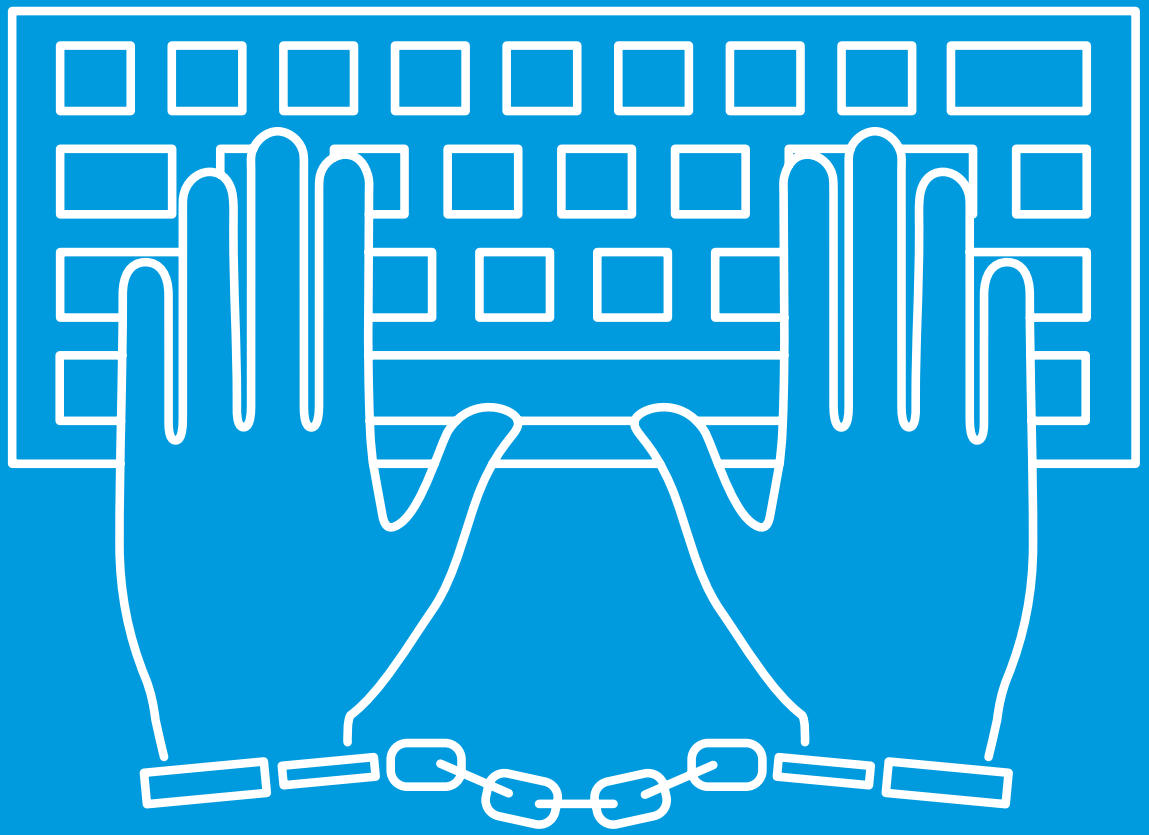
REPORT

datto

# DATTO'S STATE OF THE CHANNEL RANSOMWARE REPORT 2016

Follow us on Twitter: @Datto

Visit our Blog: www.datto.com/blog



# INTRODUCTION

If you Google "ransomware", the cyber attack in which hackers commandeer a company's data until a ransom is paid, the resulting headlines and statistics will all point to the same conclusion: the malware has become the most prominent, global threat to business cybersecurity today.

As data is the nucleus of today's businesses, ransomware has the potential to take out even the most stable businesses in a matter of minutes. While a growing number of companies are leveraging the recommended solutions for protection, such as backup and disaster recovery technologies and anti-virus software, many are not. The latter group includes a large number of small businesses who typically operate without a dedicated in-house IT expert and from antiquated systems. These businesses rely just as heavily on data as bigger organizations, yet they often operate without the proper data protections in place to defend against, prepare for, and recover from ransomware.

Today's cyber criminals, well aware of this vulnerability, are taking advantage and making billions. Yes, billions! Downtime from ransomware costs small businesses around $8,500 an hour.[1] In the US, this adds up to a loss of $75B+ per year. That's more than the combined GDP of Jamaica, Belize, Iceland, Cambodia and Nepal. That's more than the cost of buying the world a Coke ten times. And, since these criminals continue to operate with zero consequences, it's likely these crimes will get worse before they get better.

According to the Federal Bureau of Investigation's Internet Crime Complaint Center, there are nearly 2,500 complaints registered in 2015 representing $1.6M+ in damages. But the true numbers are far higher, as less than 1 in 4 incidents are actually reported.

In order to fight back against the ransomware epidemic, businesses must first be aware of the current threat they face. Next, they must implement reliable solutions and best practices as advised by the IT community and the authorities.

Datto surveyed 1,100 MSPs about ransomware and cybersecurity and published the key findings in this report. We aim to provide the Channel perspective on this growing epidemic and highlight the current prevalence of the malware, its behavior, its target, and its impact within the global small business community. In the end, we'll provide best practices and solutions for businesses looking to ensure total data protection, business continuity and disaster recovery.

1 http://resources.idgenterprise.com/original/AST-0113606_Analyst_Insight_Downtime_and_Data_Loss_How_Much_Can_you_Afford.pdf

# About This Report

With survey findings gathered from 1,100 Managed Service Providers (MSPs) in the US, Canada, Australia, the UK and around the world, Datto's report provides unique visibility into the current state of ransomware from the perspective of the Channel and the small businesses who are dealing with these malware infections on a daily basis.

The report provides a wealth of detail into ransomware, including its frequency, the most common strains, the industries and systems most targeted, the impact, and the strategies and critical business solutions necessary to ensure recovery and continuity in the face of the growing threat.

# Datto's Ransomware Protection and Recovery Solution

With Datto's ransomware detection feature, available on Datto 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 backup.

## Datto's ransomware enhancements include:

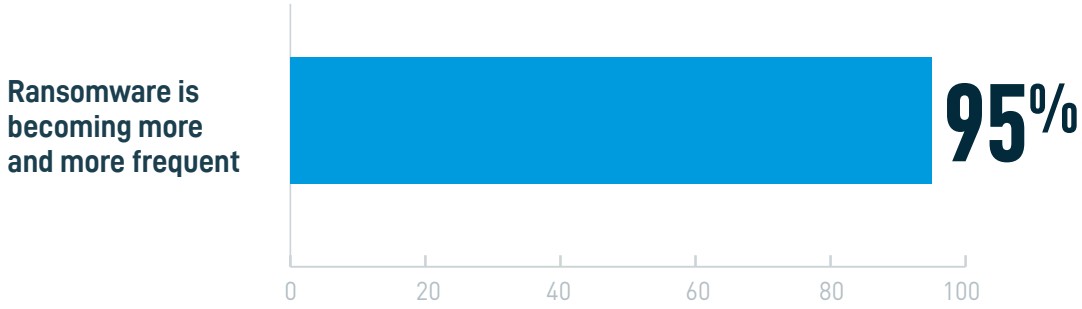
- **Datto NAS** Traditionally deployed as a cloud-protected network attached storage (NAS) device, the device now includes NAS Guard, which allows customers to protect the device and other network storage with full image rollbacks under one umbrella.
- **Backupify** Subscribers can roll files and data stored in software-as-a-service (SaaS) applications, such as Google Apps and Office 365, back to a known good state of health.
- **Datto Drive** Building on the ransomware lessons learned from Datto Backupify, Datto Drive now performs daily backups in the cloud and on customers' local appliances, protecting both from ransomware.

