Small Business Data Security

What Small Businesses Need to Know

Authored by

SMB Group
Actionable Market Insight

Sponsored by

DELL EMC

Contents

Introduction

The way we work is changing. Technology has become part of the business fabric, and our ability to effectively harness data is critical to business survival and growth. We expect to have the information we need available when and how we need it—to collaborate, transact and make decisions.

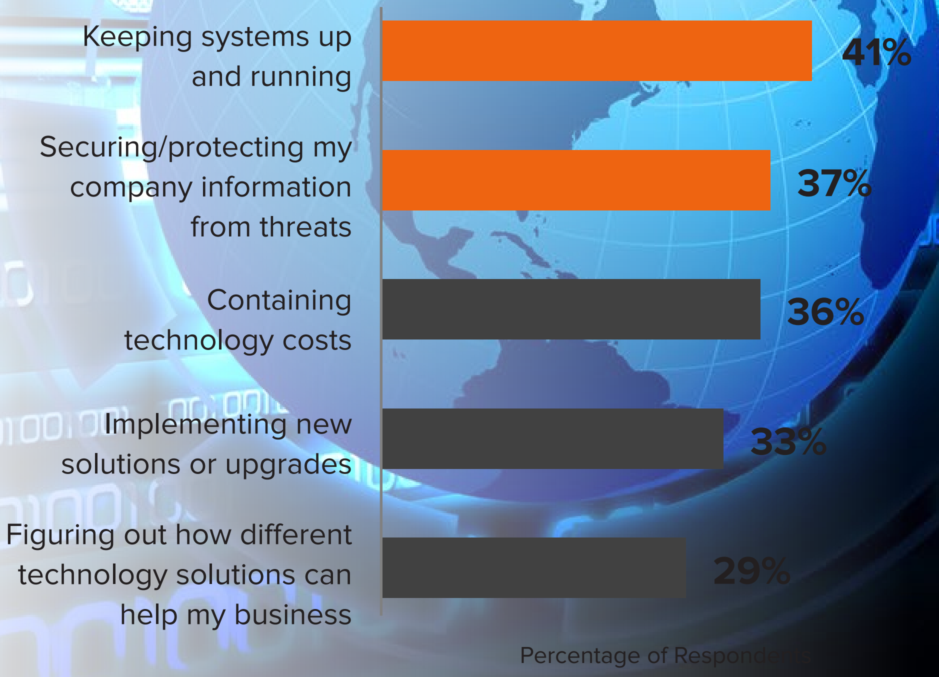
But as our reliance on technology grows, so do the requirements to access, secure and protect data. In fact, small businesses rank “keeping systems up and running” and “securing/protecting my company information from threats” as their most pressing technology challenges.

System downtime obstructs access to the data and files you need to get work done—and can result in serious consequences. Productivity suffers, revenue drops and businesses struggle to recover. Security breaches—from ransomware to hijackings, and phishing to worms—can result in severe financial and brand damage.

But for most small businesses, technology expertise is a scarce resource. As a result, many of these companies put security and data protection on the back burner—a risky bet as more data is distributed across more places and devices.

In this ebook, we discuss how your small business can address these issues in a practical, effective way. We start by discussing the importance of safeguarding your business in the digital age, as well as the difference between data security and data protection solutions. Then we take a deeper dive into cyber security and identity access and management, and we offer recommendations about what you should look for in security solutions. In our companion ebook, **Small Business Data Protection**, we focus on what you need to know about data protection for your small business.

TOP TECHNOLOGY CHALLENGES FOR SMALL BUSINESSES[1]



