REPORT

datto

Datto's State of the Channel
Ransomware Report
CANADA

Follow us on Twitter: **@Datto**
Visit our Blog: **www.datto.com/blog**

ABOUT THIS REPORT

With survey findings gathered from 200+ Managed Service Providers (MSPs) serving nearly 50,000 small-to-mid-sized businesses (SMBs) in Canada, 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 frequency, targets, impact, and recommendations for ensuring 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 Canada, an estimated 4% of small to medium-sized businesses (SMBs) fell victim to ransomware from Q2 2016-Q2 2017. The total cost of downtime from these attacks: $5.7 Million.
- **For SMBs, it's no longer a question of if, but when.** Ransomware incidents are more frequent in 2017 according to 98% of Canadian MSPs. Eighty-three percent cite SMB clients recently victimized by ransomware, 18% report six or more SMB client attacks in the first half of 2017 alone. Thirty-one 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 98% of Canadian 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 28% of ransomware attacks are reported by SMB victims to the authorities. Additionally, 32% of SMBs pay the ransom. Of those that pay the ransom, 13% 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, 70% of Canadian MSPs report clients experienced business-threatening downtime.
- **Today's ransomware hackers are ruthless and greedy.** Thirteen 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 the most common variant attacking SMBs, but new and aggressive strains pop up every single day.** Nearly 85% of MSPs who've dealt with ransomware report seeing CryptoLocker. Other common variants include CryptoWall, Locky, and WannaCry, which is a new addition to the list this year.
- **No industry, operating system, cloud, or device is safe from these attacks.** Among the industries most targeted most by ransomware attacks: 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 91% of MSP cited they are "highly concerned" about the business threat of ransomware, only 34% of SMB clients felt the same. This could be due to the lack of cybersecurity training across small businesses, 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.
- **With a reliable backup and disaster recovery solution in place, the majority of SMBs will fully recover from a ransomware infection.** With a reliable BDR in place, 96% of MSPs report clients fully recover from ransomware attacks.

THE #1 CYBERSECURITY THREAT FOR BUSINESSES TODAY: RANSOMWARE

IN CANADA, AN ESTIMATED

4% OF SMALL-TO-MID-SIZED BUSINESSES (SMBs) FELL VICTIM TO RANSOMWARE

FROM 2016-2017

SMB RANSOMWARE ATTACKS ARE ON THE RISE

98% REPORT THAT RANSOMWARE ATTACKS ARE MORE FREQUENT THIS YEAR.

98%

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

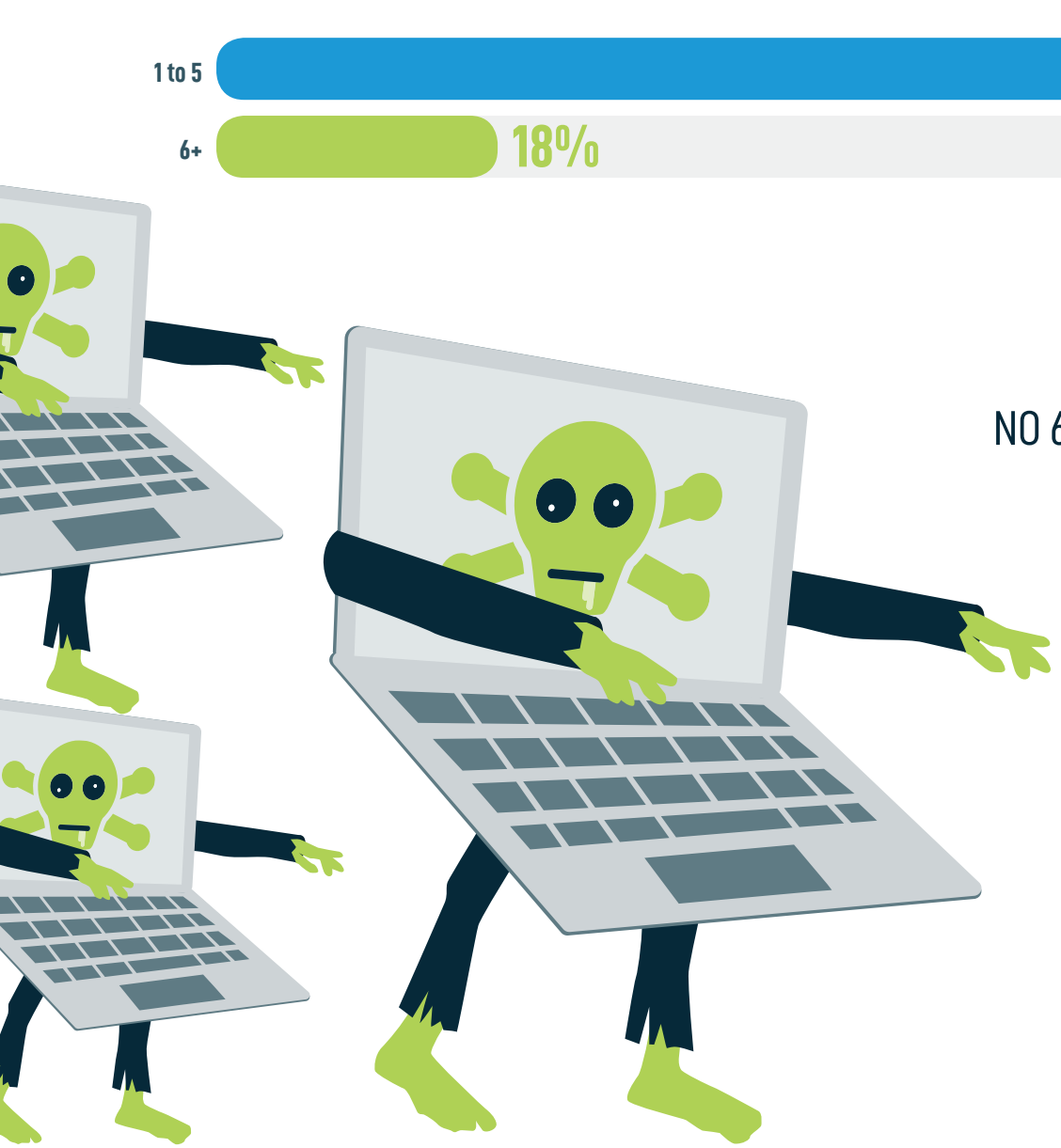
FOR SMBs, IT'S NO LONGER A QUESTION OF IF, BUT WHEN

