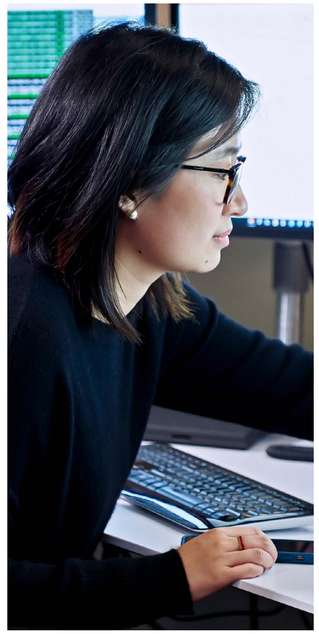
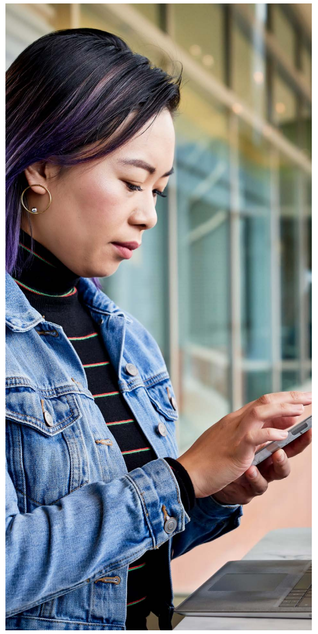
Microsoft