Why You Can't Afford to Be Complacent About Data Protection and Security

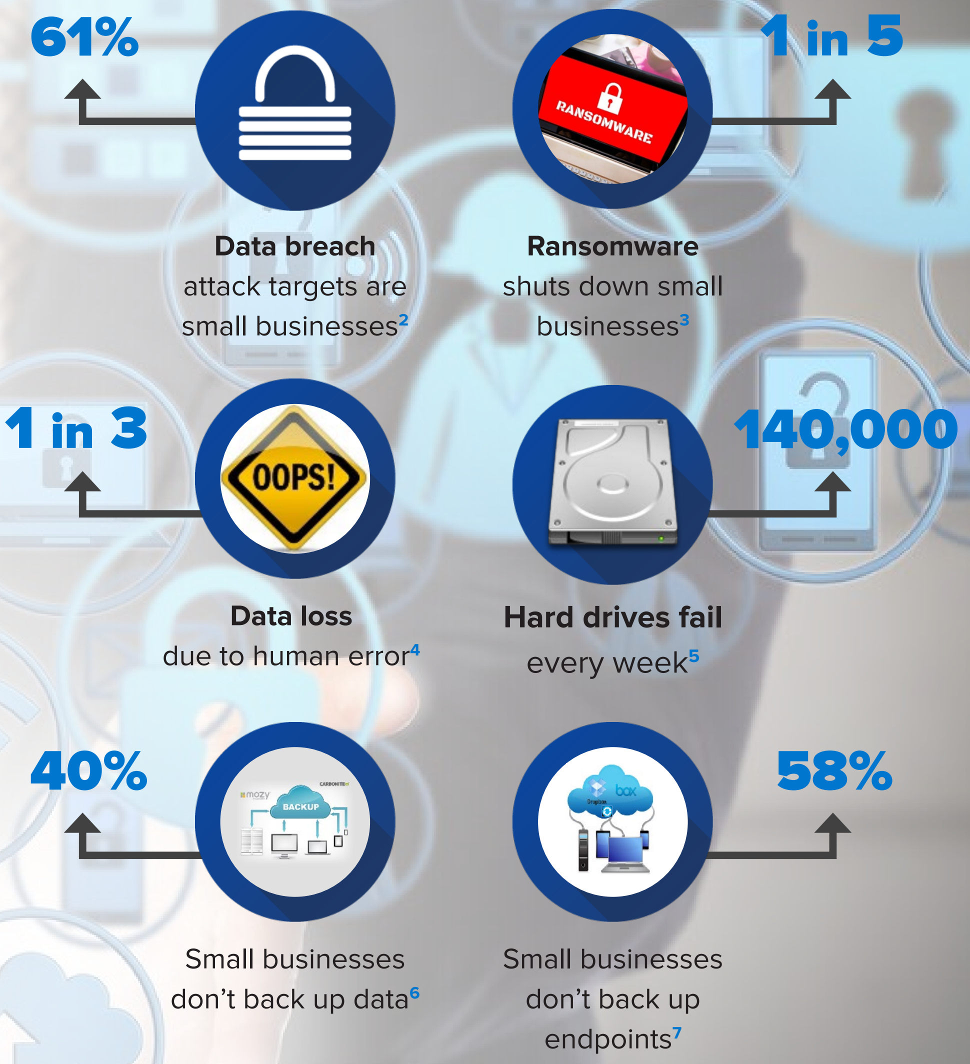
Some small business decision makers think that because their companies are small, they don't need to worry about cyber attacks and data breaches. For example, 40% of small businesses don't back up any of their data, and 58% neglect to back up client devices (aka "endpoints"). Especially in today's always-on, mobile world, this is an increasingly risky strategy.

Small businesses are more vulnerable than ever to security threats and data loss. Consider the following statistics:

- **61% of data breaches hit smaller businesses in 2016, up from 53% in 2015[1].**
- **1 in 5 small businesses were the target of a ransomware attack and experienced a shutdown due to the attack[2].**
- **1 in 3 small businesses experienced a data loss due to human error[3].**
- **140,000 hard drives fail every week in the United States[4].**
- **1 in 4 mobile apps include at least one high-risk security flaw[9].**

Data-related outages and downtime can carry heavy costs—leading to reputation damage, loss of customer trust and financial damage resulting from the inability to get the information you need to get work done, and from potential fines and penalties. In the worst-case scenario, a small business may not even recover if the infected data or system cannot be restored expeditiously. But you can avoid these issues by taking a few proactive measures to guard against data loss and security breaches.

93% *According to the Online Trust Alliance's analysis of security breaches reported through 2017, 93% of data loss incidents were avoidable.*



61%

Data breach attack targets are small businesses[2]

1 in 5

Ransomware shuts down small businesses[3]

1 in 3

Data loss due to human error[4]

140,000

Hard drives fail every week[5]

40%

Small businesses don't back up data[6]

58%

Small businesses don't back up endpoints[7]

Data Security vs. Data Protection: What’s the Difference?

The first step to protecting your business in the digital age is to understand the distinctions between data security and data protection. Both are critical to protecting business-critical data—but they have very different roles and help defend against different types of vulnerabilities.

Data security solutions

help prevent unauthorized access, use, disruption, modification or destruction of data stored on servers (either on premises or in the cloud) or client endpoint devices, including both traditional desktops and mobile devices. They are designed to keep company data safe from any kind of nefarious exploitation, including both internal and external threats. Data security solutions prevent malware attacks and also prevent hackers from gaining access to systems.