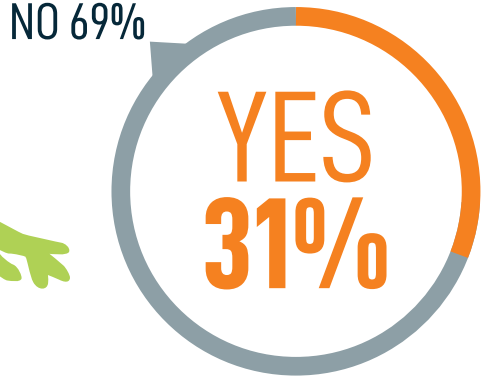
83% REPORT CLIENTS HAVE **SUFFERED FROM RANSOMWARE ATTACKS** IN THE PAST 2 YEARS.

58% REPORT **ATTACKS IN THE 1ST HALF OF 2017 ALONE.**

FOR SMBS, RANSOMWARE IS A FULL-BLOWN EPIDEMIC

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





An unlucky **31% report multiple ransomware attacks** against SMB clients in a single day.

GEO TREND: Globally, only 26% of MSPs report multiple attacks against SMBs in a single day.

RANSOMWARE ATTACKS REPORTED TO AUTHORITIES BY SMBS

LESS THAN 28% OF ATTACKS ARE REPORTED TO THE AUTHORITIES.

PAYING THE RANSOM DOESN'T GUARANTEE DATA RECOVERY

IN 2017,

32% OF MSPS REPORT SMBs PAID THE RANSOM

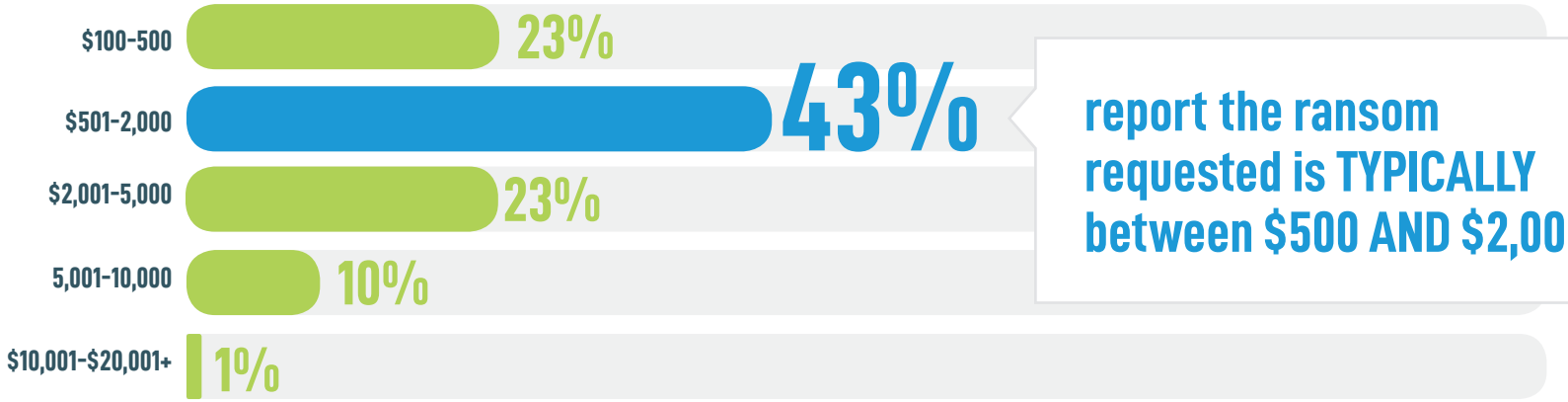
OF THOSE THAT PAID THE RANSOM,

13% STILL NEVER RECOVERED THE DATA.

GEO TREND: In the UK, 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)?



43% report the ransom requested is TYPICALLY between $500 AND $2,000.