# A 5-step security plan every business can start today

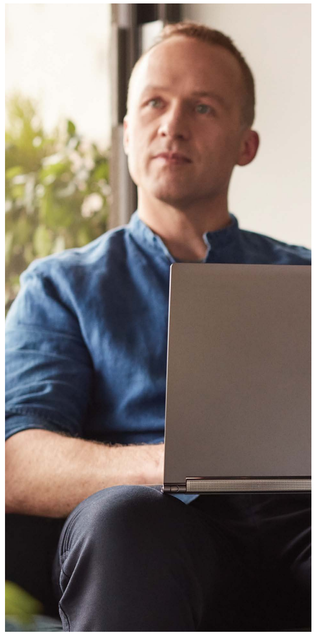
# Key insights



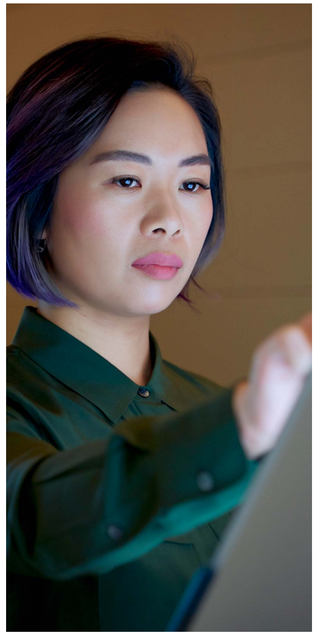
## Introduction



## Strategy 01:
On security, think bigger

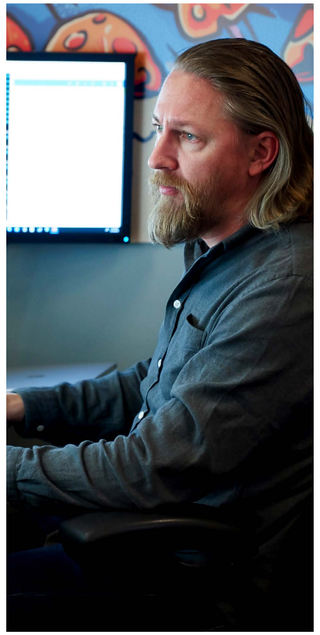


## Strategy 02:
Take small steps on security today, bigger steps as soon as you can

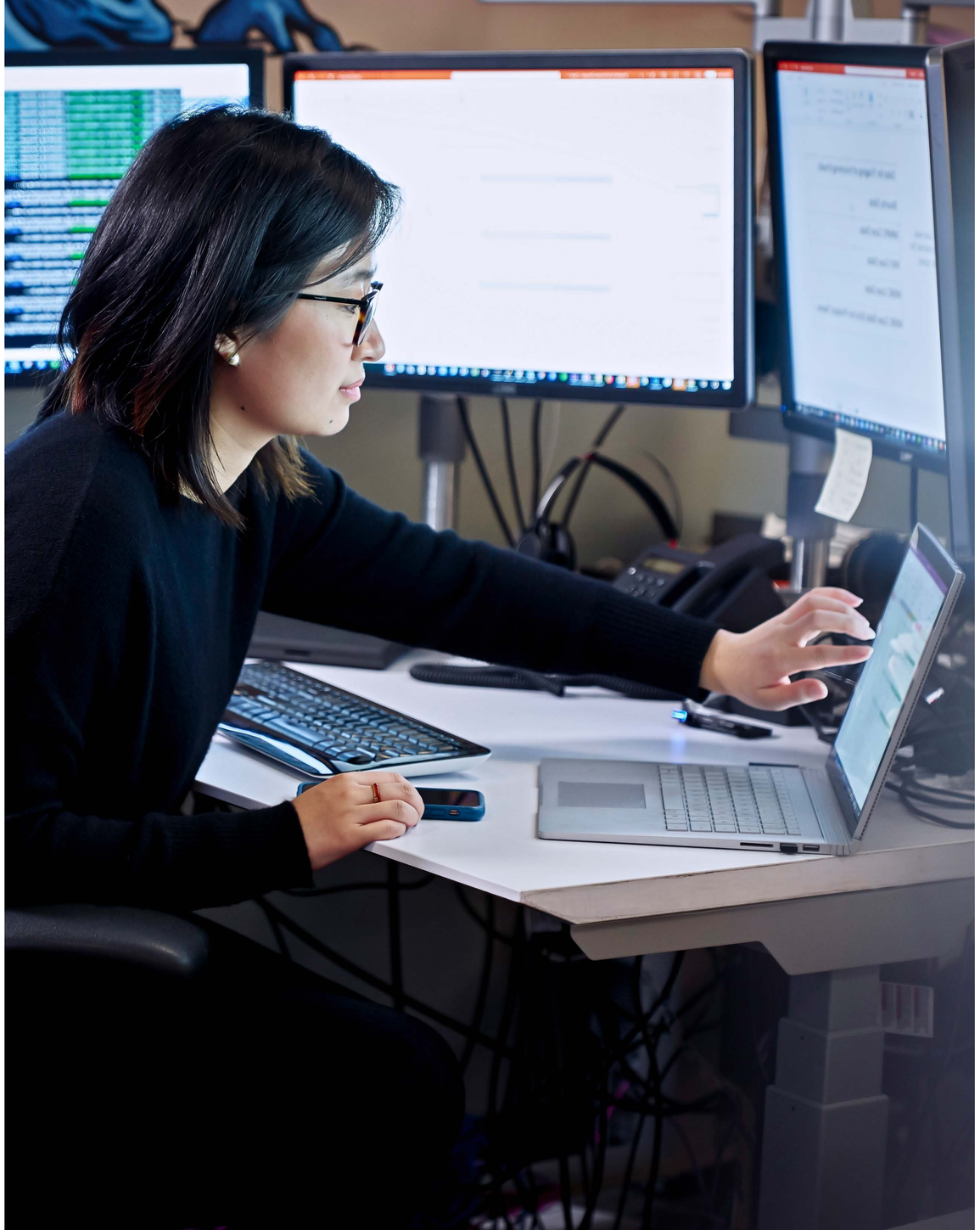


## Strategy 03:
Understand the threat from within

## Strategy 04:
Be vigilant



## Strategy 05:
Prepare for the worst



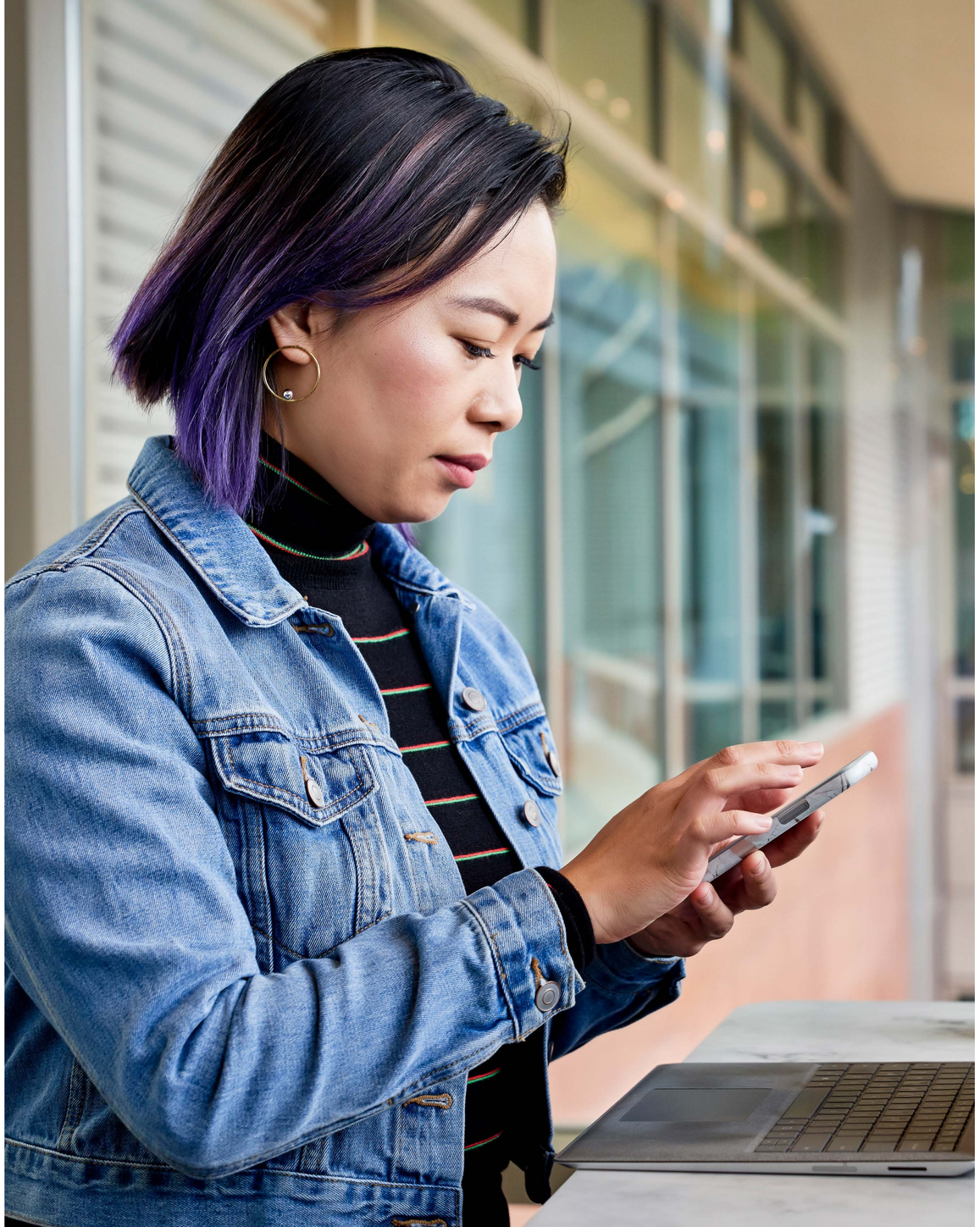


# Introduction

As a business leader, you're paying close attention to issues around cybersecurity. You have to. You've seen news stories about data breaches and you understand that cyberattacks are getting more sophisticated every day. Every business is a digital business in some way, and yours is no different.

According to our recent research, the majority of business owners are beginning to take steps to protect their business with common-sense habits like keeping software up-to-date and enforcing strong passwords. That's great news.

But it's just a start. To confidently defend against cyberattacks, businesses must take steps that advance their security position. Here we're sharing some simple ways to do that.





