RESOURCE GUIDE

Cybersecurity for Small Businesses

McAfee's Resource Guide

Table of Contents

Introduction	3
Identifying the risks	4
Country stats	5
Awareness and readiness	6
A country snapshot	7
Proposing solutions	8
McAfee Business Protection	12
About this study	13

Is Your Business Prepared? A Cybersecurity Guide for Small Businesses

News reports often paint cybercrime as a concern for big businesses, who are targeted with high-profile ransomware or data breach attacks. But the truth is that this threat is just as present in the small business world.

Driven by an increased availability of "off-the-shelf" hacking tools that have lowered the barrier to entry for malicious actors, cybercriminals are increasingly waging attacks against businesses with yearly revenues of $500,000 or less.

For large companies, cybercrime is often factored in as the cost of doing business. But for small business owners, these attacks can be devastating because they lack robust cybersecurity and are left vulnerable. On average, a business email attack (typically conducted through targeted phishing or other account hacking) siphons $125,611 in funds. Ransomware attackers hold company data hostage for an average of $14,403, and data breaches hit businesses for an average loss of $164,336.

Based on a global survey of 700 business owners and IT professionals, McAfee has prepared this guide to help inform small business professionals (organizations with less than 100 employees) of this growing threat and to arm them with the tools to keep their employees, customers, and business safe.

Threats from cyber criminals are rising, and SMBs are concerned

The threat of being hacked, experiencing business disruption, or losing trust from customers due to cybercrime weighs heavily on the minds of small business owners.

Cybersecurity was mentioned by 73% of the organizations surveyed as one of their biggest risks or vulnerabilities—and 24% of the business owners and IT professionals surveyed say they worry daily about cyberattacks.

And these fears are justified. The data shows that cyberattacks are on the rise, as 44% of the surveyed small businesses have experienced a cyberattack, and 17% have experienced more than one. For 67% of the organizations that experienced a cyberattack, the attack occurred in the last two years, indicating that the threat of cybercrime has become more prevalent.

For a small business, even a single cyber incident can be devastating to the bottom line. For 61% of the small businesses that experienced a cyberattack, the company lost more than $10,000 dealing with the attack. Many of the business owners and IT professionals surveyed (60%) indicate that the cyberattack on their business took a physical or mental toll on them and/or their staff or colleagues. In 58% of the cases, the company lost more than a week of valuable business time dealing with IT issues due to the attack.

Data makes SMBs a target

- As small businesses become more connected and digitized, they accumulate data troves that are attractive to hackers.
- Almost half of the business owners/IT professionals surveyed (46%) mention that losing data is their biggest worry.
- For those that have suffered a cyberattack, in most cases customer data (38%), passwords (34%), or other files (34%) were lost.

SMB owners feel knowledgeable about the threat of cybercrime …

Most business owners understand the risk cybercrime poses to their operations. According to our survey, 69% of business owners and IT professionals surveyed feel that they know enough to make cybersecurity decisions for their business.

Generally, they understand that cyber threats are something they need to plan for and invest in mitigating, as 84% of the small businesses surveyed currently have some form of online security protection in place, and 60% say they have an action plan in place if a cyberattack does happen.

… yet, many businesses are under-resourced to deal with the increasing complexity and frequency of these threats

While business owners know cybersecurity is a problem, they often simply don't have the staff or resources to stay abreast of this growing threat.

Despite wide awareness, only about half (48%) of business owners/IT professionals were fully confident in their business's ability to prevent cyberattacks. Most small businesses (76%) manage cybersecurity without the help of others outside the company.

- 17% have an employee whose primary job is different, but they also manage devices and IT matters.
- Only 8% of the small businesses surveyed hire an outside consultant to guide their purchases and installation of cybersecurity products.

Too many owners handle cybersecurity themselves, in addition to other duties. And it's not just cybersecurity: 45% of the business owners surveyed said they focus on overall IT issues more than 7 hours a week.