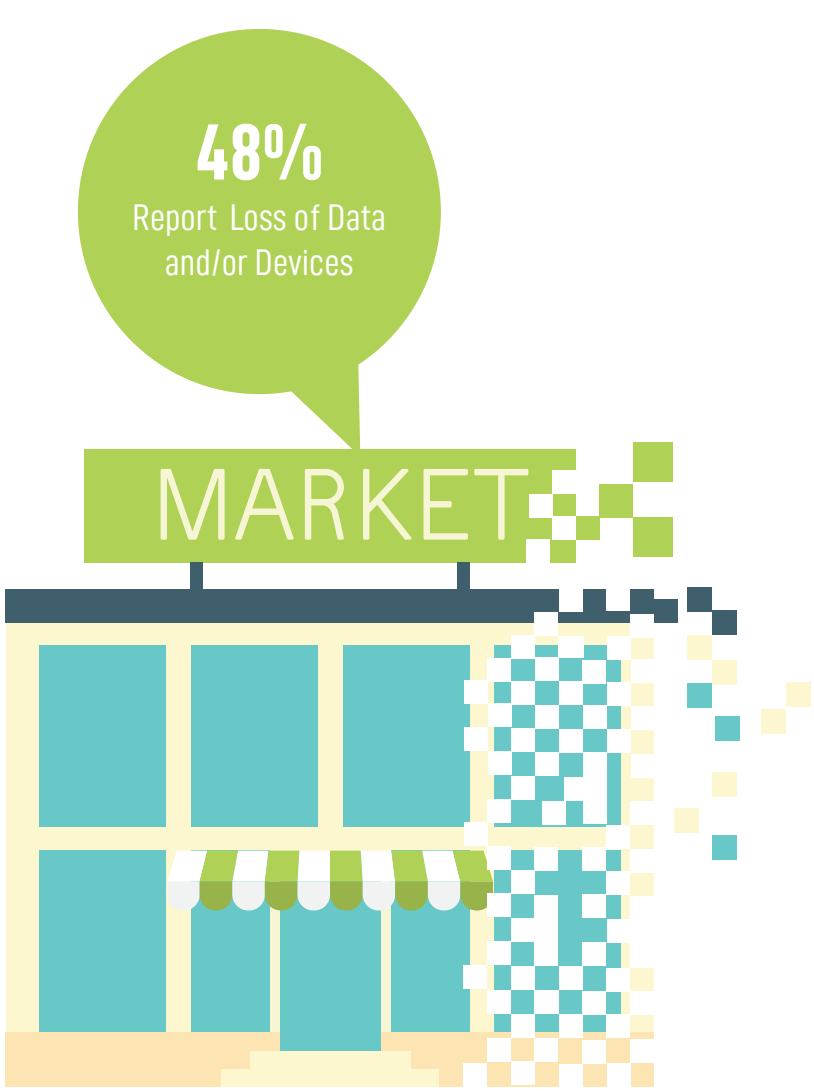
TOTAL RANSOM PAID BY CANADIAN SMBS TO RANSOMWARE HACKERS:

$5.7 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

13% of MSPs REPORT

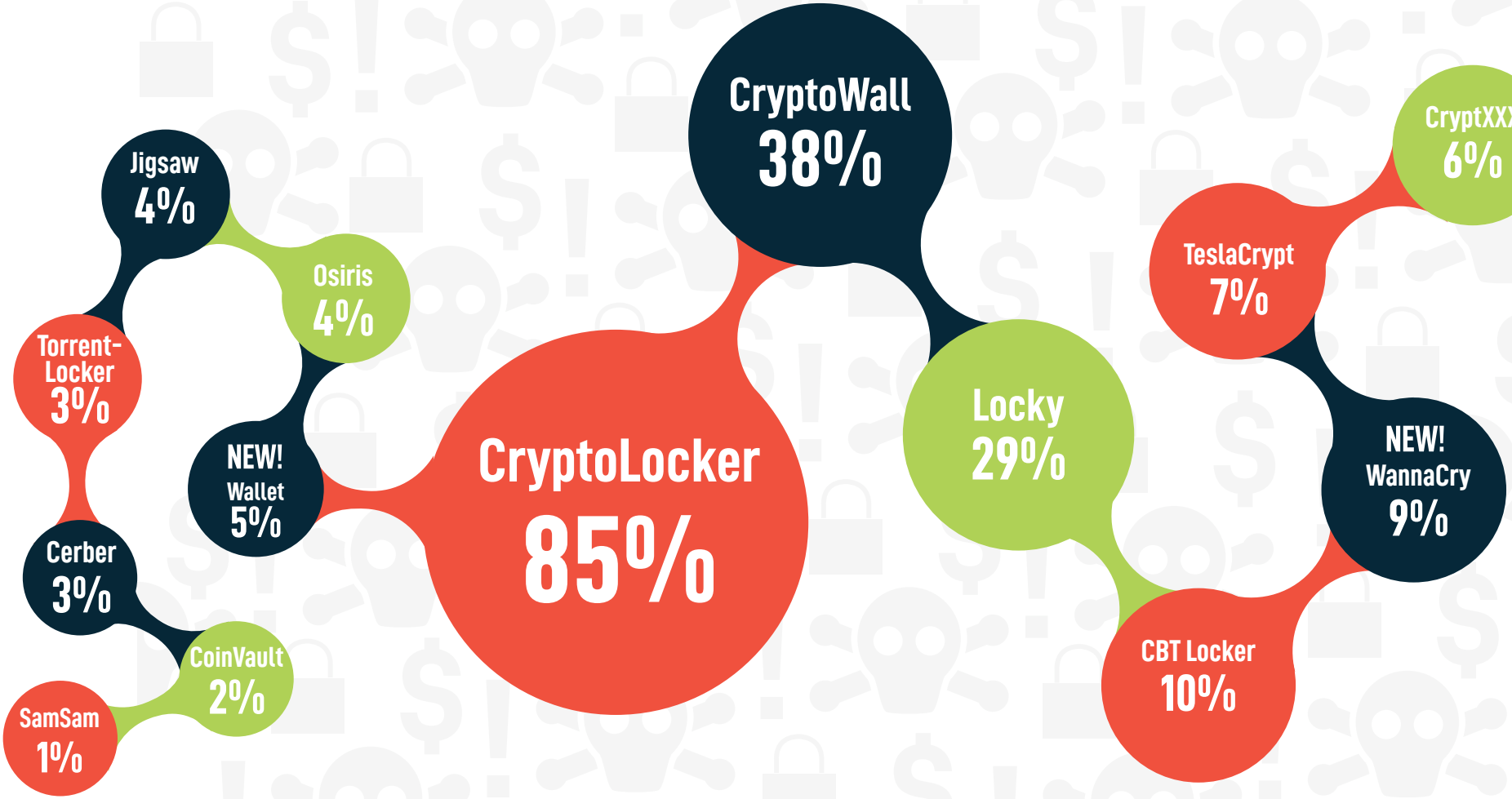
RANSOMWARE REMAINED ON A CLIENT'S SYSTEM AFTER THE FIRST ATTACK **AND STRUCK AGAIN AT A LATER TIME.**

33% of MSPs REPORT

RANSOMWARE ENCRYPTING A CLIENT'S BACKUP.

CRYPTOLOCKER STILL KING, BUT AGGRESSIVE STRAINS LAUNCH EVERY DAY

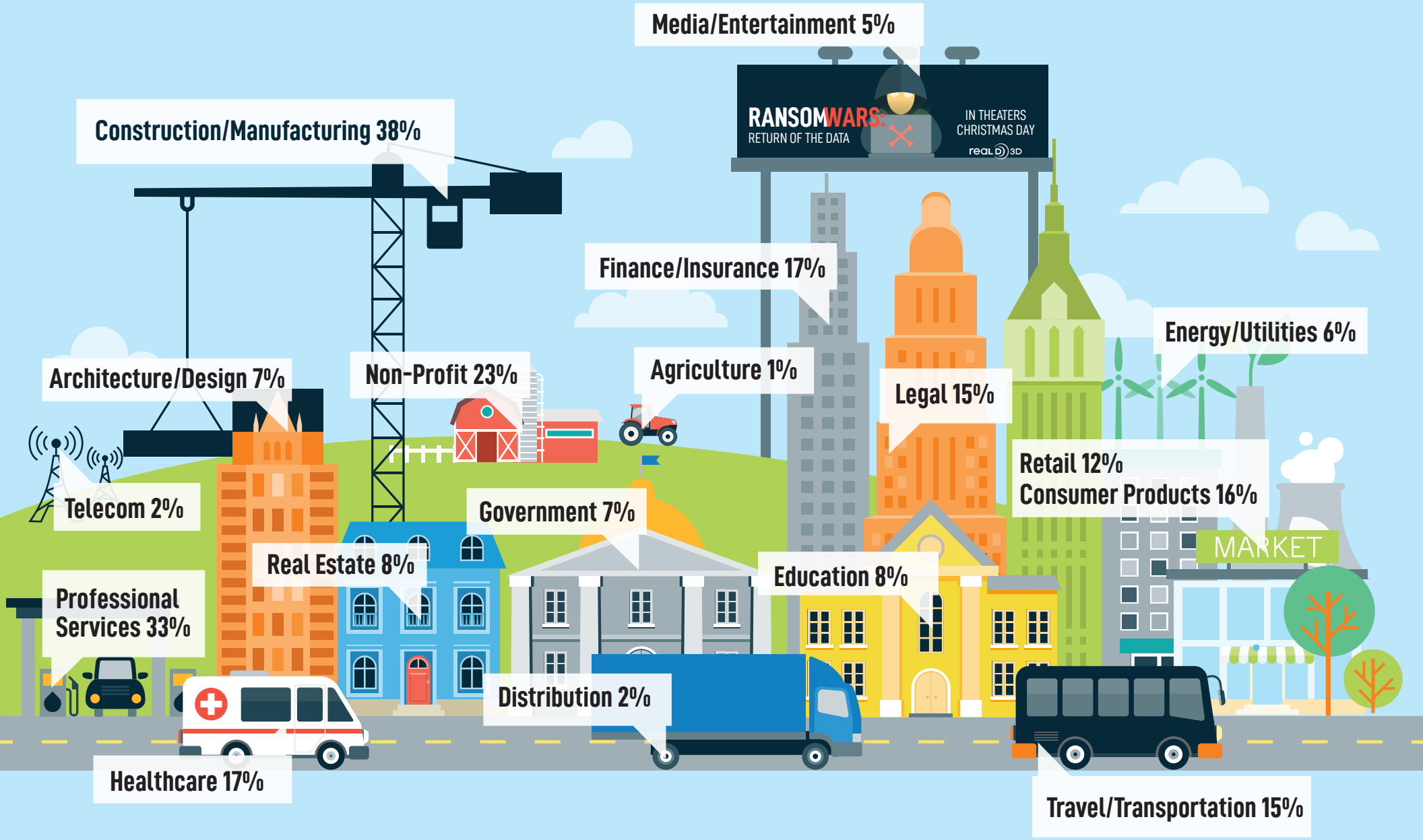
Q: Have any of your client's been victimized by any of the following?* (Check all that apply)



