PROTECTING YOUR BUSINESS IN THE DIGITAL AGE

CARBONITE

TABLE OF CONTENTS

A NEW WORLD OF DATA

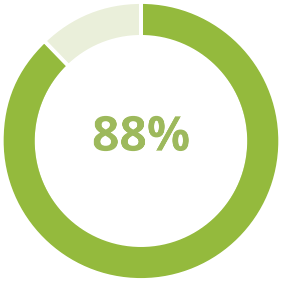
In today's data-driven business climate, the stakes have never been higher for businesses safeguarding their most valuable assets – data. With **63 percent of small and midsize businesses either executing or planning to execute data-driven projects this year**, it's safe to say that many are beginning to view their data as currency.[1] But for those tasked with managing and protecting these technical projects, the challenges of the digital age can seem daunting.

To better understand how businesses are tackling the increasingly complex IT landscape, Carbonite commissioned Regina Corso Consulting to survey small and midsize businesses regarding their top concerns with data protection. All 251 participants were IT decision makers at U.S. companies with 250 or fewer employees. Carbonite uncovered four key areas of concern, which we'll explore in this eBook: data protection, IT security, cloud environments, and data privacy and compliance.

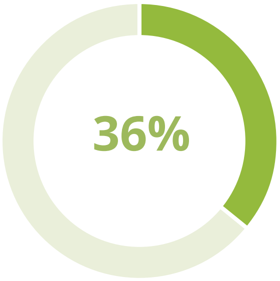
ROLLING THE DICE ON DATA PROTECTION

Nearly half of businesses (47 percent) report that fear of losing data is one thing that keeps them up at night, and with good reason – it's likely to happen! In the past year, almost one-quarter (22 percent) have experienced data loss, with nearly 50 percent recovering less than half of their data. This is a common – and costly – challenge businesses face in the digital age. According to IDC, 80 percent of small and midsize businesses have experienced downtime in the past, with associated costs ranging from $82,200 to $256,000 per event.[2]

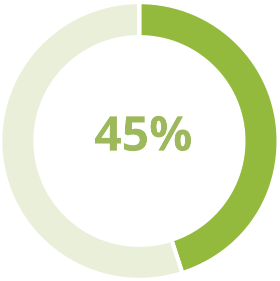
But while a majority understand the importance of having a disaster recovery plan in place, surprisingly few actually have one.



88% of small businesses equate a disaster recovery plan to a data insurance policy

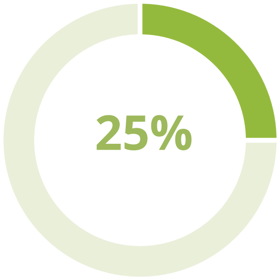


Only **36%** of small businesses have a detailed disaster recovery plan in place

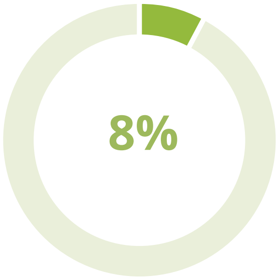


45% of small businesses have only a BC/DR framework

Carbonite's research found that organization size directly correlates with respondents' interest and investment in disaster recovery planning.



25% of companies with fewer than 100 employees have no disaster recovery plan in place

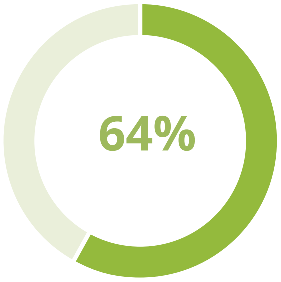


8% of companies with 100-250 employees have no disaster recovery plan in place

This could be because the likelihood of a data disaster increases alongside employee count.

While 39 percent of larger organizations surveyed experienced data loss in the past year, only 12 percent of businesses with fewer than 100 employees experienced the same.

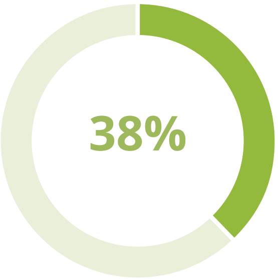
Not surprisingly, those smaller businesses were less likely to have a separate budget for disaster recovery solutions and were more likely to "roll the dice" on data protection. But is this wise?