# KEY FINDINGS

- According to 97% of IT service providers, ransomware attacks on small businesses are becoming more frequent, a trend that will continue over the next two years.
- There is a large disconnect between IT service providers and their small business customers when it comes to feelings on the ransomware threat. The majority of former are "highly concerned" while only 34 percent of end users feel the same, likely due to lack of awareness.
- More than 91 percent report clients victimized by ransomware, 40 percent of whom have experienced 6 or more attacks in the last year.
- Around 31 percent of IT service providers have experienced multiple ransomware incidents in a single day.
- CryptoLocker is the most common strain impacting small businesses as 95 percent report customers contracting this variant.
- Less than 1 in 4 ransomware incidents are reported to the authorities.
- The leading cause of a ransomware infection is phishing email scam followed by a lack of employee awareness.
- Ransomware has evolved past today's top defense solutions, as 93 percent of IT service providers report customers victimized despite Anti-Virus / Anti-Malware software in place.
- The most common impact of a ransomware infection is business-threatening downtime followed by lost data and/or device.
- Paying the ransom doesn't guarantee the return of data; 7 percent of IT service providers report recent incidents of end users paying up to no avail.
- The average ransom requested is typically between $500 and $2,000, however 10 percent of MSPs reported the ransom average to be greater than $5,000.
- Windows is the most common system infected by ransomware followed by OS X.
- Only 3 percent of IT service providers report seeing a ransomware infection on a mobile device and/or tablet.
- Ransomware is targeting cloud-based applications as seen by 35 percent of IT service providers, particularly Dropbox, Office 365 and Google Apps.
- The leading industries victimized by ransomware: Professional Services, Healthcare, and Construction & Manufacturing.
- The #1 most effective solution for business protection from ransomware is a backup and disaster recovery (BDR).
- If small businesses has a backup and disaster recovery (BDR) solution in place, nearly 100 percent of MSPs dealing with ransomware have been able to resolve the issue.

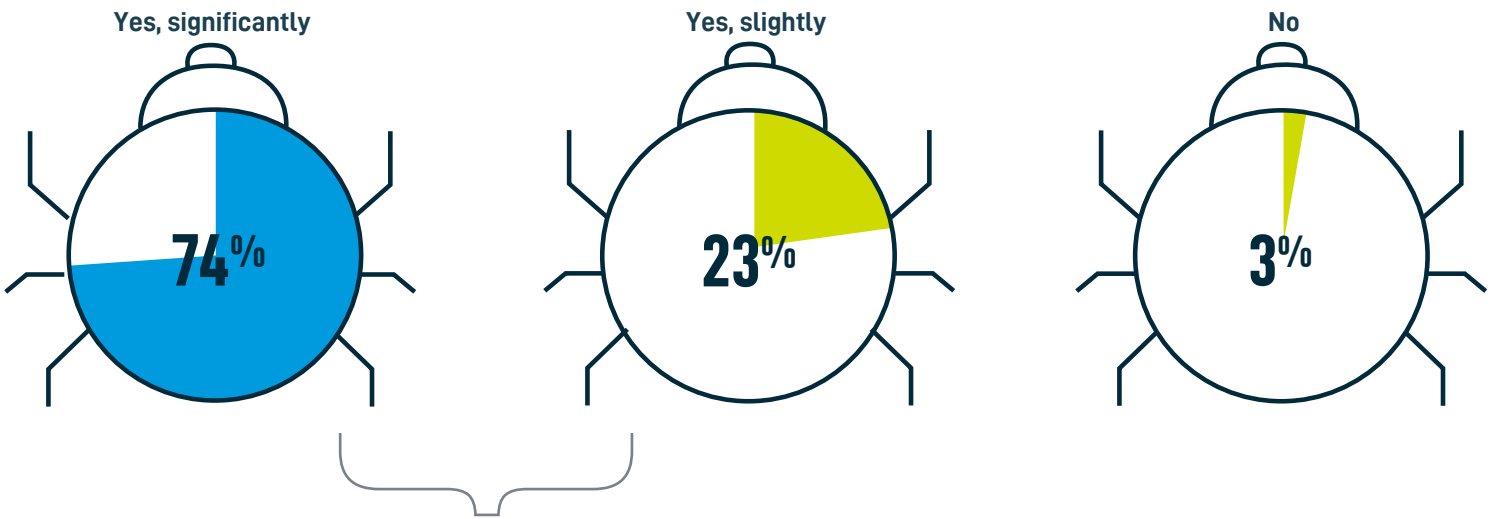
# MAJORITY OF IT SERVICE PROVIDERS AGREE: RANSOMWARE IS HERE TO STAY

▶ **With which of the following statements, do you most agree?**




**say ransomware is becoming more frequent.**

▶ **Will the # of ransomware attacks continue to increase over the next 2 years?**




**97% predict these incidents will continue to increase.**

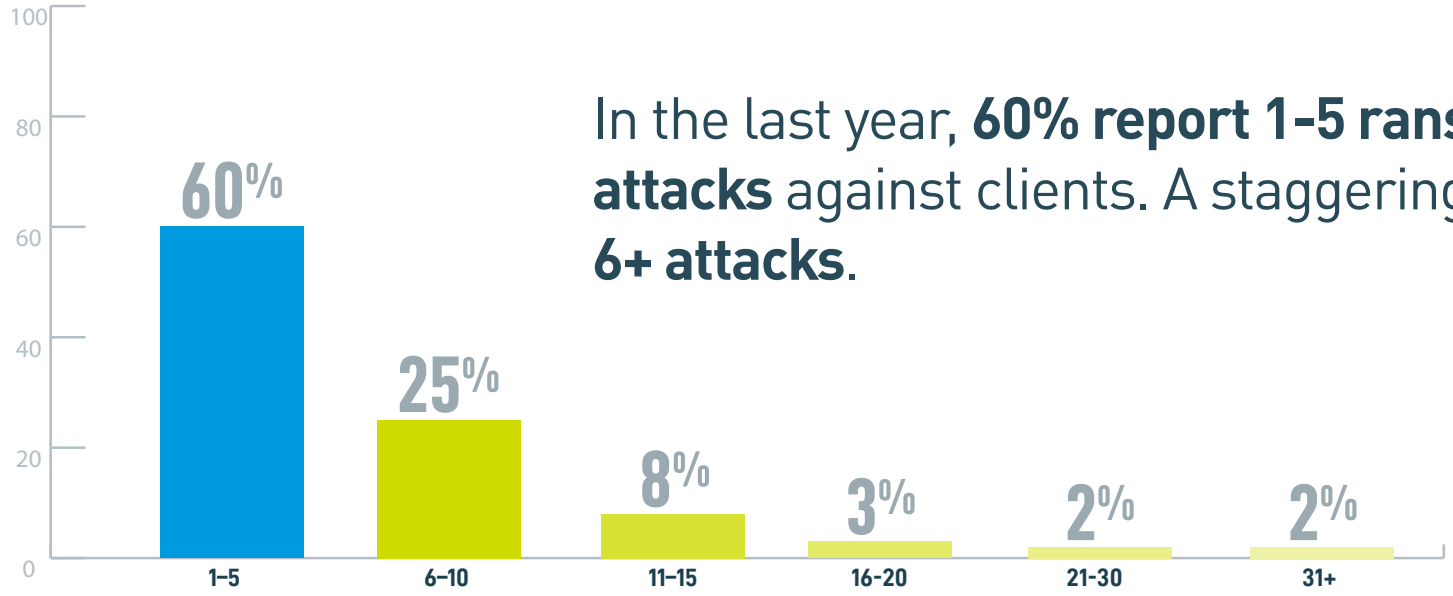
# FOR SMALL BUSINESSES IN PARTICULAR, RANSOMWARE INFECTIONS HAVE BECOME A COMMON OCCURRENCE

▶ **Have any of your small business clients recently become victims of a ransomware attack?**

The threat of falling victim to the malware is undeniable. In fact, **9 out of 10 managed services providers report recent attacks** amongst small business clients.