*This survey was closed before 2017 NotPetya attacks.

GEO TREND: The top three most common ransomware strains in Canada are the same as the top three globally.

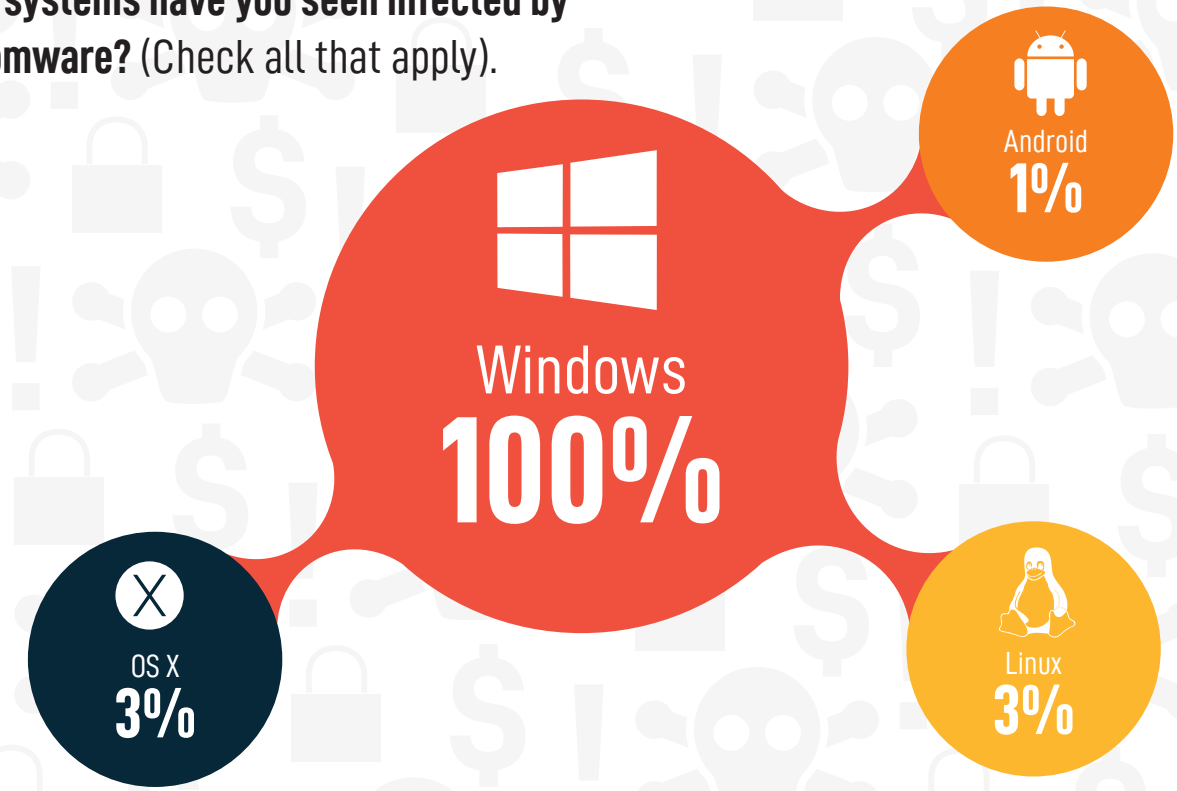
CONSTRUCTION & MANUFACTURING ARE HIGHLY TARGETED, BUT NO INDUSTRY IS SAFE



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).