How hackers are getting in

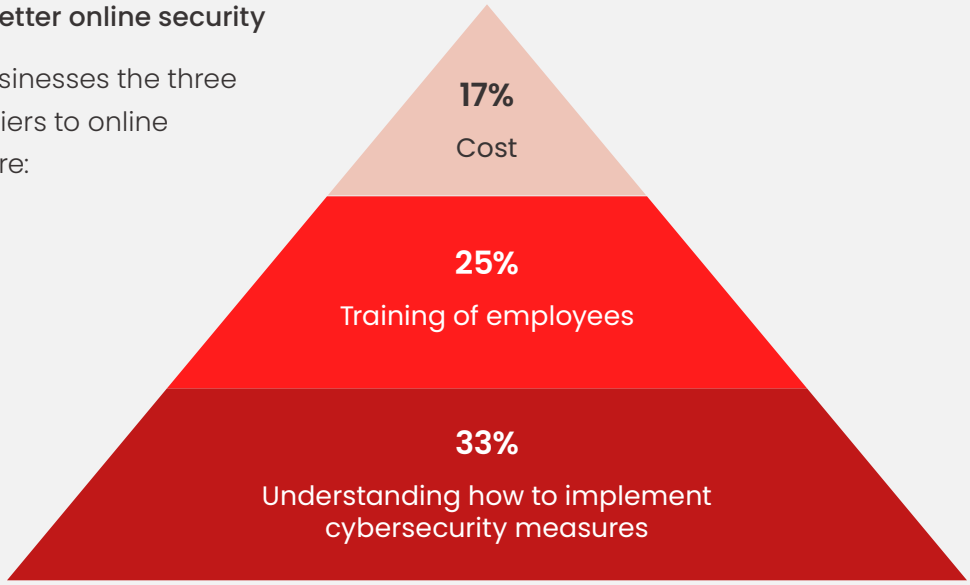
While there are many ways a cybercriminal can disrupt a small business, there are a few methods they tend to favor. Being vigilant and educating employees about these types of attacks—and how to prevent them—can save business owners time and money.

Our survey indicated that most attacks (43%) were caused by employees mistakenly downloading malware by clicking on a phishing link and/or opening a malicious attachment. In 36% of these cases, login credentials were mistakenly inputted to a phishing site, and 35% of the attacks were caused by a weak password that was hacked on a user account.

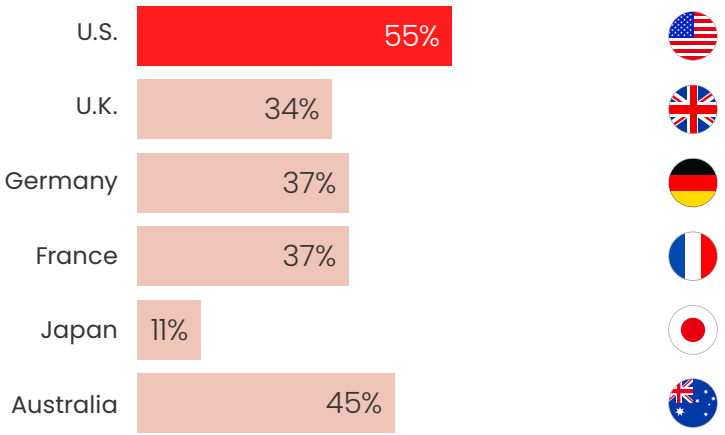
And it's not just about preventing cyberattacks on your company—sometimes a business's name/likeness have been used by criminals as a tool. 17% of survey respondents indicated that their business information had been used in phishing attacks targeting others.

Barriers to better online security

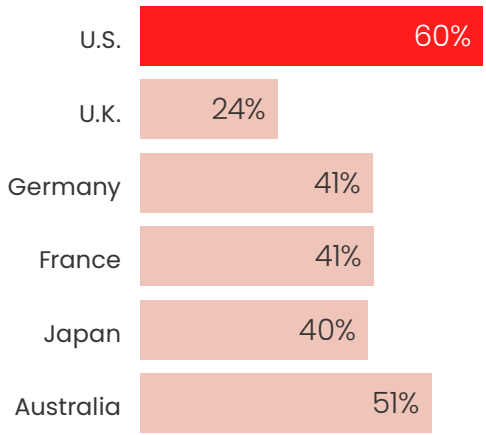
For small businesses the three biggest barriers to online protection are:



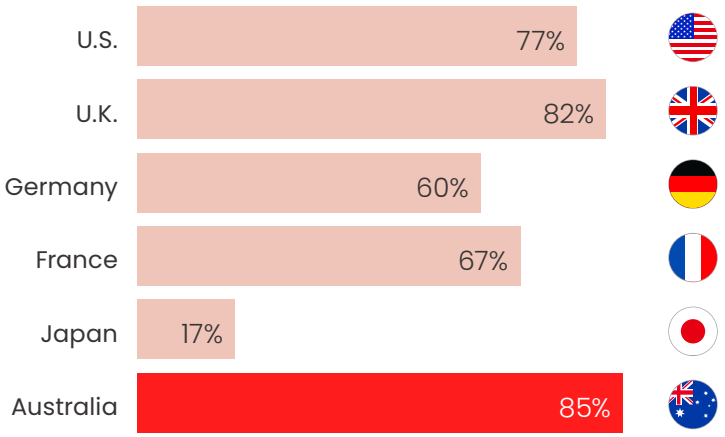
U.S. SMBs have the highest adoption rate of AI for cybersecurity...



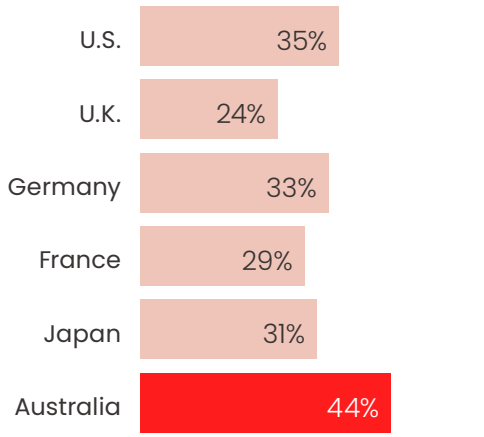
...but are also most concerned about cybersecurity with the proliferation of AI.



Australia SMBs are the most confident their employees know how to spot a scam...

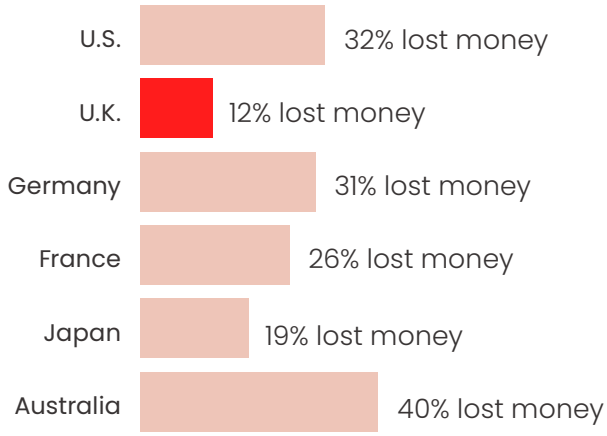


...yet report at a higher rate that their biggest barrier to online protection is understanding how to implement cybersecurity measures.



U.K. SMBs worry the least about cyber-attacks...

...and are also the least likely to lose money in a hack.



Preparation is key to preventing cyber crime

The key to effective cybersecurity is being prepared. Preventing an attack is far simpler and less costly to your business than dealing with the aftermath. Here are a few important elements to a good cybersecurity plan for SMBs:

#1: Train your employees

Of the small businesses we surveyed, 72% provide cybersecurity training for their employees. But less than half of the business owners and IT professionals (46%) are fully confident in employees'/colleagues' ability to take necessary steps to protect devices and IP.

Cybersecurity training should be more than an onboarding video. Every employee should know what they can do to prevent attacks, the company's plan in the event that one takes place, and what their responsibilities are in terms of data security, reporting, etc.

#2: Carry out risk assessments

Conducting risk assessments can help identify vulnerabilities, ensure your business is not at risk for a major attack, and ensure compliance with government rules and regulations.

#3: Deploy antivirus software

Antivirus software can protect your devices from a variety of threats, including viruses, spyware, ransomware, and phishing scams. The best software offers tools to clean and reset devices as well as to protect them in the first place.

#4: Keep software updated

Many of the more harmful malware attacks take advantage of software vulnerabilities in common applications like operating systems, browsers, and any other key programs small businesses use.

