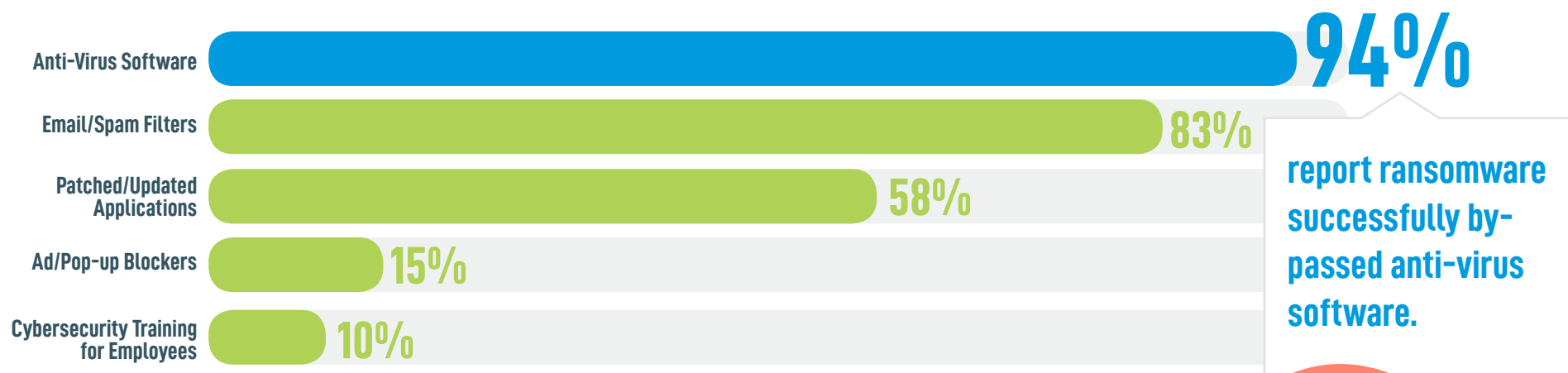


In 2017, the **leading cause of ransomware attacks was lack of cyber security training for employees** according to majority of MSPs.