Data security solutions include the following:

Cyber security solutions

Identity and access management (IAM) solutions

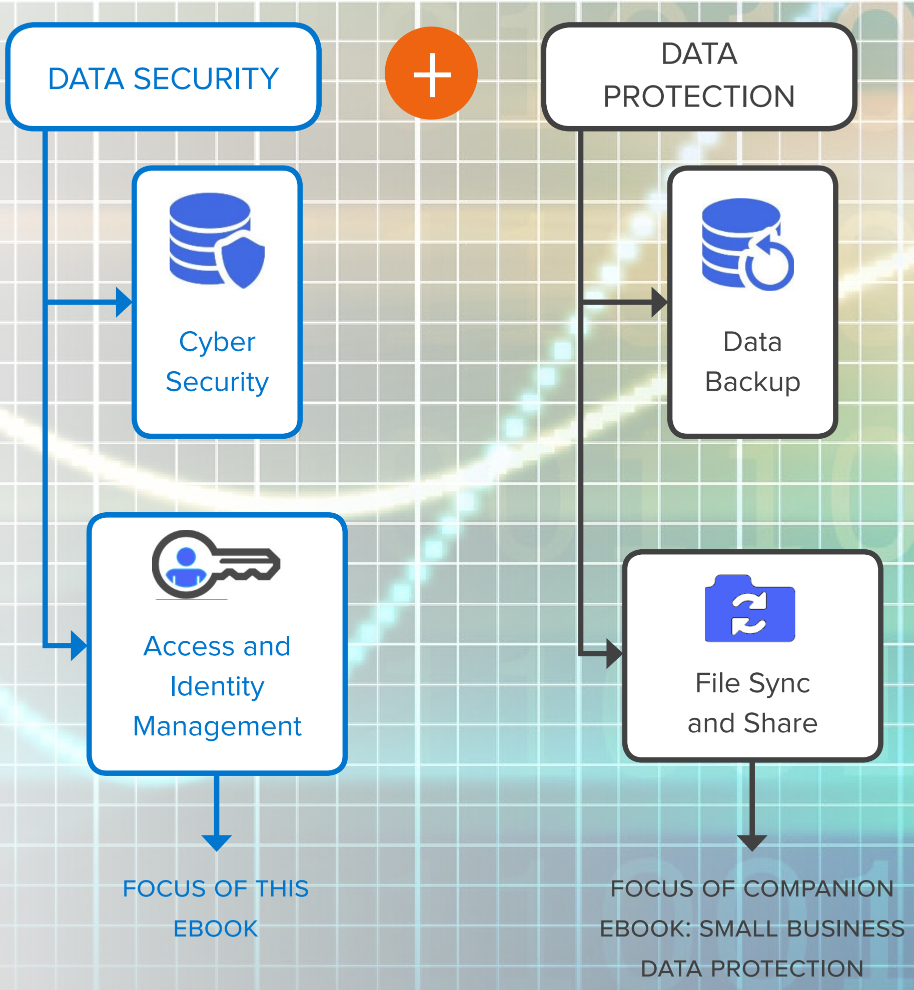
Data protection solutions

provide a mix of services to protect companies from data loss and downtime. These solutions restore data that is compromised at the system level or the file level, whether as a result of data security attacks, device loss, employee negligence or natural disasters, such as hurricanes and floods.

Data protection offerings include the following:

Data backup solutions (on premises, cloud and mobile)

File sync and share solutions



Cyber Security and Identity and Access Management: Why You Need Both

Data security solutions focus on preventing malicious attacks from happening in the first place, safeguarding data from cyber threats and access by unauthorized users. Business benefits include prevention of the following incidents:

- Data loss–related downtime and related financial costs
- Temporary or permanent loss of sensitive information
- Unauthorized access to company resources and data
- Disruption to regular operations
- Financial losses incurred to restore systems and files

Two of the most important security solutions that small businesses need to put in place are cyber security solutions and identity and access management.

