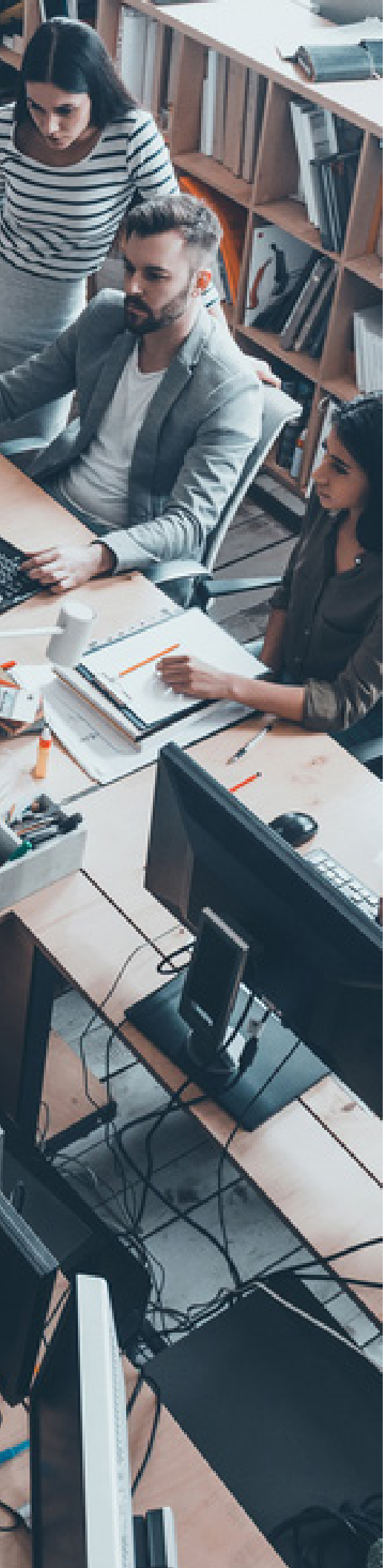
QUICKBRIDGE

Cybersecurity and Small Businesses:

Are You Protecting Your Customers?



QUICKBRIDGE

Table of Contents

Introduction

Small businesses aren't immune to cybercrime. The cyberthreat landscape has evolved; attacks don't stem from just rogue hackers hoping to get access to corporate secrets from large businesses. Instead, small businesses are just as likely to be the victim of cyberattacks as large corporations, with organized crime groups targeting points of weakness in the hopes of making quick money.

Today's attacks are simple enough to be deployed at a large scale, and hackers are using them to target small businesses that typically have a moderate amount of data with minimal security.

A Better Business Bureau study found that even the smallest of businesses are at risk. Of respondents representing businesses with 0 to 5 employees, 16 percent have faced a cyberattack, and 9 percent don't know if they've been targeted. Similarly, approximately 12 percent of survey respondents from organizations with 6 to 10 employees have been attacked, and 14 percent are unaware if they've ever fallen victim to a cybercrime.

Cyberattacks don't represent a small threat either. A Kaspersky study indicated that among small businesses, the average direct cost of recovering from a data breach is $38,000. And the direct costs commonly associated with data breaches are far less significant than the "hidden" costs.

Companies must also consider the operational implications of a cybersecurity incident. Businesses rely on data. In fact, the Better Business Bureau survey found that just 35 percent of businesses could maintain profitability for more than three months if

they were to permanently lose access to critical data. It doesn't take much to run into a data loss incident either. Ransomware is more likely to create sizable data loss than a hard disk failure and is emerging as one of the most common types of attacks.