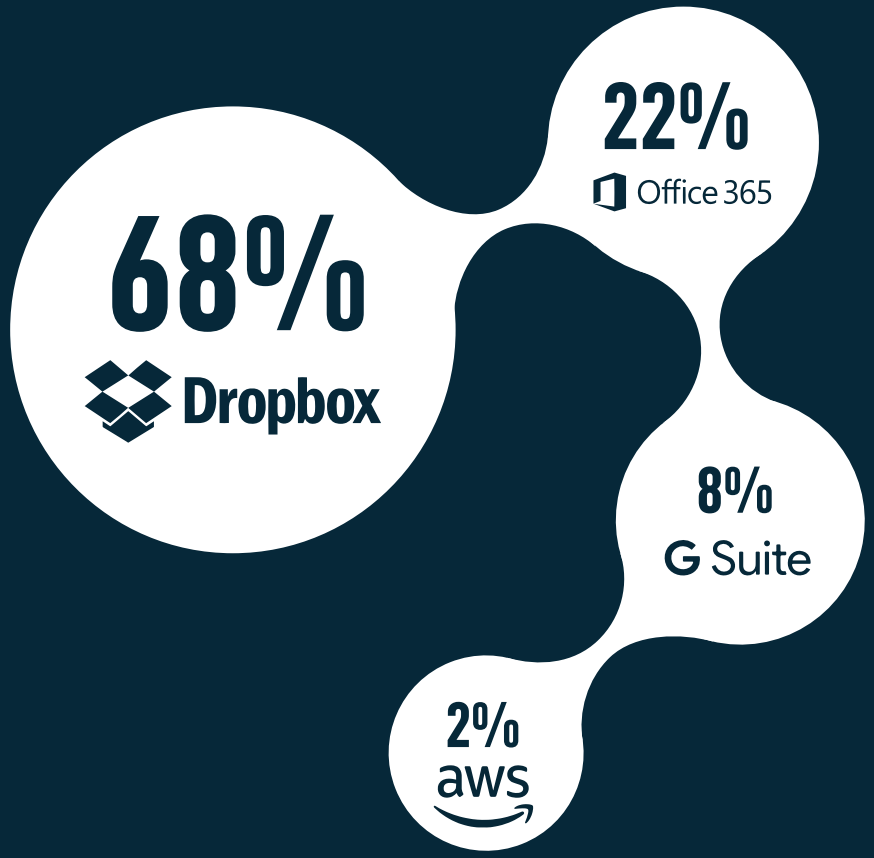
OS X, ANDROID, LINUX ARE ON THE RISE

MOBILE/TABLET RANSOMWARE ATTACKS ARE ON THE RISE

4% 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: Globally, 26% of MSPs report ransomware infections in cloud-based applications (vs. 33% in Canada).

2017

33% REPORT RANSOMWARE INFECTIONS IN CLOUD APPS SUCH AS DROPBOX, OFFICE 365, AND G SUITE.

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

Who's "HIGHLY CONCERNED" about ransomware?