# FROM A MILD CONCERN TO A FULL BLOWN EPIDEMIC

▶ **How many clients experienced a ransomware attack in the last 12 months?**



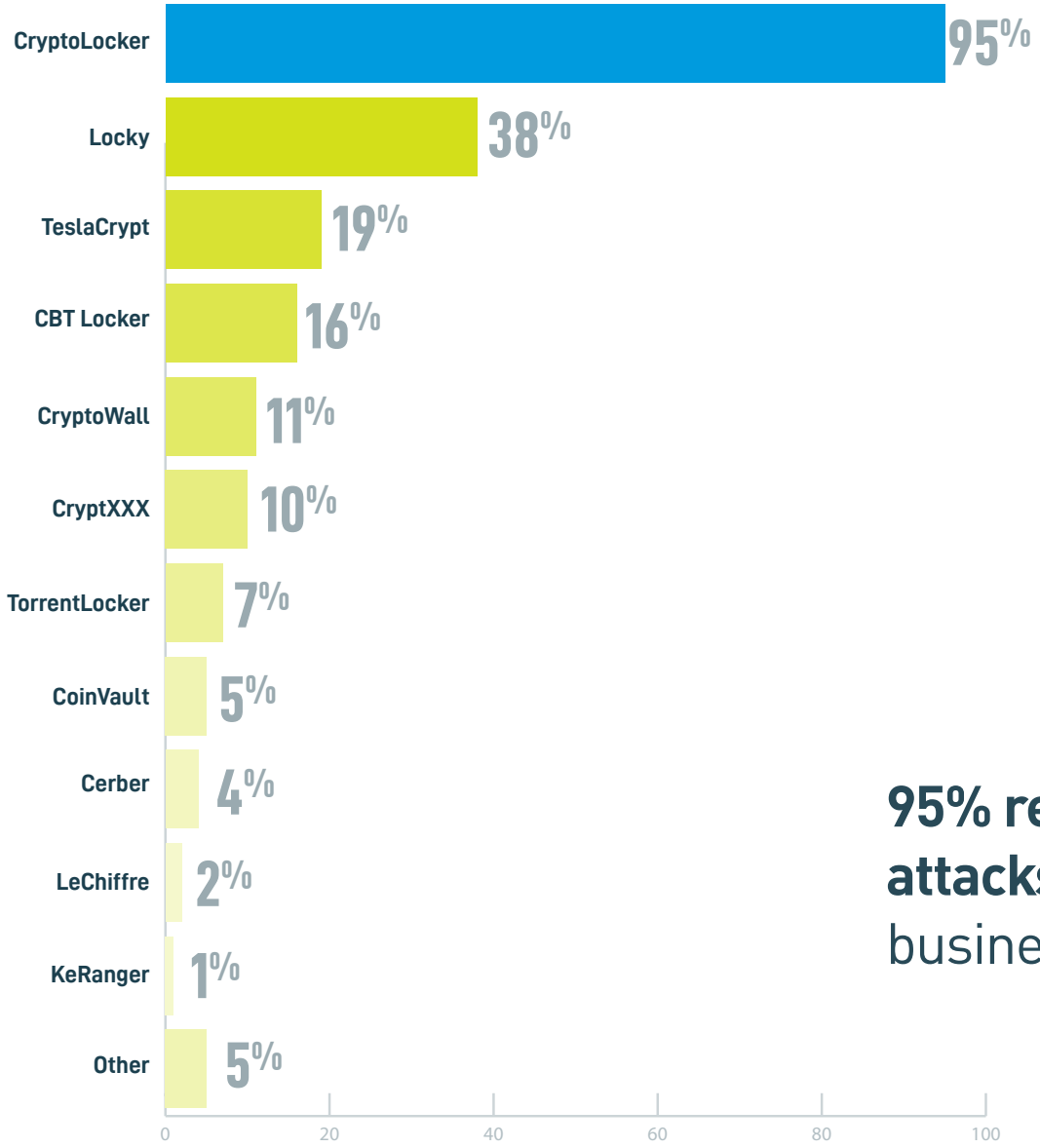

In the last year, **60% report 1-5 ransomware attacks** against clients. A staggering **40% report 6+ attacks**.

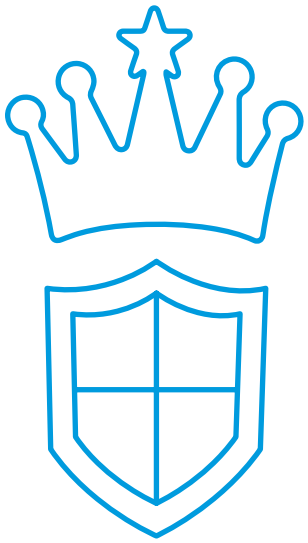
▶ **Have you ever experienced multiple ransomware attacks against multiple clients in a single day?**

An unlucky **31%** of IT service providers **experienced multiple ransomware attacks** against small business clients **in a single day.**

# CRYPTOLOCKER IS KING

▶ **Have any of your customers fallen victim to one or more of the following strains of ransomware?** (Check all that apply)

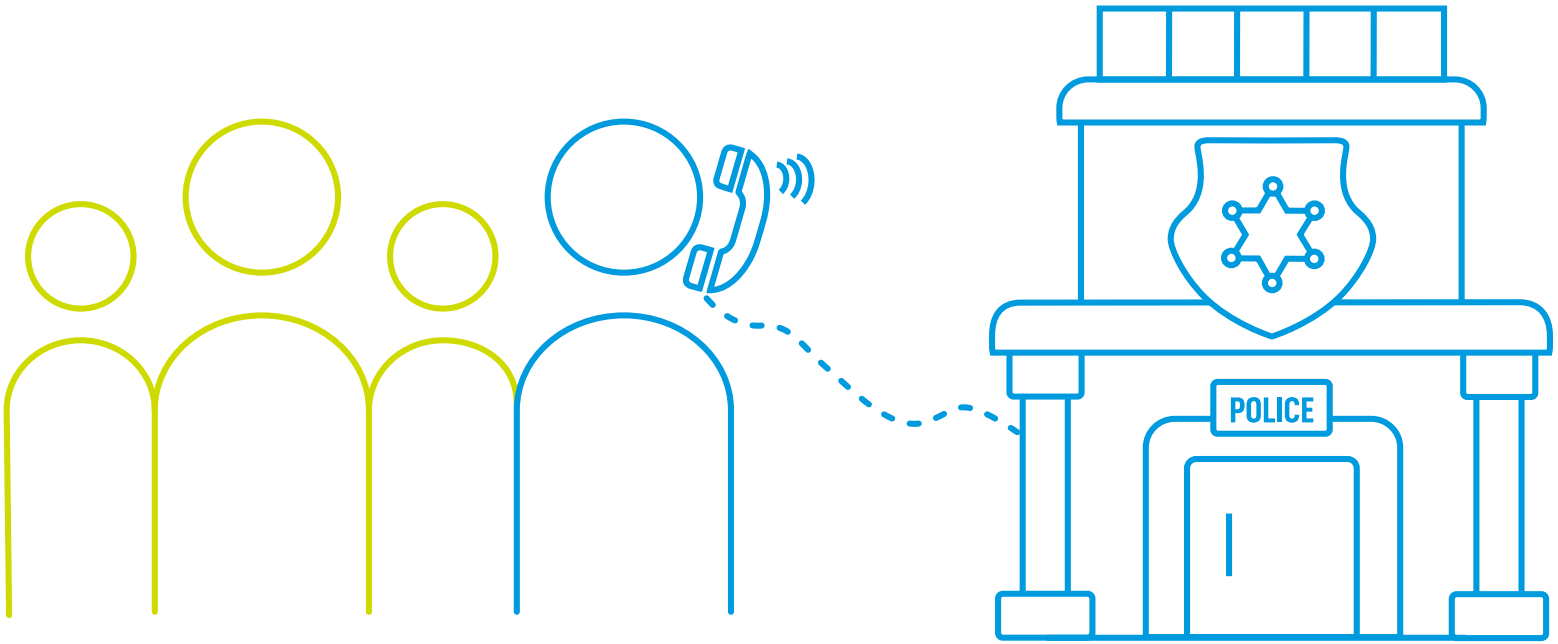


**95% report CryptoLocker attacks** against their small business customers.

# DESPITE THE FREQUENCY OF THE ATTACKS, RANSOMWARE IS RARELY REPORTED

▶ **Of the ransomware incidents you've encountered, what percent was reported to the authorities?**