TOP CYBERSECURITY SOLUTIONS ARE NO MATCH FOR RANSOMWARE TODAY

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

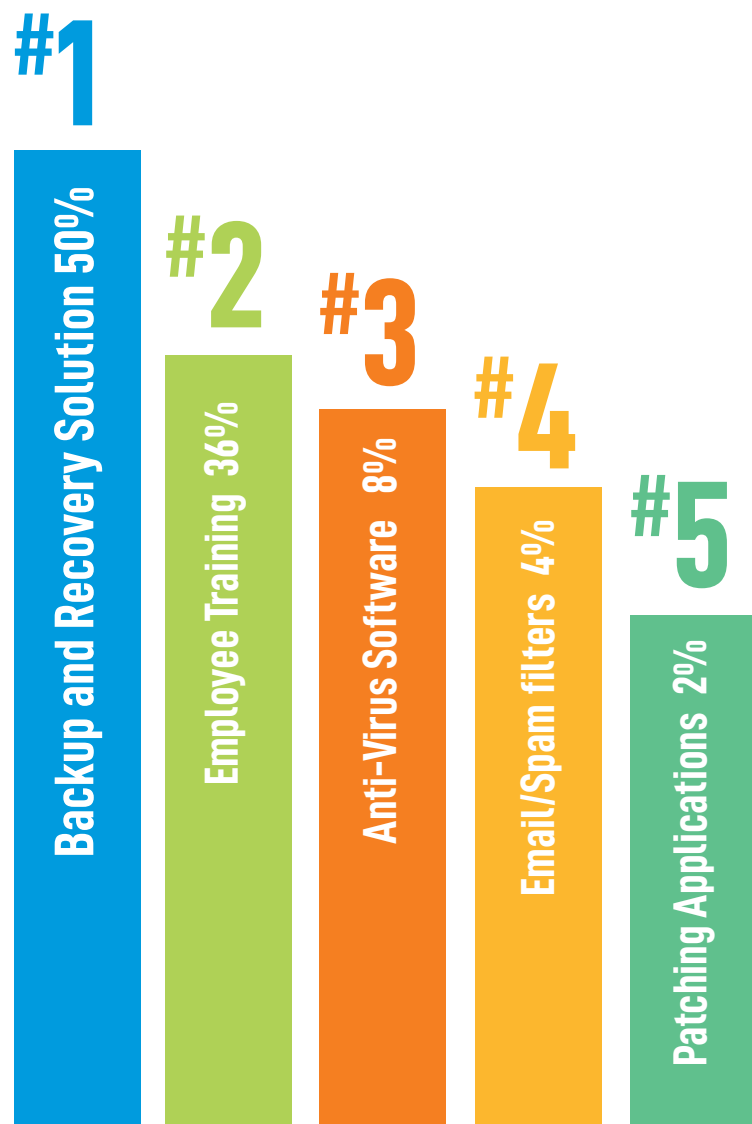


AS NO SINGLE SOLUTION IS GUARANTEED TO PREVENT A SUCCESSFUL ATTACK, **A MULTILAYERED SOLUTION PORTFOLIO IS HIGHLY RECOMMENDED.**



BACKUP & DISASTER RECOVERY (BDR) MOST EFFECTIVE RANSOMWARE PROTECTION

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



The most effective means for business protection from ransomware?

A **backup and disaster recovery (BDR) Solution** according to majority of MSPs. #2 most important to prevent these attacks: **cyber security training for all employees.**



WITHOUT BDR, MAJORITY OF SMBS WILL NOT FULLY RECOVER FROM RANSOMWARE



WITH a reliable backup and recovery solution (BDR) in place, **93% OF MSPS REPORT CLIENTS FULLY RECOVER FROM RANSOMWARE ATTACK.**



WITHOUT a reliable backup and recovery solution (BDR) in place, **54% OF MSPS REPORT CLIENTS DID NOT FULLY RECOVER FROM ATTACK.**

**93% OF MSPS
FEEL “MORE
PREPARED”**

to respond to a client
that falls victim to
ransomware.

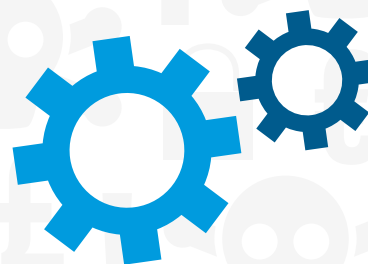
FINAL TAKEAWAYS



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 organisations 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.

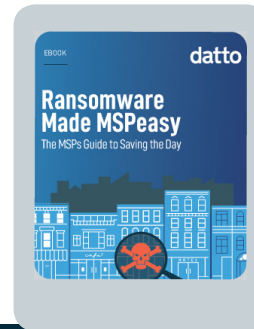
Datto protects all of your business data, no matter where it lives:

- **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 reduced 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 and to learn more about ransomware visit: www.datto.com/uk/ransomware

ADDITIONAL RESOURCES

You Also Might
Be Interested In:



Knowledge is Power:
Ransomware Education
for Employees



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

Join the fight against ransomware!

ABOUT THE SURVEY

Datto's annual Global State of the Channel Ransomware Report is comprised of statistics pulled from a survey of 150+ managed services providers in Europe.

To learn more about the report, please reach out to [Katie Thornton](#), Senior Manager of Content Marketing at Datto, Inc.

ABOUT DATTO

Datto protects business data and provides secure connectivity for tens of thousands of the world's fastest growing companies. Datto's Total Data Protection solutions deliver uninterrupted access to business data on site, in transit and in the cloud. Thousands of IT service providers globally rely on Datto's combination of pioneering technology and dedicated services to ensure businesses are always on, no matter what. Datto is headquartered in Norwalk, Connecticut and has offices in Rochester, Boston, Portland, Toronto, London, Singapore and Sydney. Learn more at www.datto.com.

Founded in 2007 by Austin McChord, Datto is privately held and profitable. In 2013, General Catalyst Partners invested \$25M in growth capital, and in 2015 McChord was named to the Forbes "30 under 30" ranking of top young entrepreneurs.

Copyright © 2018 Datto Inc. All rights reserved.

Follow us on Twitter: [@DattoEMEA](#)