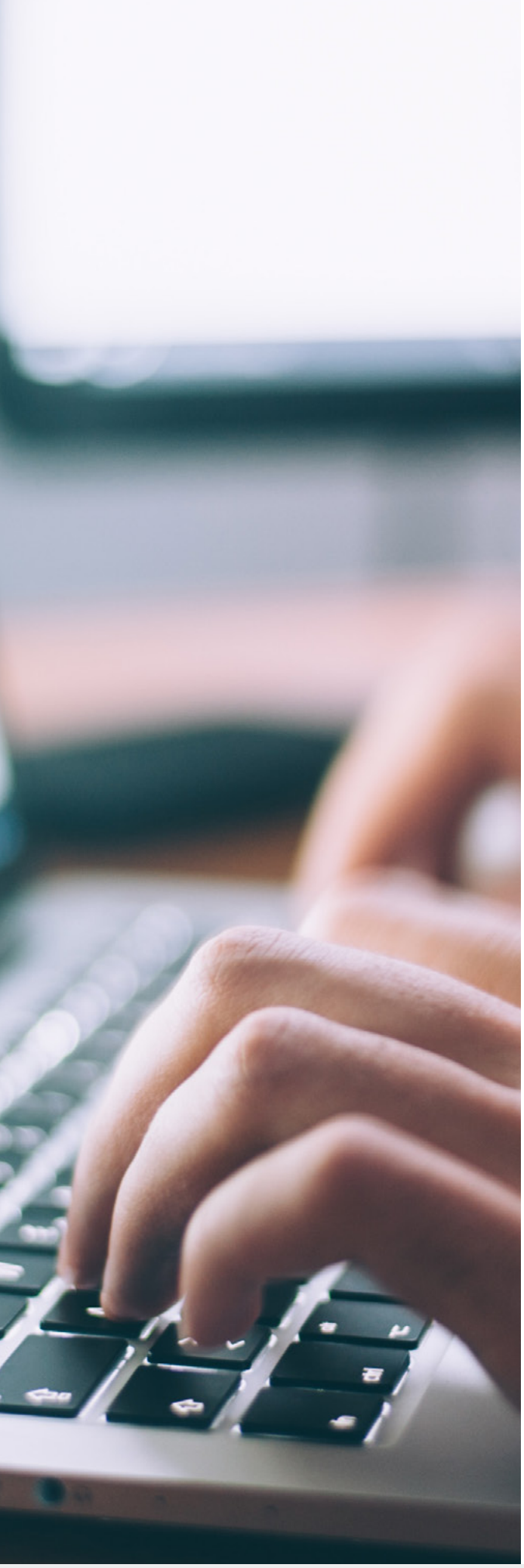
Beyond data loss, organizations must also contend with reputation-related damages, legal costs, customer defection, and similar issues when impacted by a data breach.

The threat for small businesses is real and growing. The Identity Theft Resource Center found that the number of tracked U.S. data breaches reached a new high in 2017, as the figure climbed 44.7 percent year over year.

Taking cybersecurity seriously isn't just important in preventing damages. It can also create a positive starting point with customers by showing you care about the security of their private information.

With risk rising at an astronomical pace, small businesses must prepare themselves to not only keep attackers at bay, but also respond effectively in the event of a disaster. This process begins by understanding the entire threat climate.

The number of tracked U.S. data breaches reached a new high in 2017, as the figure climbed **44.7 percent** year over year.



Which Industries Are Most At-Risk for Cyberattacks?

Any type of organization may be threatened. However, a few industries stand out as being highly targeted based on data from the Identity Theft Resource Center. These industries include:

General businesses:

The average business is the biggest target for attacks. The Identity Theft Resource Center found there were 1,579 tracked data breaches in the U.S. in 2017, with 870 of those breaches impacting enterprises. If that number seems low, remember that it covers only reported and tracked data breaches, not the many attacks that go unnoticed or are kept quiet.

Health care:

The study indicated that approximately 24 percent of all data breaches in 2017 happened at health care industry businesses. These statistics aren't limited to just hospitals and care networks—83 percent of physicians polled by the American Medical Association said they've faced a cyberattack.

Banking and finance:

Banks and financial institutions are heavily targeted by cybercriminals seeking to hack into the accounts of customers. Organizations in this sector were struck by 8.5 percent of all breaches.

Retail:

While not mentioned in the study, the rise of e-commerce is leading to a rapid increase in the number of attacks targeting merchants online and through attacks at the point of sale.

Social Security numbers were attacked **eight times** more often in 2017 than they were in 2016.

What Data Are Hackers Targeting?

Beyond knowing what industries are most at risk, it's important to identify what data is targeted most often. For example, the information stored on mobile devices. Many smartphones and tablets lack the same security protections offered by traditional computers.

What's more, many users rely on passwords as the sole form of protection for their devices and applications. But passwords are faulty and often poorly created. The Better Business Bureau study we mentioned found that 33 percent of data breaches impacting respondents lead to the theft of passwords or similar data.

For small business owners, losing control of a customer's account information can lead to an immediate loss of trust. You're not only failing customers, you're also leaving their private information exposed, potentially leading to further problems. This can damage your brand, force you to spend on credit monitoring, or lead to legal problems. The costs and long-term damages can be substantial, and even a small incident can escalate quickly because of the types of attacks cybercriminals employ.

In simplest terms, hackers are attacking data that allows them to take control of your identity. If they're able to retrieve password data, they can use it to force their way into email accounts. Once there, they can reset passwords to accounts that use email for a login. If they steal payment card data, they can claim a person's identity and set up accounts or make purchases. For small businesses, these attacks can put customers at considerable risk. If an employee email account is compromised, for example, then hackers can gain access to your backend systems where customer information is stored. From there, they can use the data to target your clients.