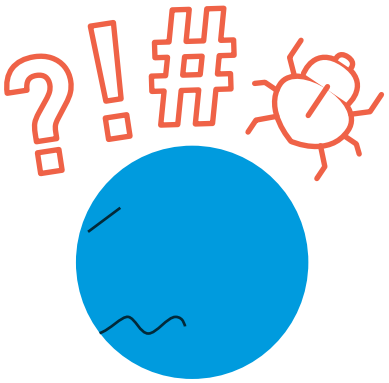



Less than **1 in 4 have reported ransomware to the authorities.**

# THE SIGNIFICANT DISCONNECT BETWEEN THE IT SERVICE PROVIDER AND THE CLIENT ON RANSOMWARE

▶ **How concerned are you about the threat of ransomware? How concerned are your small business customers?**

Who is **"highly concerned"** about the threat?



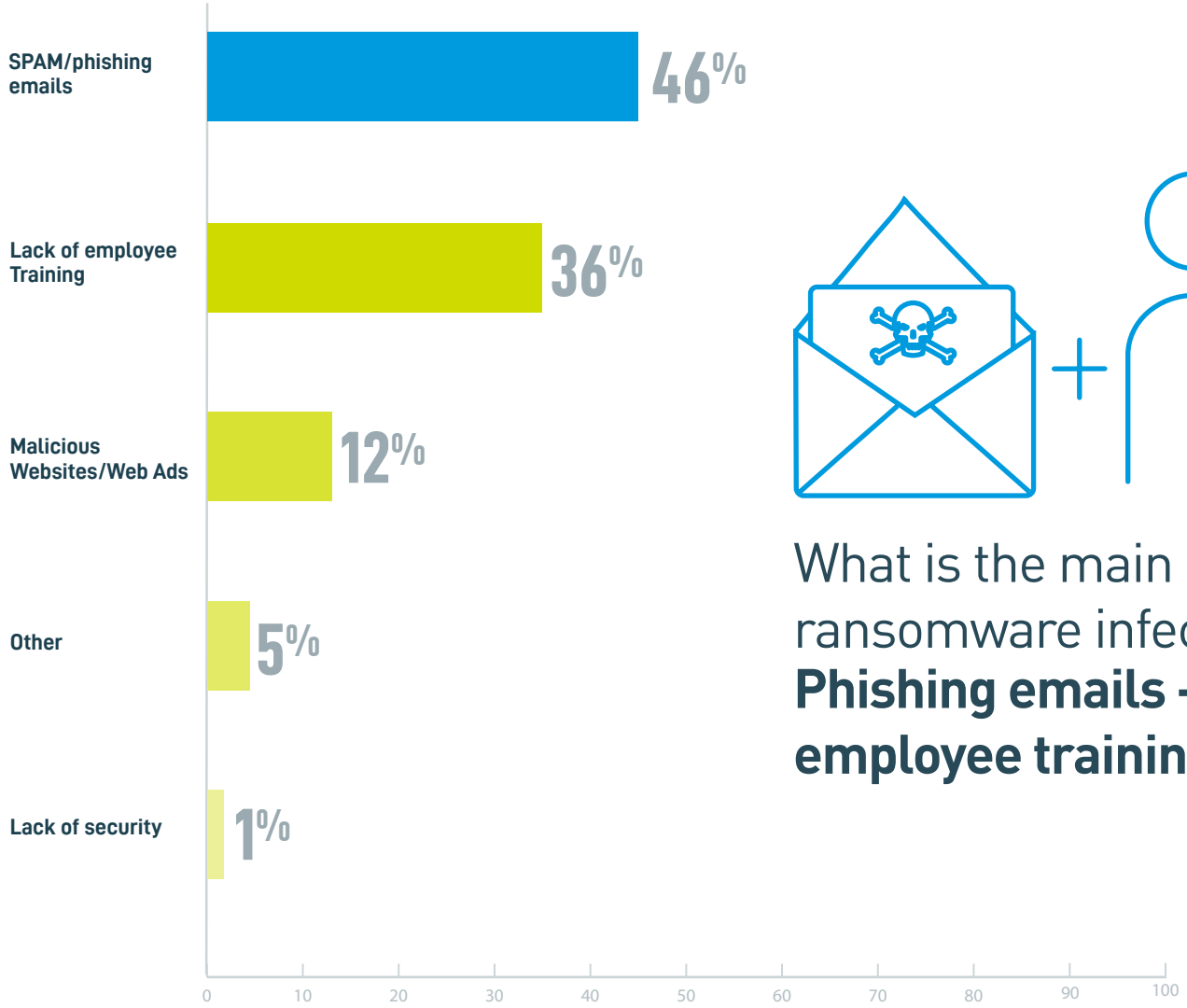
**88% of IT Pros**

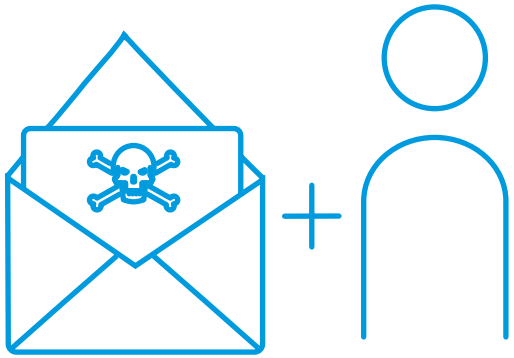
**Vs.**

**34% of Small Business Owners**

# PHISHING EMAILS PLUS A LACK OF EMPLOYEE TRAINING IS A BAD COMBO FOR CYBERSECURITY

▶ **From your experiences, what is the leading cause of a ransomware infection?**