Cyber security solutions protect your organization from malware and malicious attacks. Identity and access management—which enables the right people to get access to the data and resources they need, when they need it—prevents the wrong people from exploiting your applications and data

Data Security

Cyber Security

- Protects data from being exposed to malware (e.g., ransomware, viruses, Trojans)
- Keeps data secure from any kind of malicious exploitation
- Ensures data security via anti-malware solutions

+

Identity and Access Management

ACCESS CONTROL
AUTHORIZATION
IDENTITY
AUTHENTICATION

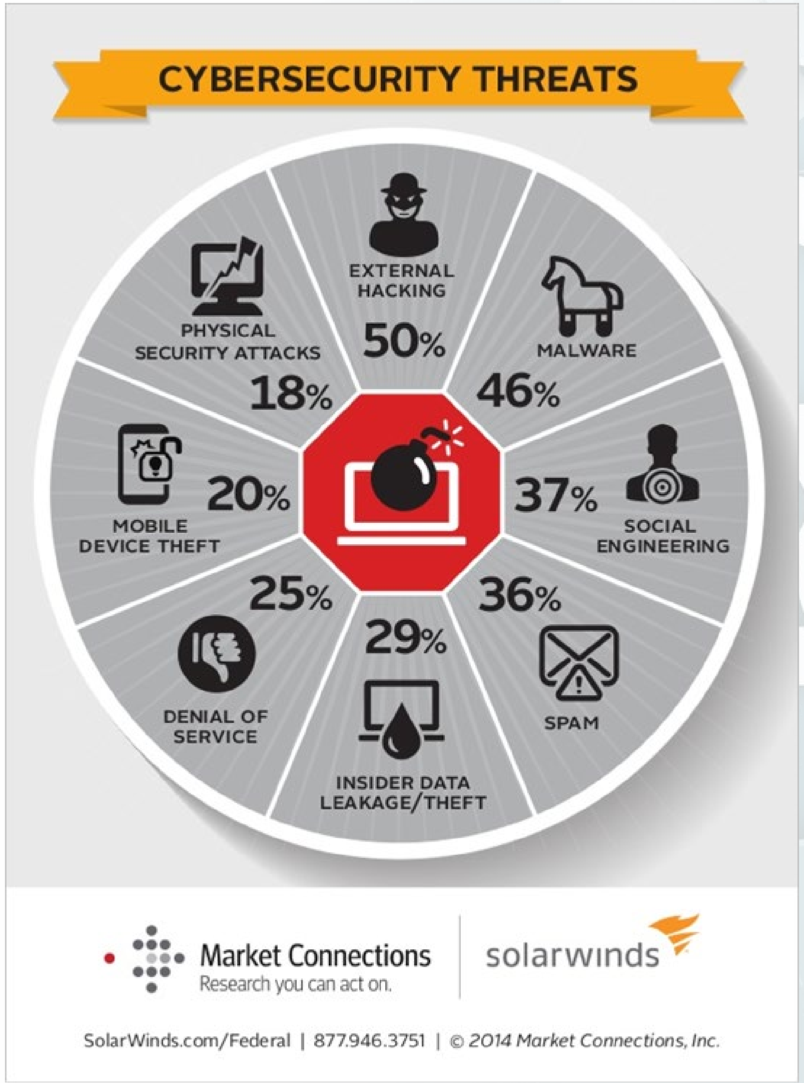
- Allows easy and secure access to company resources and data
- Protects data from unauthorized access
- Enhances user experience
- Improves user productivity
- Increases business agility

Cyber Security: What to Look For

Provides safeguards against malicious attacks

- Anti-virus software to catch viruses and Trojan horse programs
- Anti-spam software to control spam, which could contain malicious code or links to hacker websites
- Anti-phishing software to detect financial hacking techniques
- Anti-ransomware software to prevent ransomware attacks
- A network, server-based or endpoint firewall program that monitors internet connections
- Encryption technology to protect email and other network traffic, particularly for wireless networks

Companies that offer small business–focused security solutions include McAfee, Trend Micro and Symantec.



SolarWinds.com/Federal | 877.946.3751 | © 2014 Market Connections, Inc.

Small Business Cyber Security

Threat Checklist

- Ransomware attacks
- Phishing attacks
- Malware infiltration through HTTPS
- Viruses and Trojans
- Malicious attacks from insiders
- Use of unauthorized cloud apps and services
- Use of personal social apps
- Surfing websites that violate policy