91% of CANADIAN MSPs

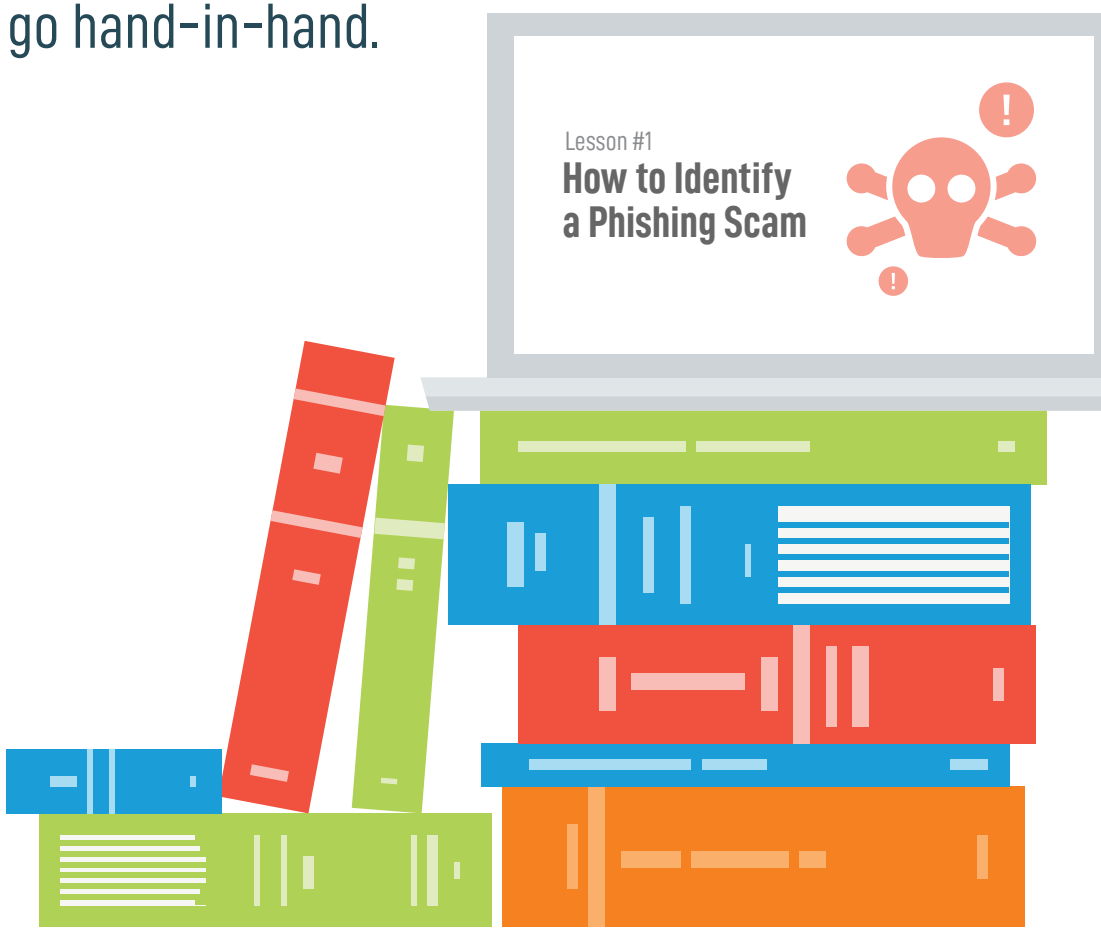
34% of CANADIAN SMBs

IN 2017, **91% OF MSPs ARE "HIGHLY CONCERNED" ABOUT RANSOMWARE** WHILE ONLY 34% OF SMBS FEEL THE SAME.

PHISHING IS #1 CULPRIT BEHIND RANSOMWARE SUCCESS

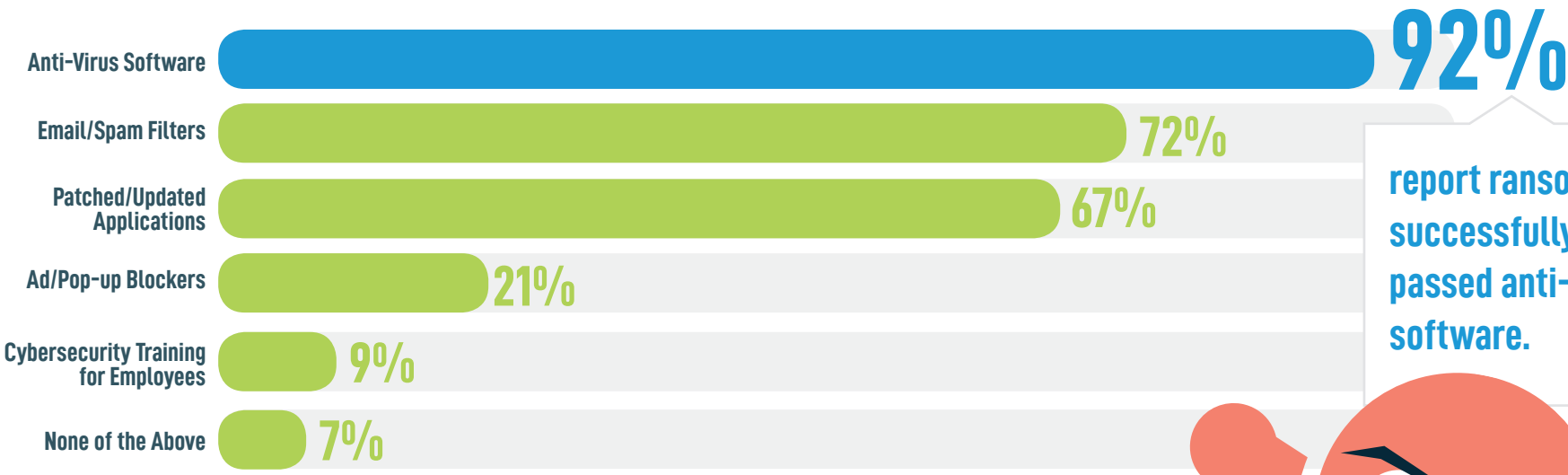
Q: From your experience, what would you say is the leading cause of a ransomware infection?

The majority of MSPs blame **phishing emails** followed by **lack of cybersecurity training across businesses.** It's safe to say the two go hand-in-hand.