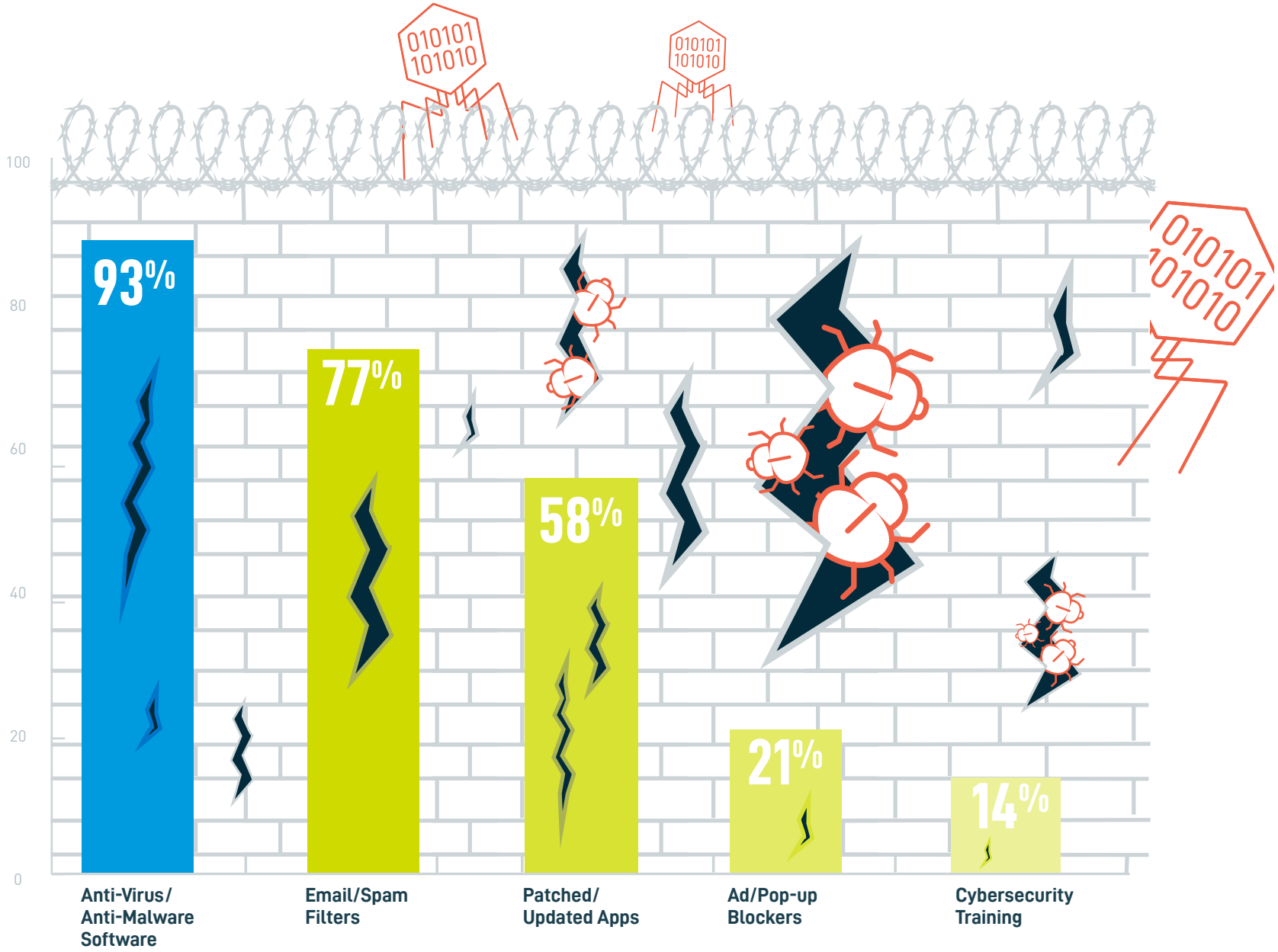


What is the main cause of a ransomware infection?
**Phishing emails + lack of employee training is to blame.**

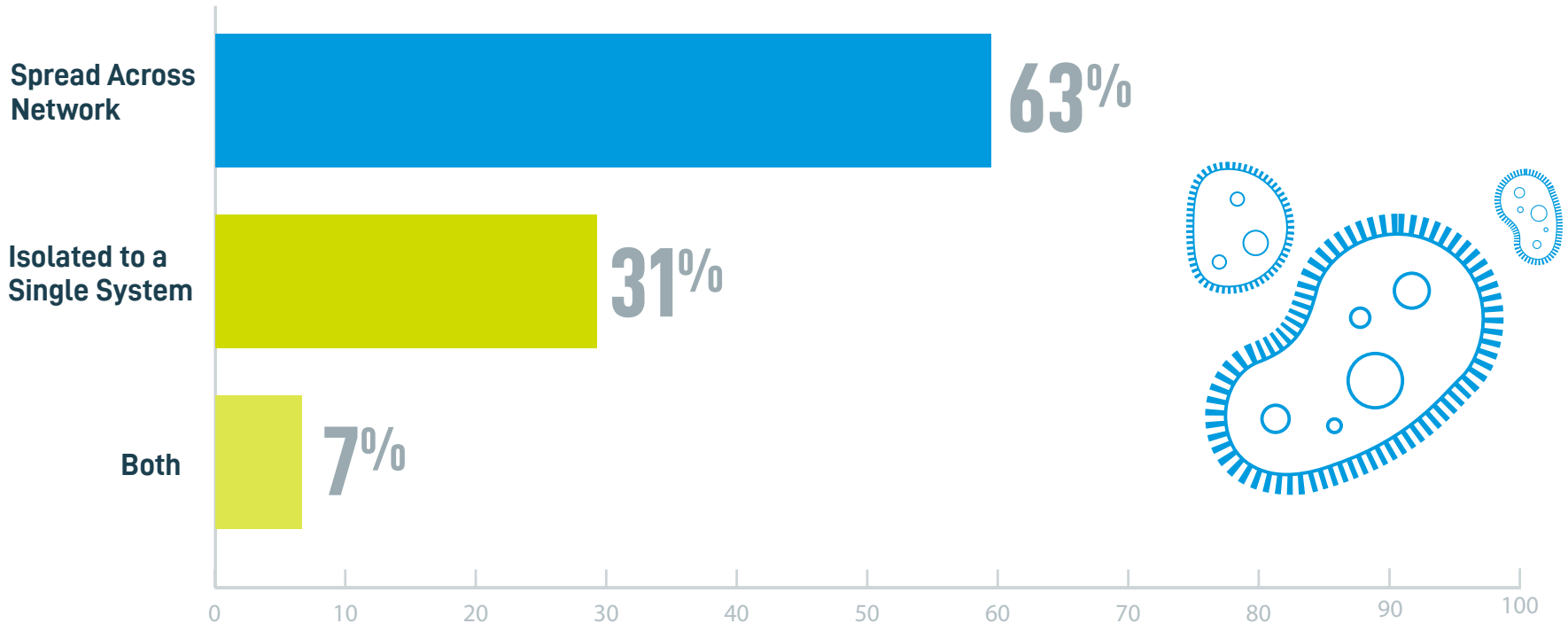
# RANSOMWARE OUTSMARTS TODAY'S TOP DEFENSE MEASURES

▶ **Of the ransomware attacks against your customers, had they implemented any of the following?** (Check all that apply)