Supported Infrastructure

- Endpoints: desktops, laptops, tablets, smartphones
- Servers

Security Services

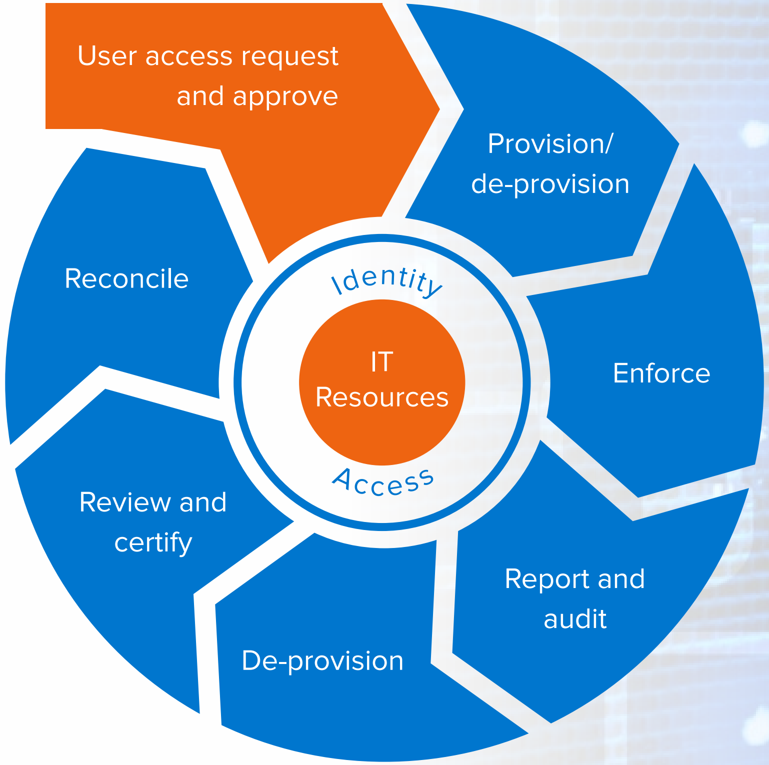
- Malware detection and remediation
- Malicious website blocking
- Ransomware blocking
- Exploit protection
- Email protection and scanning

Identity and Access Management: What to Look for When Comparing Data Protection Solutions

Manage user identity and access

- Identity and access management functionality to authorize users to access the appropriate computing resources, data and applications
- Prevents hackers from gaining access to sensitive applications and data should they compromise an employee's credentials
- Single sign-on (SSO) capabilities to improve employee productivity, alleviate employee and customer frustration, and reduce help desk costs

Companies that offer small business–focused IAM solutions include LogMeIn, OneLogin and Okta.



Small Business – Identity and Access Management

Threat Checklist

- Access-related compliance needs
- Identity analytics to identify high-risk user access and behavior profiles
- Rule and exception-based access analysis and reporting
- Enforcing access to company resources

Supported Infrastructure and Applications

- Endpoints: desktops, laptops, tablets, smartphones
- Servers
- Applications (on premises and cloud)

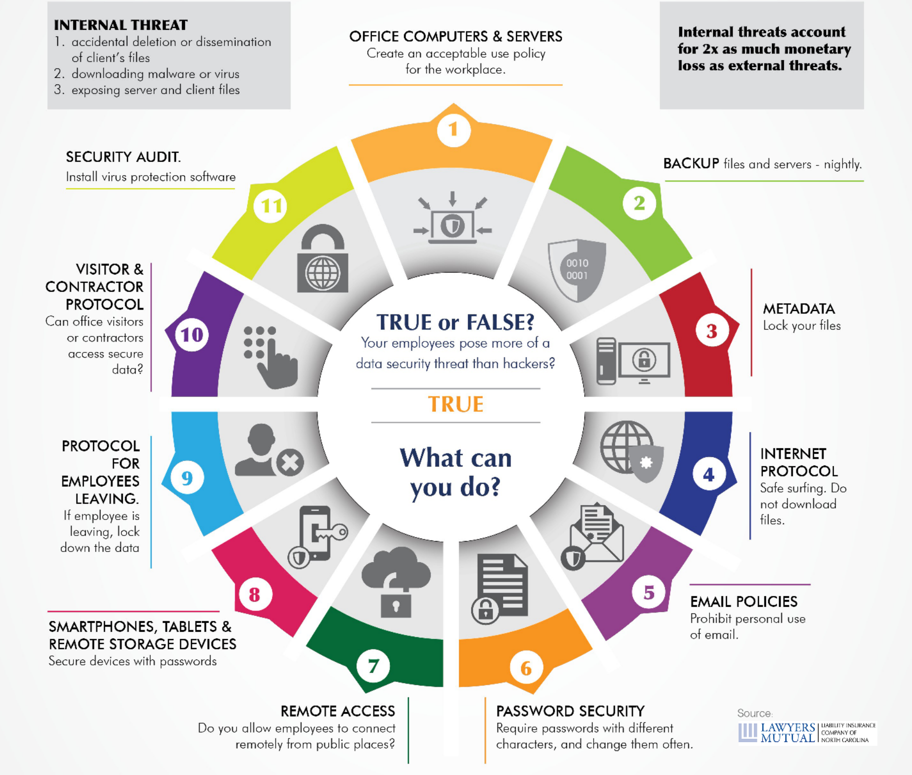
Security Services

- All user identity management (e.g., employees, contractors, system accounts)
- Centralized directory services used for authentication and authorization
- Centrally manage identities and access privileges across applications in the cloud and on premises