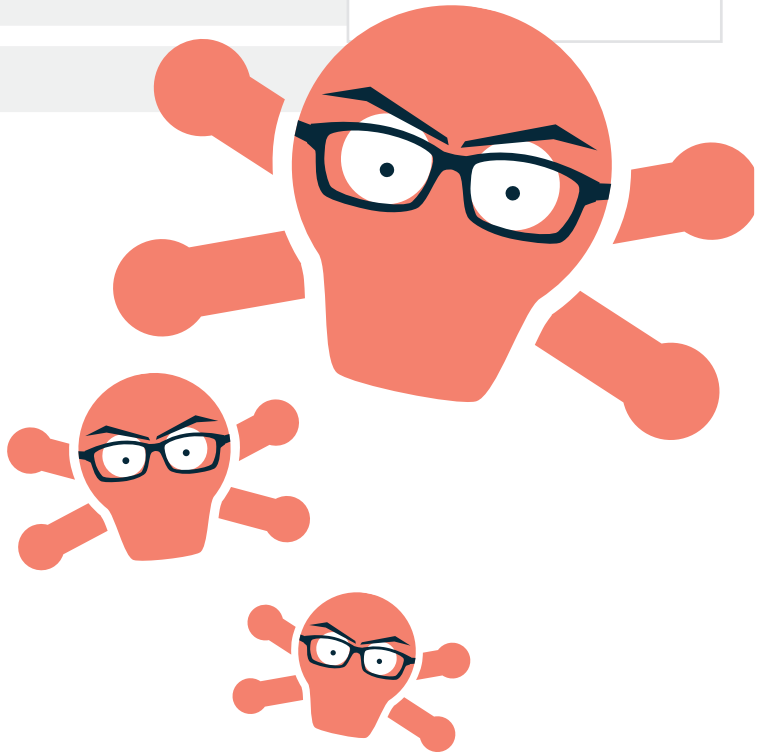


TOP CYBERSECURITY SOLUTIONS ARE NO MATCH FOR RANSOMWARE TODAY

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

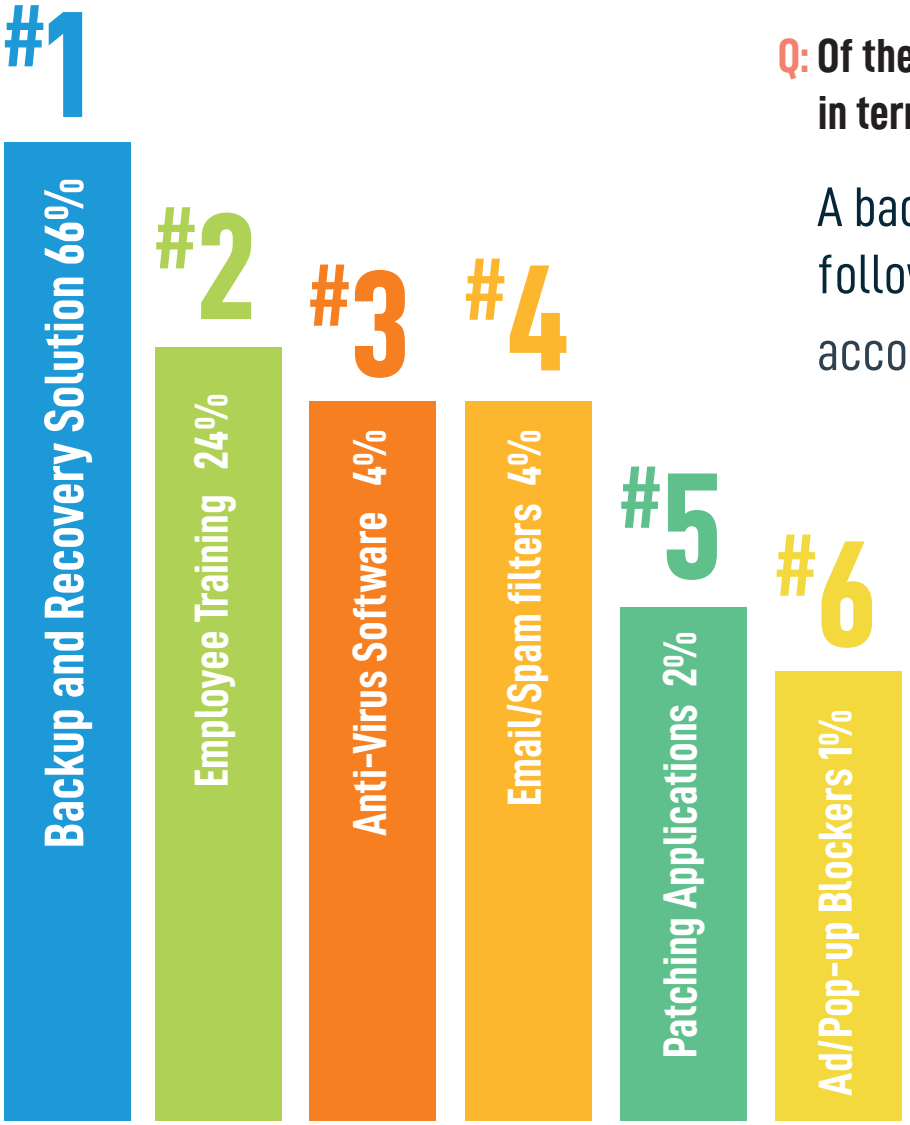


report ransomware successfully by-passed anti-virus software.



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?

A backup and disaster recovery (BDR) solution followed by cybersecurity training for all employees, according to the majority of Canadian MSPs.

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

WITH a reliable backup and recovery solution (BDR) in place,

96% 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.

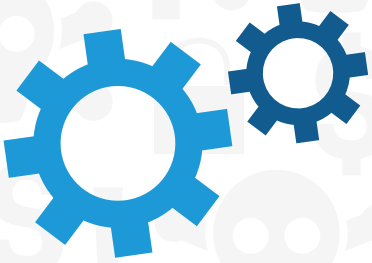
97% OF MSPS FEEL "MORE PREPARED"

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 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.

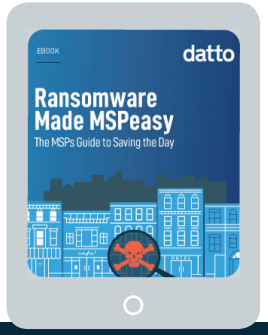
Datto protects all of your business data, no matter where it lives:

- **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 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/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 Canadian State of the Channel Ransomware Report is comprised of statistics pulled from a survey of 200+ managed services providers in the Canada.

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 Monroe, Rochester, Boston, Portland, Toronto, London, Singapore, Sydney, Frankfurt, and Amsterdam. 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.

Follow us on Twitter: @Datto