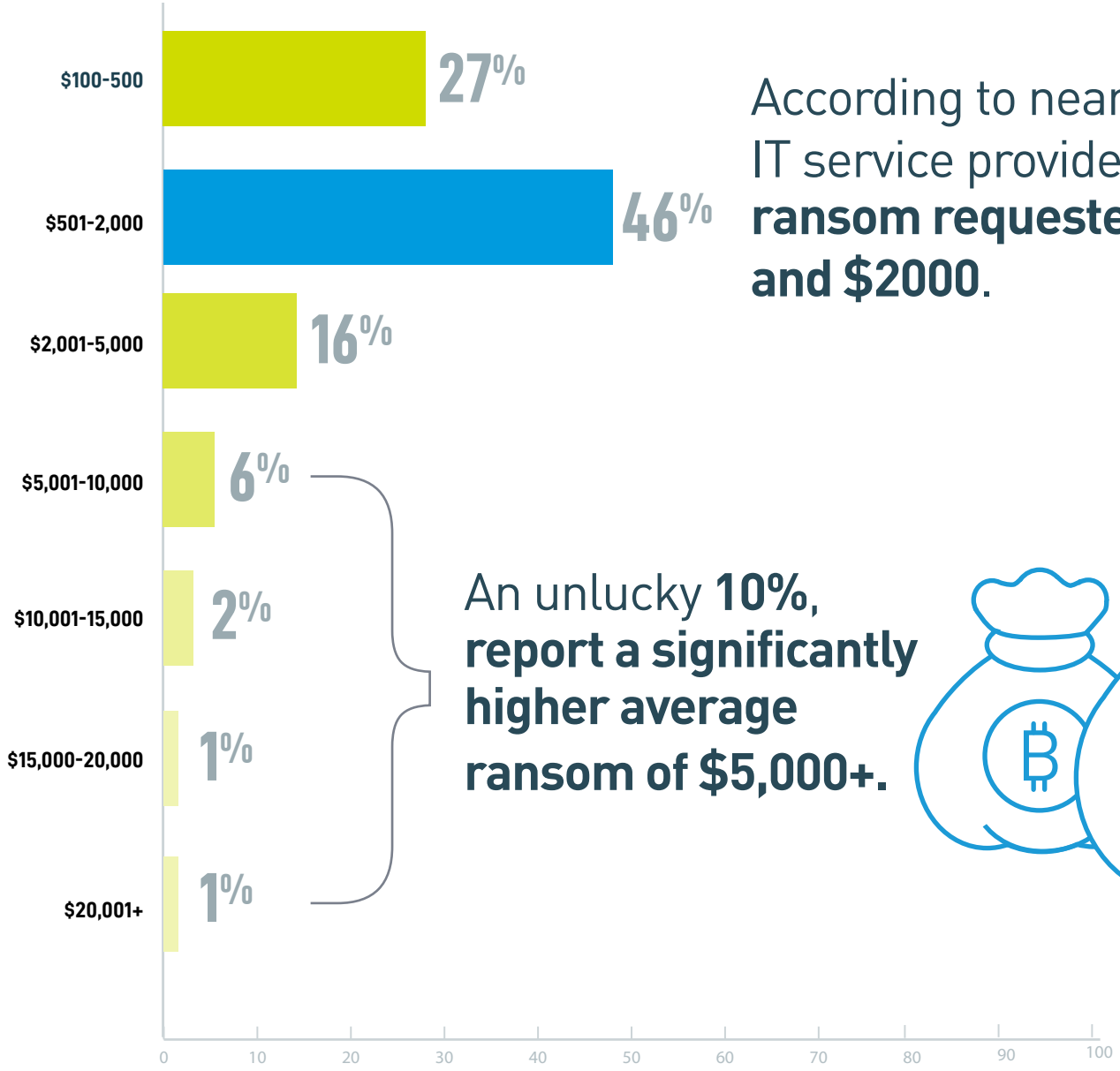
# RANSOMWARE IS CONTAGIOUS, SPREADS VIA SHARED RESOURCES

▶ **From your experience, is ransomware typically isolated to a single system or has it spread?**



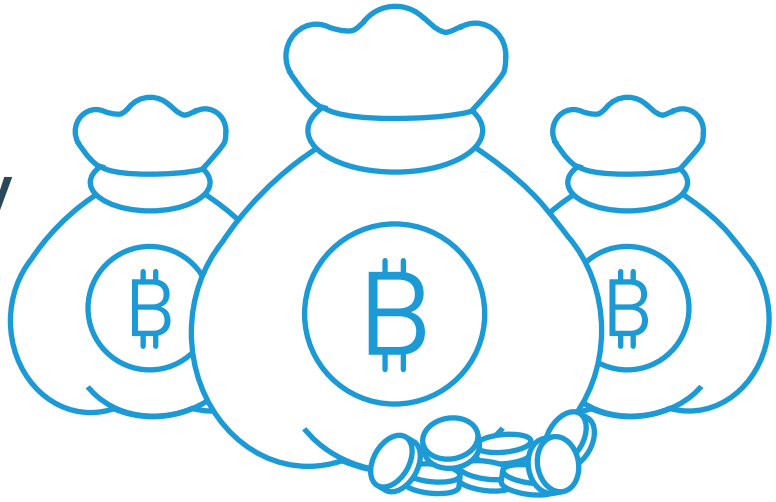
# THE RANSOM ISN'T WHAT BREAKS THE BANK

▶ On average, how much ransom is requested?



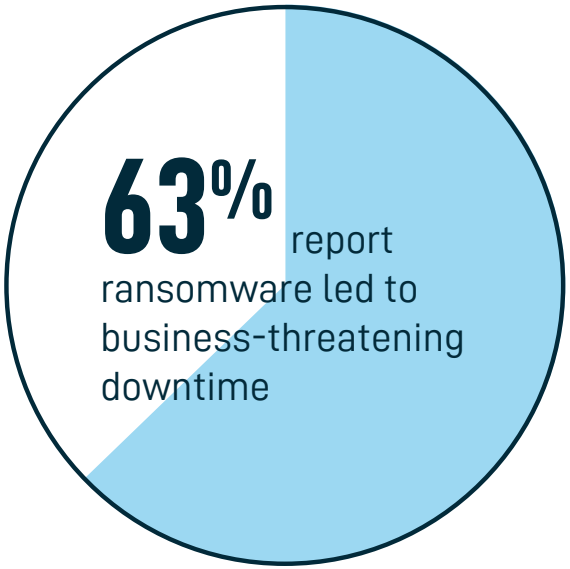

According to nearly 50% of the IT service providers, the **average ransom requested is between $500 and $2000**.

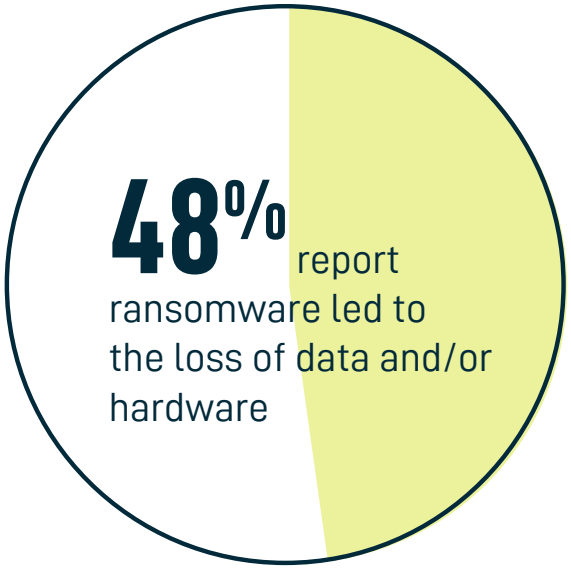
An unlucky **10%, report a significantly higher average ransom of $5,000+.**



# THE DOWNTIME AND DATA LOSS IS WHAT CUTS THE DEEPEST

▶ **Which of the following have your customers experienced because of a ransomware attack?**

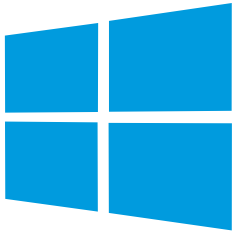



**42%** report customers **paid the ransom**, **1 in 4** of whom did so and **never recovered the data**. This is largely why the FBI recommends victims do not pay up.