In fact, 30% of the small businesses that experienced cyberattacks reported the attacks occurred due to a vulnerability in outdated or unpatched software that was breached.

Software updates often include critical patches to security holes, making them one of the best lines of defense—and one of the simplest.

#5: Back up your files regularly

Cyberattacks often result in data failures. That's why it's essential to back up files regularly so data can be retrieved if necessary.

#6: Encrypt key information

Encryption allows technology providers like website owners to convert sensitive information, such as credit card numbers, passwords, or other financial details, into a code that cannot be read by cybercriminals. McAfee® Business Protection™ includes a secure VPN to keep data private and secure with bank-grade Wi-Fi encryption.

#7: Limit access to sensitive data

Cyberattacks aren't always high-tech—hackers often access data through social engineering. In preparing cybersecurity plans, businesses need to consider the human element, too.

When fewer people have access to critical data, businesses can minimize the impact of a data breach and reduce the possibility of giving unsuspecting employees authorized access to data. Creating a plan that outlines which individuals have access to various levels of information can help ensure that roles and accountability are clear.

#8: Secure your Wi-Fi network

Wireless networks are particularly vulnerable to cyberattacks because they use radio waves to transmit data, which is why securing your Wi-Fi network is crucial to protecting your data.

McAfee's Wi-Fi Scan will automatically scan and alert you when attempting to connect to an unsafe Wi-Fi network so you can turn on your VPN or choose a different network. Feel confident that your connection is safe before sharing any sensitive data.

#9: Ensure a strong password policy

To effectively protect your accounts from being hacked, it's important that you have a strong password with each account that you create.

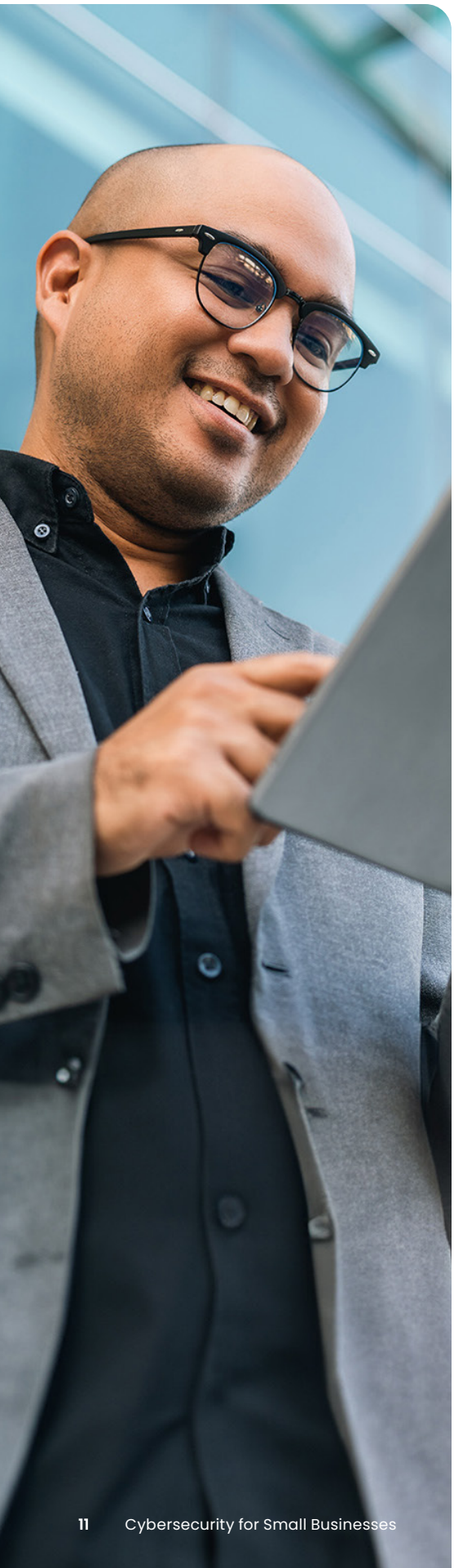
A strong password should be at least 7-8 characters long and use a combination of numbers, symbols, and both uppercase and lowercase letters. Other key measures are to change passwords every day, use different passwords for different accounts, and never write them down.