Recommendations for Small Businesses

If you haven't already done so, now is the time to work with your service provider to conduct a thorough self-assessment of your existing data protection policies and processes to identify gaps and determine how to fill them. As you move ahead to safeguard your business better, consider the following steps:

1. **Take a proactive approach.** Don't wait for employees to start using consumer tools. If companies don't provide these tools, employees will adopt them through their personal accounts, creating a more significant management and control issue.
2. **Create a data protection policy with your service provider.** It should contain best practices that employees are expected to follow.
3. **Train employees in security policies.** Establish basic security practices and strategies for employees, such as requiring strong passwords, and develop appropriate internet use guidelines that detail penalties for violating company cyber security policies. Establish rules on customer privacy and the protection of customer information and company data.
4. **Protect computers, networks and data from cyber attacks.** Keep systems updated with the latest security software, web browser and operating systems. This is the best defense against cyber threats and ransomware.
5. **Secure network and internet connections.** Make sure the network and Wi-Fi router firewall is enabled. If employees work from home, ensure that their home system(s) are protected by a firewall.
6. **Create a mobile device action plan.** Mobile devices (specifically "bring your own device" [BYOD]) create significant security and management challenges. Require users to password-protect their devices, encrypt data and install security apps to prevent cyber criminals from stealing information while employees are on public networks. Establish reporting procedures for lost or stolen equipment.
7. **Implement identity and access management.** IAM needs to be a key part of a small business security solution. Employees must confirm identities before granting access, and authorized users must be managed and tracked.
8. **Password management.** Require employees to use unique passwords and to change their passwords every three months. Employees need access to the specific data systems that they need to do their jobs.



INTERNAL THREAT
1. accidental deletion or dissemination of client's files
2. downloading malware or virus
3. exposing server and client files

Internal threats account for 2x as much monetary loss as external threats.

TRUE or FALSE? Your employees pose more of a data security threat than hackers?

TRUE

What can you do?

1 OFFICE COMPUTERS & SERVERS Create an acceptable use policy for the workplace.

2 BACKUP files and servers - nightly.

3 METADATA Lock your files

4 INTERNET PROTOCOL Safe surfing. Do not download files.

5 EMAIL POLICIES Prohibit personal use of email.

6 PASSWORD SECURITY Require passwords with different characters, and change them often.

7 REMOTE ACCESS Do you allow employees to connect remotely from public places?

8 SMARTPHONES, TABLETS & REMOTE STORAGE DEVICES Secure devices with passwords

9 PROTOCOL FOR EMPLOYEES LEAVING. If employee is leaving, lock down the data

10 VISITOR & CONTRACTOR PROTOCOL Can office visitors or contractors access secure data?

11 SECURITY AUDIT. Install virus protection software

Source: LAWYERS MUTUAL LIABILITY INSURANCE COMPANY OF NORTH CAROLINA

Read our companion ebook, **Small Business Data Security**, for more information on what you need to know about security.

About

DELL EMC

Dell Small Business Central

Dell has over 30 years of experience partnering with small businesses to help them thrive. We're using that experience to help you guide your small business' success today and far into the future.

SMB Group
Actionable Market Insight

SMB Group is a research, analysis and consulting firm focused on technology adoption and trends in the small and medium business (SMB) market. Founded in 2009, SMB Group helps clients to understand and segment the SMB market, identify and act on trends and opportunities, develop more compelling messaging, and more effectively serve SMB customers.

Sources

1. SMB Group 2017 Routes to Market Study
2. Online Trust Alliance Cyber 2017 Data Breach Investigations Report
3. CNET, "Ransomware shuts down 1 in 5 small businesses after it hits" (assessment of cyber security company Malwarebytes)
4. Online Trust Alliance 2017 Cyber Incident & Breach Trends Report
5. Seagate, "Tips for What to Do If Your Hard Drive Fails"
6. IDGresearch.com, 2015
7. IDC Study, 2015
8. Spiceworks 2018 State of IT Report
9. NowSecure 2016 Mobile Security Report