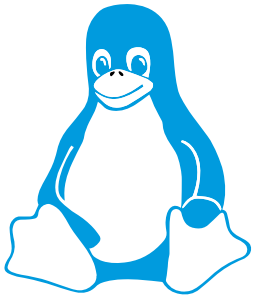
# WINDOWS IS THE LEADING SYSTEM TARGETED BY RANSOMWARE

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



**Windows 100%**

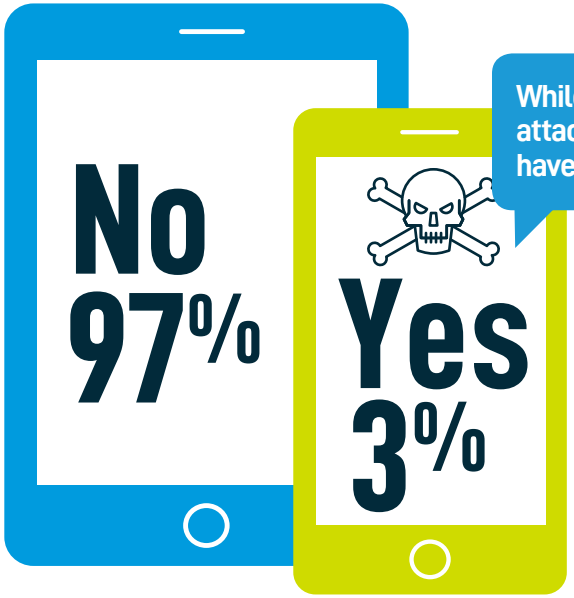
**OS X 3%**



**Linux 2%**

**Android 2%**

▶ **Have you dealt with a customer with ransomware on a mobile or tablet device?**

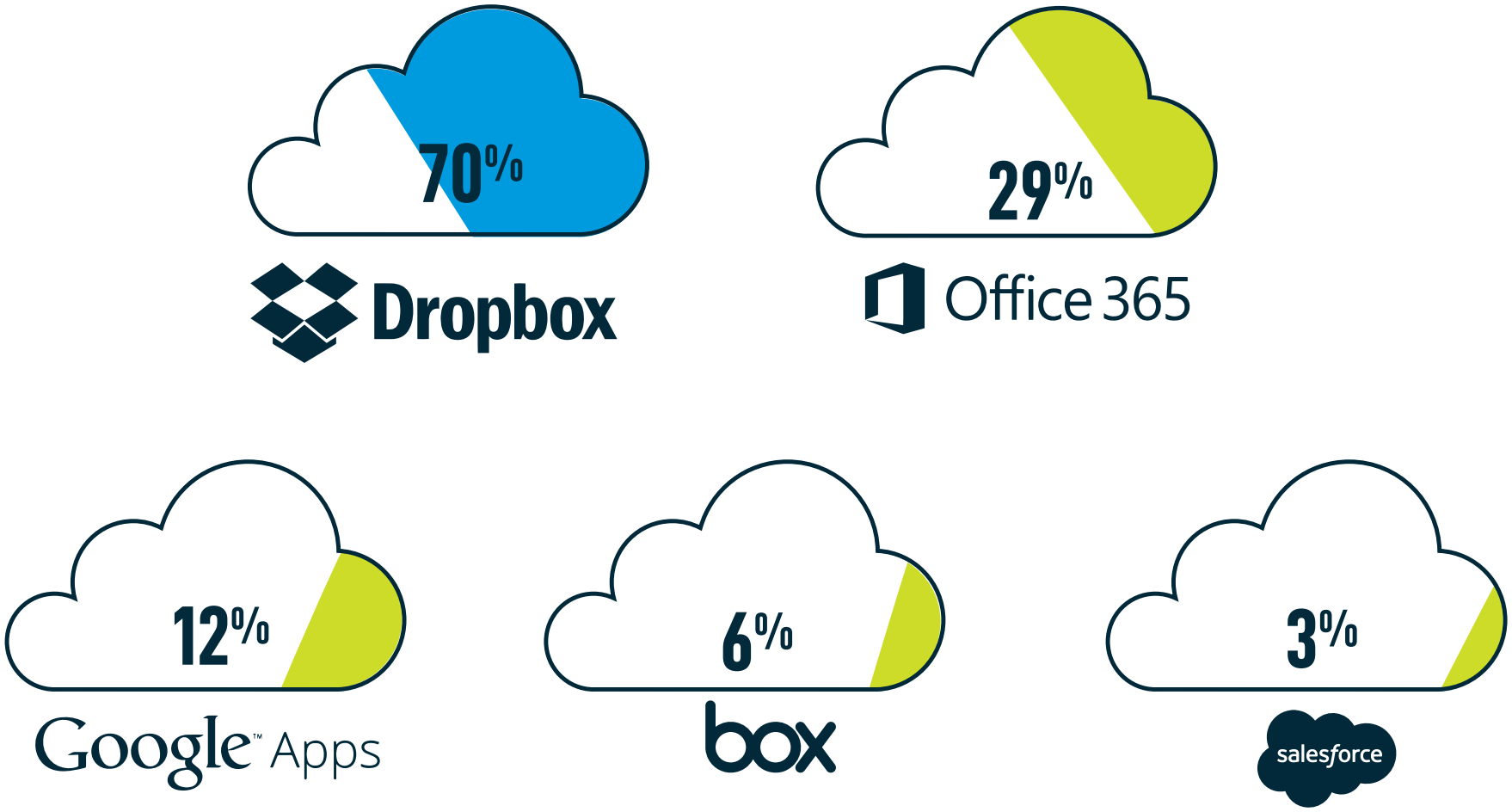



While news reports a growing # of ransomware strains attacking mobile devices, only 3 percent of IT service providers have dealt with this..

# DESPITE POPULAR BELIEF, THE CLOUD IS NOT IMMUNE TO RANSOMWARE

**35% report ransomware in the cloud,** particularly within the following popular SaaS applications: Dropbox, Office 365 and Google Apps.

▶ **Have your clients experienced ransomware infect any of the following cloud-based applications?** (Check all that apply).



# PROFESSIONAL SERVICES, HEALTHCARE, CONSTRUCTION & MANUFACTURING ARE MAJOR TARGETS

▶ **What industries have you seen infected with ransomware?** (Check all that apply).

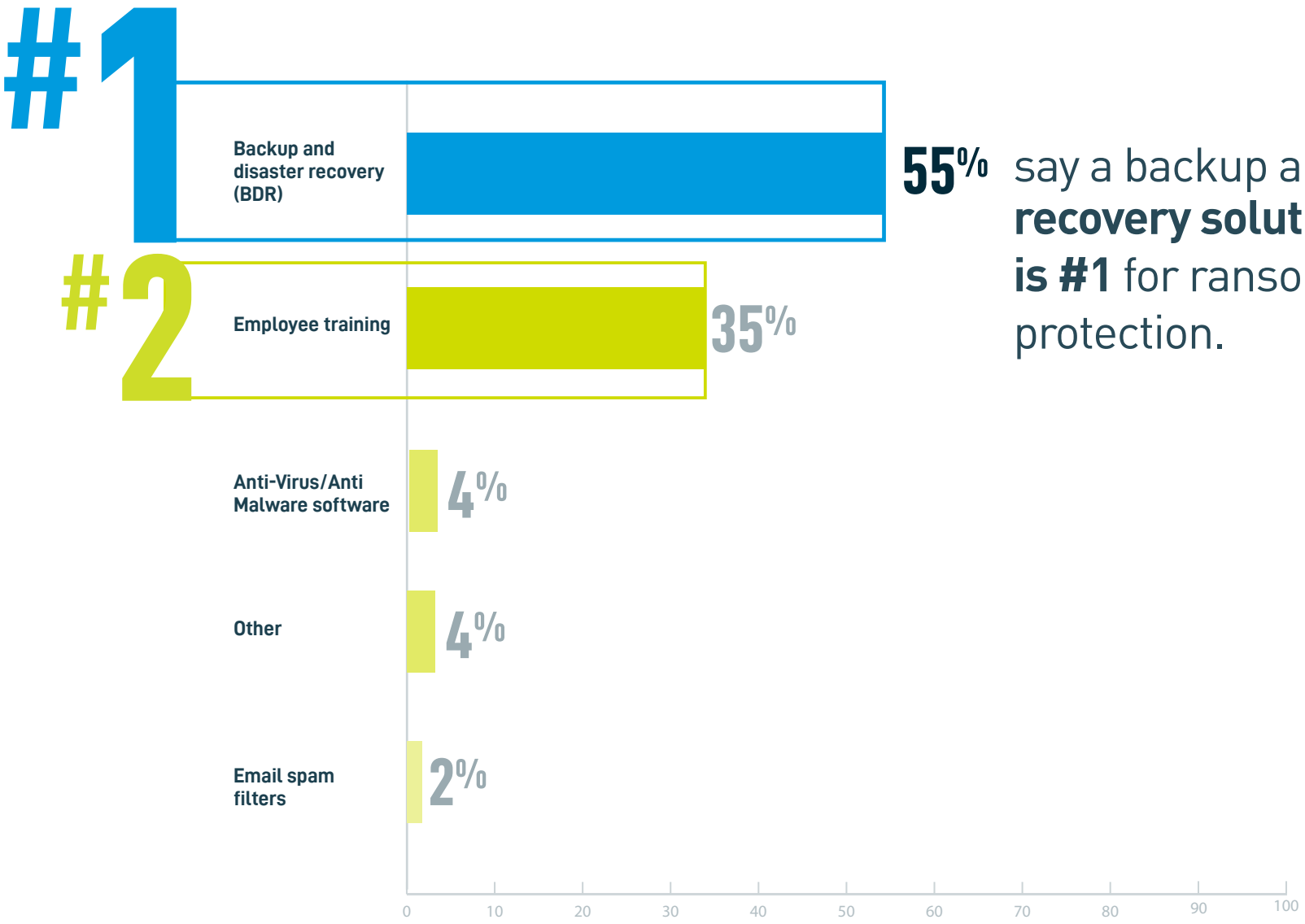
| #1 | #2 | #3 |
|---|---|---|
| Professional Services | Healthcare | Construction + Manufacturing |
| 44% | 38% | 33% |