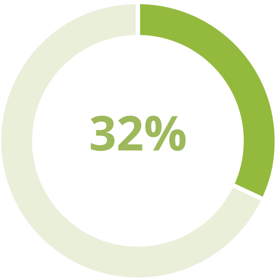
64% of IT pros believe that their organization would go out of business if they experienced a data loss event without backup protection[3]

IT SECURITY: CAN YOU HACK IT?

Finding your organization at the center of a data heist used to be the burden of enterprise IT, but in today's data-centric world, no business is safe. IT security incidents have nearly doubled since 2011, according to PricewaterhouseCoopers, and concern among small and midsize businesses has risen alongside this risk.[4]



38% of businesses have experienced internal IT security incidents in the past year



32% of businesses have experienced external IT security incidents in the past year

But while stories of external hacks have made headlines, most organizations are still focused on internal threats propagated by their own employees. That could be because viruses, malware and ransomware are wreaking havoc on businesses at a steadier pace than ever before.

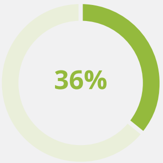
GET THE FACTS: RANSOMWARE

RAN·SOM·WARE

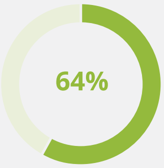
[NOUN] – a type of malicious software designed to block access to a computer system until a sum of money is paid.

Modern ransomware first appeared in 2005

TWO MOST PREVALENT TYPES OF RANSOMWARE:



LOCKER RANSOMWARE
Denies access to
the computer or device



CRYPTO RANSOMWARE
Prevents access
to files or data

TOP SIX COUNTRIES IMPACTED BY RANSOMWARE IN 2015:

United States | Japan | United Kingdom

Italy | Germany | Russia

AVERAGE RANSOM AMOUNT

U.S.
$300

AT-RISK DEVICES:

COMMON ATTACK METHODS

Malvertisements
Spam Emails | Botnets

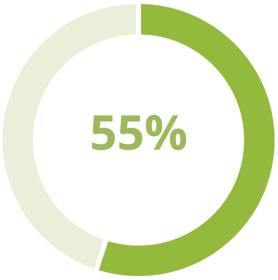
TO PAY OR NOT TO PAY?

NO!

Report instances of fraud to the
FBI/Internet Crime Complaint Center

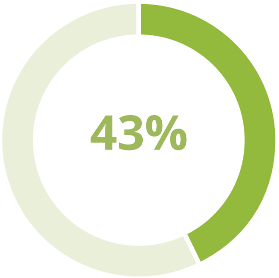
HOW TO PROTECT YOUR BUSINESS:

- Perform **regular data backups**
- Maintain up-to-date **anti-virus software**
- Keep your operating system and software **up-to-date**
- Warn employees not to open **unsolicited web links**
- **Use caution** when opening email attachments



55% of SMB IT decision makers surveyed are more concerned with internal threats than outside forces, such as hackers

Not surprisingly, **concern over internal risks increases alongside employee count** – nearly three in four organizations with 100-250 employees are more concerned with internal threats, while just under half of small organizations feel the same.



43% of respondents say they wouldn’t know what to do if they were hacked

This highlights a need for further education and planning for both internal and external security risks.

EMPLOYEE ERROR

TECHTIP

HOW TO PROTECT YOUR BUSINESS...FROM ITSELF!

According to a new study by CompTIA, human error is the cause of more than half of all security breaches in the U.S. This shouldn't come as a surprise. Carbonite's own research shows that a majority of business owners consider internal threats from employees – who may unknowingly open an infected email, for example – greater than external cyber-attacks. With viruses, malware and ransomware more prevalent than ever, it's vital that business owners put these three safeguards in place:

TRAIN EMPLOYEES TO BE SECURITY-AWARE

The first step in protecting your data from cyber-attacks is educating your employees. Attack methods are getting more sophisticated every day and employees are easily fooled by emails, links and attachments that masquerade as everyday business requests from clients and partners.

It only takes one click for viruses, malware and ransomware to infiltrate your organization and compromise your data. Make sure your employees are aware of the latest methods being used by cyber-criminals and advise them to avoid interacting with any suspicious emails or documents.

TEST EMPLOYEES' SECURITY SAVVY

One of the best ways to teach employees how to avoid falling victim to cyber-attacks is to test them regularly in real-life scenarios. Many IT security vendors offer solutions that allow you to simulate the latest phishing tactics and test your employees' responses. You will gain insight into common mistakes and your employees will gain exposure to the latest threats.