McAfee Business Protection includes a Password Protection Status that sends alerts if the company's devices are not password protected.

#10: Use password managers

When you create strong, unique passwords for every device and account, it's difficult to remember each one. A password manager stores your passwords and automatically generates the correct username and password for each account.

McAfee® True Key is designed to create lengthy, strong, unique passwords and includes local data encryption, the support of numerous browsers, the ability to sync across PC, Mac, iOS, and Android devices, and a variety of methods for signing in.



#11: Use a firewall

A firewall protects both hardware and software and can block or deter viruses from entering your network. With a firewall in place, you can protect your business's network traffic and stop hackers from attacking your network by blocking certain websites.

#12: Use a Virtual Private Network (VPN)

VPNs protect your data by preventing others from reading it as it passes over the internet. By replacing the IP address of your device with a different IP address, VPNs hide your location for additional privacy. VPN encryption also anonymizes network traffic, so advertisers trying to serve ads targeted or based on customer behavior aren't able to obtain your browsing or search habits through conventional means.

#13: Guard against physical theft

Protecting your hardware is just as crucial as protecting software. Preventing unauthorized individuals from accessing devices, physically secure devices, and adding trackers to recover lost devices are a few steps business owners can take to guard against theft. And setting up remote wiping capabilities can also protect data on lost or stolen devices.

#14: Don't overlook mobile devices

As mobile devices are increasingly used for business purposes, it's essential to consider them in your cybersecurity plans. Asking employees to password-protect mobile devices, install security apps, and encrypt their data is key to preventing criminals from stealing information while mobile devices are on public networks.

#15: Ensure third parties you work with are also secure.

When working with business partners or suppliers that might need access to your systems, make sure they follow strong cybersecurity practices before sharing access.

Introducing McAfee Business Protection

Cybercrime is increasingly targeted at small businesses. But by having the right tools and support, business owners can keep their operations secure and their employees and customers protected.

We're pleased to offer McAfee® Business Protection™ as an exclusive solution for Dell small business customers. McAfee Business Protection is purpose-built with small businesses in mind. It can help secure your business from hackers, malware, viruses, and more with a single solution.

All-in-one: helps secure business, data, devices, online connections, and more with a single solution.

Simple and guided: simple setup with automated protection and timely alerts makes securing one's business a breeze; and it can all be done from the Security Console. Timely alerts to let you know when something needs your attention, even when on the go.

Grows with you: it's protection that grows as your business grows. Employers can easily extend protection to each employee and their devices.

A few key features of the service include:

- **Security Console:** Easily view the company's protection status, manage employee invitations to set up protection, and take necessary actions, all in one place. It even works on mobile.
- **Next-gen Threat Protection:** Award-winning protection for unlimited[1] business devices from threats known and unknown, including malware, ransomware, viruses, and more with lightning-fast scans that keep devices running smoothly.
- **User-managed protection:** Each employee will receive an invitation to set up protection from their employer and can then create their own login, can set up their own data and device protection, and take necessary security actions, all under one single business subscription.
- **Secure VPN:** Keep data private and secure anywhere with bank-grade Wi-Fi encryption. VPN can be set to connect automatically when accessing an unsecure network.
- **Security Report:** Highlights status and open items to improve the protection posture for your business, devices, and employees.
- **24/7 Dedicated Support:** Get 24/7 technical assistance and peace of mind from McAfee's dedicated support team via phone or chat to help set up protections, and more.

1. Unlimited is subject to the reasonable and foreseeable scope of a typical small business.

Methodology/About this study

- In September 2023 McAfee conducted a study about online security among small businesses in six countries: U.S., U.K., Germany, France, Japan, Australia.
- Respondents were either **[business owners and IT professionals]** working for an organization with less than 250 employees.
- The research was conducted between August 24th – September 5th, 2023, by MSI-ACI via an online questionnaire to 700 business owners and IT Professionals from six countries.

About McAfee

McAfee is a worldwide leader in online protection. We're focused on protecting people, not devices. Our solutions adapt to our customers' needs and empower them to confidently experience life online through integrated, easy-to-use solutions.

www.mcafee.com

For more information,
visit mcafee.com

McAfee™

6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com

gd-cybersecurity-for-small-businesses_0124 JANUARY 2024