| Non-profit | Finance + Insurance | Retail | Consumer Goods | Legal | Education |
|---|---|---|---|---|---|
| 27% | 25% | 17% | 16% | 13% | 12% |

| Government | Energy + Utilities | Transportation | Media & Entertainment | Telecom/Tech | Real Estate |
|---|---|---|---|---|---|
| 10% | 9% | 9% | 6% | 6% | 4% |

# BACKUP AND DISASTER RECOVERY (BDR) MOST EFFECTIVE RANSOMWARE PROTECTION

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




55% say a backup and **recovery solution is #1** for ransomware protection.

# WITH BDR IN PLACE, RECOVERY IS MUCH MORE LIKELY

▶ **Do you feel more prepared for a ransomware attack if your customer has a backup and disaster recovery (BDR) solution in place?**


The majority of **MSPs feel "more prepared" with BDR.**

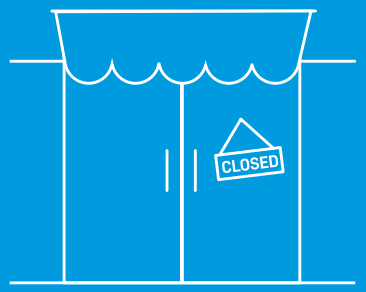


Why does BDR bring such confidence? It works! With a good **BDR solution in place, 97% have quickly resolved the issue.**

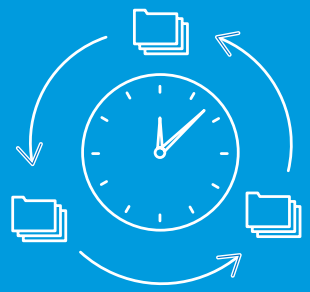

On the flip side, **without BDR, only 68% have fully recovered the data.**

# FINAL TAKEAWAYS

Ransomware attacks have become a common, growing occurrence for small businesses around the world. According to IT service providers, the majority of end users aren't as concerned as they should be, making them even more vulnerable to an infection.




While the typical ransom requested won't break the bank, the cost of downtime and data loss that typically follows an attack is what cuts the deepest.



Today's leading security solutions are no match for today's ransomware, including anti-virus software and email filters. The most effective means for business protection from ransomware is a backup and disaster recovery (BDR) solution.

Malicious emails coupled with a general lack of employee cybersecurity training is the leading cause of a successful ransomware attack. Today's businesses must provide regular cybersecurity training to ensure all employees are able to spot and avoid a potential phishing scam in their inbox, a leading entrance point for the malware.

# CONCLUSION

Until now, very few studies have examined the current prevalence and ramifications of ransomware attacks on small businesses. The results from this study further emphasize that these companies in particular are incredibly vulnerable to ransomware, which can lead to significant downtime, data loss, financial losses and, of course, a damaged reputation. We learned that paying the ransom doesn't help the situation - not only does it further fuel the crimewave, but it also doesn't guarantee the data will be returned.

The ransomware challenge requires a combination of innovative technologies and end user education. As the ransomware variants continue to evolve to a level of sophistication that surpasses our top defense solutions, so must the approach to thwart these threats.

Standard preventative measures, such as anti-virus software, SPAM filters, and regularly updating systems should be taken, but 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.

Lastly, as most ransomware attacks start with the single click of an employee's mouse, companies must ensure all employees are regularly trained on cybersecurity best practices, including how to avoid phishing scams and spot a bad website.

It's vital for businesses of every size to review their cybersecurity and data backup procedures to ensure that they can protect their business but also restore their data smoothly in the event of a ransomware incident.

# ADDITIONAL RESOURCES

## You Also Might Be Interested In:

EBOOK
**Ransomware Made MSPeasy**
DOWNLOAD NOW


EBOOK
**The Business Guide to Ransomware**
DOWNLOAD NOW

EBOOK
**Stopping Crypto Ransomware Infections in SMBs**
DOWNLOAD NOW

## Knowledge is Power: Ransomware Education for Employees

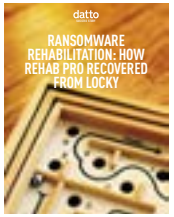

SLIDESHARE
**What is Ransomware?**
VIEW

BLOG
**5 Social Engineering Tactics of Hackers (How to avoid them!)**
VIEW

ARTICLE
**The US Department of Homeland Security's Alert - Ransomware and Other Variants**
VIEW

## Ransomware Survivor Stories:


**No Room at the Inn for Crypto-Creeps:** How Crowne Plaza survived CryptoLocker attack
HERE




**Ransomware Rehabilitation:** How Rehab Pro Recovered from Locky
HERE


**Merry CryptoLocker:** How Backup and Recovery Saved the Vacation
HERE

## Stay Up-To-Date on All Things Ransomware

SUBSCRIBE
to The Datto Blog

CHECK OUT
The Datto Website

# ABOUT THE SURVEY

Datto's 2016 State of the Channel Ransomware report is comprised of statistics pulled from a survey of nearly 1,100 managed services providers in the US, Canada, Australia, the UK and around the world.

To learn more about the results, please reach out to Katie Thornton, Content Marketing Manager at Datto, Inc.

# ABOUT DATTO

Datto protects essential business data for tens of thousands of the world's fastest growing companies. Our Total Data Protection platform delivers uninterrupted access to data on site, in transit and in the cloud. Through Datto's network of partners, we provide companies with products and services designed to continually keep business running. Businesses rely on Datto for industry leading technology combined with unrivaled customer service. Datto is headquartered in Norwalk, Connecticut, and has offices in Rochester, Boston, 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.



Follow us on Twitter: @Datto

## ABOUT NETCETERA

Netcetera is a Datto Enterprise Partner located in North Vancouver British Columbia. Netcetera was the first company to bring Datto products into Canada. We are a long term member of the Datto Partner Advisory Council and the recipient of the Datto 2015 Community Partner of the Year award. All of our technical and sales consultants are fully certified on the Datto BDR products. If you are considering a Backup and Disaster Recovery solution from Datto, we are available to assist you in selecting and implementing the right products. After inplementation, we will provide ongoing monitoring and management of all your backups so you can go back to what you do, running your business.

To learn more contact Netcetera... by e-mail at sales@netcetera.ca or by phone at 604-980-2700. You can also visit our web site at www.netcetera.ca