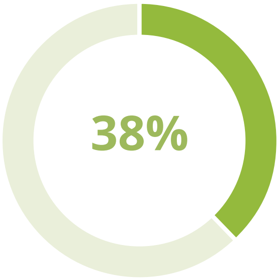
BACK UP VITAL DATA

While investing in firewall protection and security software should be a first step, those safeguards won't guarantee complete protection. To ensure your vital data is never lost, you should also back up regularly to both on-premise and cloud environments. Invest in a service that offers automatic, versioned backup and excellent customer service to ensure a seamless, speedy recovery. Most importantly, test the backup system's restore capabilities on a regular basis so you know your data will be in a usable state when you need it most.

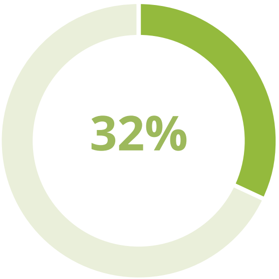
DATA DECISIONS: COMPLIANCE, PRIVACY AND THE CLOUD

Data has never been more valuable to businesses than it is today.

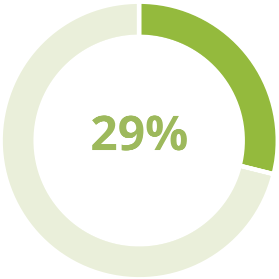
It's also never been more challenging to maneuver or protect. The IT landscape is growing in complexity, leaving businesses caught in a web of compliance and privacy regulations. More than half of businesses surveyed feel that data privacy concerns are now worse for IT than they are for healthcare professionals.



38% of businesses report that they have to meet HIPAA regulations



32% of businesses report that they have to meet ISO standards



29% of businesses report that they have to meet PCI standards

A small portion (8 percent) are still unsure of what regulations their business needs to meet.

More than half of survey respondents feel that data privacy concerns are now worse for IT than they are for healthcare professionals.

So, what is driving this shift? As businesses dive deeper into the digital realm – moving paper processes online and adopting cloud computing – tighter oversight of company data is needed to make sure protected information isn't exposed. More small and midsize businesses are embracing cloud computing than ever before.

HIPAA COMPLIANCE COMPASS

More than two-thirds of businesses must meet regulations, with HIPAA being the most prevalent. It's more important than ever for businesses to ensure they're compliant, as consequences (and monetary fines) can be steep.

Companies required to meet HIPAA regulations must meet a number of administrative, physical and technical safeguards to stay in compliance.

ADMINISTRATIVE SAFEGUARDS

These include administrative actions, policies and procedures to protect electronic protected health information (ePHI). For example:

RISK MANAGEMENT

Businesses must implement security measures to reduce risks and vulnerabilities to ensure the confidentiality, integrity and availability of data.

LOGIN MONITORING

Businesses must implement procedures for monitoring log-in attempts and reporting discrepancies.

PHYSICAL SAFEGUARDS

Physical measures, policies and procedures to protect electronic information systems and related buildings and equipment. For example:

ACCESS CONTROL AND VALIDATION PROCEDURES

Businesses must control and validate a person's access to facilities based on their role or function.

DISPOSAL

Businesses must implement policies and procedures to address the final disposal of ePHI and/or the hardware or electronic media on which it is stored.

TECHNICAL SAFEGUARDS

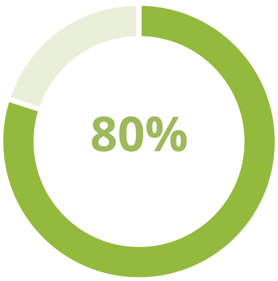
Policies and procedures that ensure stored PHI is adequately protected and access is controlled. For example:

ENCRYPTION AND DECRYPTION

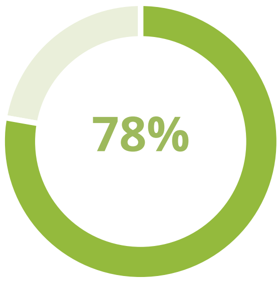
Businesses must implement a mechanism to encrypt and decrypt ePHI.