The result of these tactics is an increase in other types of identity fraud. The Identity Theft Resource Center found that credit card attacks increased 88 percent from 2016 to 2017. And according to FICO, attacks on debit cards rose 10 percent year over year in 2017. Payment credentials aren't alone in being attacked. Social Security numbers, for example, were attacked eight times more often in 2017 than they were in 2016. As a business owner, you are responsible for the safekeeping of your customers' credit card and debit card information, so the fact that these types of attacks are increasing is even more reason to stay vigilant.

What Methods Do Hackers Use?

There are several types of cyberattacks. However, a few stand out as particular threats for small businesses.

Malware:

According to the Kaspersky study mentioned previously, approximately 24 percent of businesses have been hit by malware. Malware is malicious software that accesses a system and resides in the background sending data to attackers. For example, keyloggers – applications that record all keystrokes a user makes – are a common malware system. They are used to steal passwords that users type repeatedly.

Phishing attacks:

Ten percent of those polled in the Kaspersky study said they were hit by phishing scams. Phishing tactics use fake emails to get users to click a link or open an attachment, often to get malware or ransomware onto a system. For example, an email may look like it has come from an equipment supplier and ask one of your workers to reset a password. When the worker does so, it gives the hacker access to your system.

Ransomware:

This is a relatively new type of malicious software designed to block access to a computer system. When ransomware gets onto a machine, it turns the data in the system into a coded format. From there, the attacker demands a ransom from the victim in order to get the data decoded.

Software vulnerabilities:

Sometimes software will have a glitch that moves data around in an unsafe way. These vulnerabilities let hackers get into systems they otherwise wouldn't be able to access. It's important to keep up with patches and software updates to avoid these problems.

These attack types are particularly problematic for small businesses because they don't take much skill to use. Because they're easy for criminals to employ, hackers have no problem using them at large scale to attack many organizations, regardless of size. Being a small business won't keep you off of attackers' radars. It's time to adapt and employ modern security strategies.

24 percent of businesses have been hit by malware.

What's the Solution?

There isn't a single strategy to deal with cybersecurity. However, a few best practices and emerging tactics help businesses protect themselves and their customers.

Collaborate with peers:

Don't leave yourself vulnerable by ignoring what's happening around you. It's vital to react to emerging attacks. For example, the National Retail Federation is trying to bring merchants together to share new threats and tips on securing data.

Look out for legislation:

Legal advances frequently emerge to help organizations safeguard data. These can range from regulatory standards that come with penalties for poor compliance to reporting requirements that ensure data breaches are recognized and responded to effectively.

Create better day-to-day practices:

Are passwords failing you? Establish multifactor authentication. Is malware an issue? Purchase an advanced antivirus program. Are mobile devices compromising data? Take advantage of mobile device management. Strategic tech investments can go a long way in protecting data.

Train your workers:

Many attacks directly target employees, making cybersecurity employee training and education critical to your data protection efforts. Take the time to train your employees so they know how to protect themselves and spot potential attacks.

How Can QuickBridge Help?

In practice, small businesses face a simple problem. They are experiencing increasingly frequent cyberattacks from a wider range of sources. However, they don't have the resources or security protocols in place to guard against these attacks. That's where QuickBridge can help.

QuickBridge can provide your business with the supplementary capital needed to invest in cybersecurity measures. The funds can be used to hire additional IT staff, train employees, update your software, or purchase cybersecurity insurance to safeguard against the after-effects of a breach.

If getting funding just for a security upgrade seems drastic, you may want to consider the long-term damage of a security incident. Approximately 60 percent of small businesses shut down within six months in the aftermath of a data breach.

Cyberattacks tarnish both your customer's trust and your business's reputation. Allocating resources toward data protection can give you a competitive advantage by demonstrating how strongly you value your customers' data and limit your business's liability.

Contact us today to learn how QuickBridge can help you fund your next cybersecurity project.

QUICKBRIDGE

Sources:

1. www.bbb.org/globalassets/shared/media/state-of-cybersecurity/updates/cybersecurity_final-lowres.pdf
2. https://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf
3. www.idtheftcenter.org/Press-Releases/data-breaches-up-nearly-45-percent-according-to-annual-review-by-identity-theft-resource-center-and-cyberscout
4. nrf.com/blog/nrf-exploring-information-sharing-prevent-data-theft
5. wire.ama-assn.org/practice-management/8-10-doctors-have-experienced-cyberattack-practice
6. www.prnewswire.com/news-releases/fico-data-10-percent-more-debit-cards-were-compromised-in-us-last-year-300608839.html
7. www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html