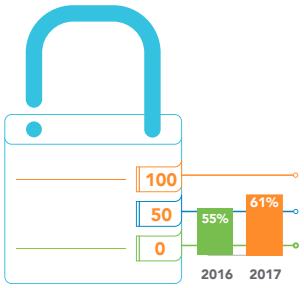
Small and Mid-Sized Business Security: What You Need to Know

A more human resource.®

Did you know that cybercriminals specifically target small and mid-sized businesses? Fraudsters bet that most of these businesses may not have the security safeguards that larger companies do—and unfortunately that's frequently the case.

Over 61% of small to medium sized businesses have been breached in 2017 vs. 55% in 2016[1]



- **71%** of cyberattacks occur at businesses with fewer than 100 employees[2]
- Average price for small businesses to clean up after their businesses have been hacked is **$690,000**[2]
- **60%** of small companies are unable to sustain their businesses over six months after a cyberattack[2]

Business owners have a lot to manage, but making security a priority is critical. When it comes to cyberattacks, it's not a matter of if, but when. If you use the internet, you're at risk.

Know the Risks

Threats are ever-changing, but these are some of the most common ones impacting small and mid-sized businesses:

- **Phishing:** Phishing emails try to fool you into thinking the sender is from a legitimate organization in an effort to get you to click on a malicious link or attachment, or provide personal or financial information.
- **Malware:** Malicious software, including viruses and spyware, can take control over your computer and record every keystroke to collect data to use for fraud.
- **Ransomware:** Hackers use this malicious software to take control of your files and lock you out of your system. Then they demand money from you in exchange for giving you your access back.

If your employees or customers notice anything suspicious, tell them to report it to you immediately.

Protect Your Business

Prevention is key, but there is no single solution for cybersecurity. The use of anti-malware software, firewalls and automatic updates is crucial, but don't rely on those alone.

Protect Your Systems and Restrict Access

Get educated from your hardware and software providers and turn on available defenses in your technology to protect your systems, including mobile devices, networks, stored data, and point of sale systems. Patch applications by installing security updates as soon as they're available. Limit access to administrator accounts and sensitive information, and prohibit sharing of credentials among employees.

Educate Your Employees and Make Someone Accountable

Security is everyone's responsibility. Set expectations about what is appropriate—including browsing safe sites and applications allowed on computers. Encourage them to use strong passwords that differ from other accounts, and teach them how to spot and report phishing emails—one of the top ways fraudsters gain access to data. Assign a trusted employee in a management role to be responsible for security procedures that you establish.

Be Ready to Respond

Can you afford to be offline for a day or more until you're operational—or even longer if it was a serious security incident that caused lasting damage to your business and its customers? Having a plan in place is critical to help keep your business secure and moving ahead.

Think Resilience

If you manage your own technology, ensure that you backup all of your important systems and data to another offsite and safe location, and on occasion test to make sure you can recover from those backups. If you use a service provider or a cloud service, make sure there are service level agreements in place that dictate backup strategies and recovery times.

Use the Pros

Use professionals when setting up a new office, when you suspect a problem—like being hacked, or even on a periodic basis. Using a professional will help make sure that it is done right and the upfront costs can significantly offset the cost to your business if you are hacked, lose customer data, or your systems become unavailable.

Report Immediately

If you think an attack has happened, alert your staff and report it to the authorities. The quicker you address it, the quicker you can minimize or prevent negative impacts to your business and customers.

If your budget is tight, use free resources available from official organizations to learn about how to secure your business and train employees to help do their part.

- **Small Business Administration:** **www.sba.gov**
- **Federal Trade Commission:** **www.ftc.gov**
- **Department of Homeland Security:** **www.dhs.gov**
- **Better Business Bureau:** **www.bbb.org**
- **National Cyber Security Alliance:** **www.staysafeonline.org**

Taking security precautions now will pay off for you in the future, and help your business succeed.

Protecting our clients and their data from malicious activity is a top priority for ADP. Visit our website at www.adp.com/trust to learn more about how ADP protects data, and how clients can help protect themselves.

1 Ponemon Institute Study Finds SMBs are a Huge Target for Hackers, PR Newswire, September 2017
2 What Happens When Your Small Business is Hacked, Entrepreneur, June 2017

The recommendations contained in this document are not intended to be an exhaustive list of all possible steps that can be taken to secure your business.