AUTOMATIC LOGOFF

Businesses must terminate an electronic session after a pre-determined time of inactivity.



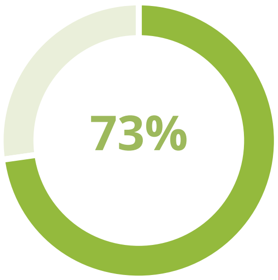
80% of small and midsize businesses are using some form of SaaS application[5]



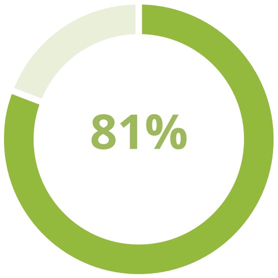
78% of small and midsize businesses are expected to fully adopt cloud solutions by 2020[6]

Like enterprise organizations before them, small businesses have their sights set on greater innovation and a faster, more agile approach to everyday business challenges.

Fortunately, small businesses are benefiting from more secure cloud environments, which could be the reason small business comfort with cloud solutions is keeping pace with adoption.



73% of small businesses are already using cloud solutions for business data



81% of small businesses are already using cloud solutions for personal data

Newer entrants into IT – those with less than 10 years' experience – were the most likely of those surveyed to use cloud solutions when working with both personal and business data. And while a majority of businesses trust cloud vendors to protect their data, they are still playing it safe – three-quarters research a vendor's ability to meet compliance requirements before making technology purchases. Similarly, more than half (57 percent) of businesses are on the hook to meet the compliance requirements of their customers and partners, adding yet another layer of complexity for IT decision makers.

AVOIDING MOBILE MISHAPS

TECHTIP

By Robert Siciliano

Robert is an expert in personal privacy, security and identity theft.

Small businesses can put in place simple solutions to protect the company information employees download to their personal devices. The following steps can help your employees put security first when working from their mobile devices:

PASSWORD PROTECTION

Ensure employees' devices are password-protected so that a thief or the person who finds it can't access the data on the device. Enable the "erase data" function when there are, for instance, 10 password entry attempts.

REMOTE WIPE

All devices used for business purposes should have a "wipe" function. With this feature, an Internet connected device can be located if it's stolen or misplaced. They can then wipe the data remotely.

UPDATES

Stay on top of all those update alerts. Reasons people get these: Functionality or security vulnerability was probably discovered. Waste no time downloading the updates or set them up automatically.

ANTIVIRUS

Beware of free download offers; they can be infected. Buy all apps from an approved app store, rather than from 3rd party sites. Anti-virus protection is a must to protect against this, especially for Androids.

NO JAILBREAKING

Installing software that breaks a device's walled garden opens a gate for malware to get in. Malware can be anywhere, including an app that they download.

Small businesses that want to gain control over sensitive or proprietary data residing on BYOD, as well as business owners and IT managers should consider "mobile device management" or "enterprise mobility management" technologies to help them control devices brought inside the corporate firewall.

KEEPING PACE WITH DIGITAL INNOVATION

Dealing with data has never been more challenging for small businesses.

Even as cloud adoption and greater data fluency are benefiting small businesses in the form of increased productivity, lower costs and faster transactions, many still struggle to support the rapid pace of innovation. Data loss – at the hands of well-meaning employees or malicious hackers – presents a growing risk to organizations that are increasingly reliant on data to survive and thrive. With the right strategies and safeguards in place, however, businesses are more apt than ever to leverage digital information as currency and be successful.

Sources:

1. IDG: 2015 Big Data and Analytics Survey; March 2015
2. International Data Corporation: The Growth Opportunity for SMB Cloud and Hybrid Business Continuity Sponsored by: Carbonite, by Raymond Boggs, Christopher Chute & Laura DuBois; April 2015
3. Carbonite/Spiceworks: Backup and Disaster Recovery: The IT Experience; September 2015
4. PricewaterhouseCoopers: The Global State of Information Security Survey 2015; October 2014
5. Aberdeen: Who are Heavy users of SaaS Applications?; January 2013
6. Intuit Developer: The Appification of Small Business; April 2015
7. CompTIA: Trends in Information Security Study; March 2015

NONSTOP PROTECTION FOR NONSTOP BUSINESS

Carbonite provides cloud and hybrid backup solutions for better protection and faster recovery of all your business data.

carbonite.com

CARBONITE™