# Strategy 01

## On security, think bigger

Some businesses wonder if they are big enough to even be noticed by hackers. This idea persists because newsworthy cyberattacks happen to very large companies—that's what makes them newsworthy. When a large company has a data breach, thousands or millions of people are impacted. When a small business has a data breach, the impact is less, and we rarely learn about it. But cyberattacks on small and medium-sized businesses are just as common as attacks on larger corporations.

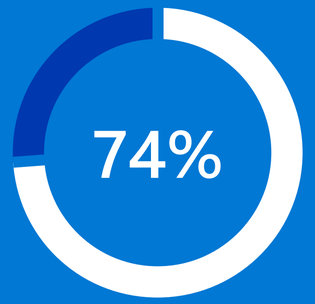
# Take action

**Become a small company with a big-company attitude on security. This isn't about budget. It's about awareness and mind-set.**

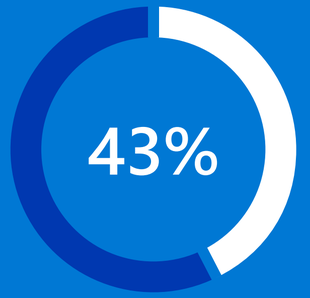
**01** Adopt a security-aware approach. This means looking at security the same way you look at getting things done—you just do it.

**02** Assign IT security responsibilities to someone with the interest and aptitude to take on the tech. This might be the person in charge of rolling out new software across the company, or it might be someone on your engineering team who wants an opportunity to grow.

**03** Train your employees on security best practices. Keep the trainings rolling every six to 12 months so the topic stays fresh in their minds.




74% of small and medium sized business owners don't believe they are likely to be attacked at all.[1]



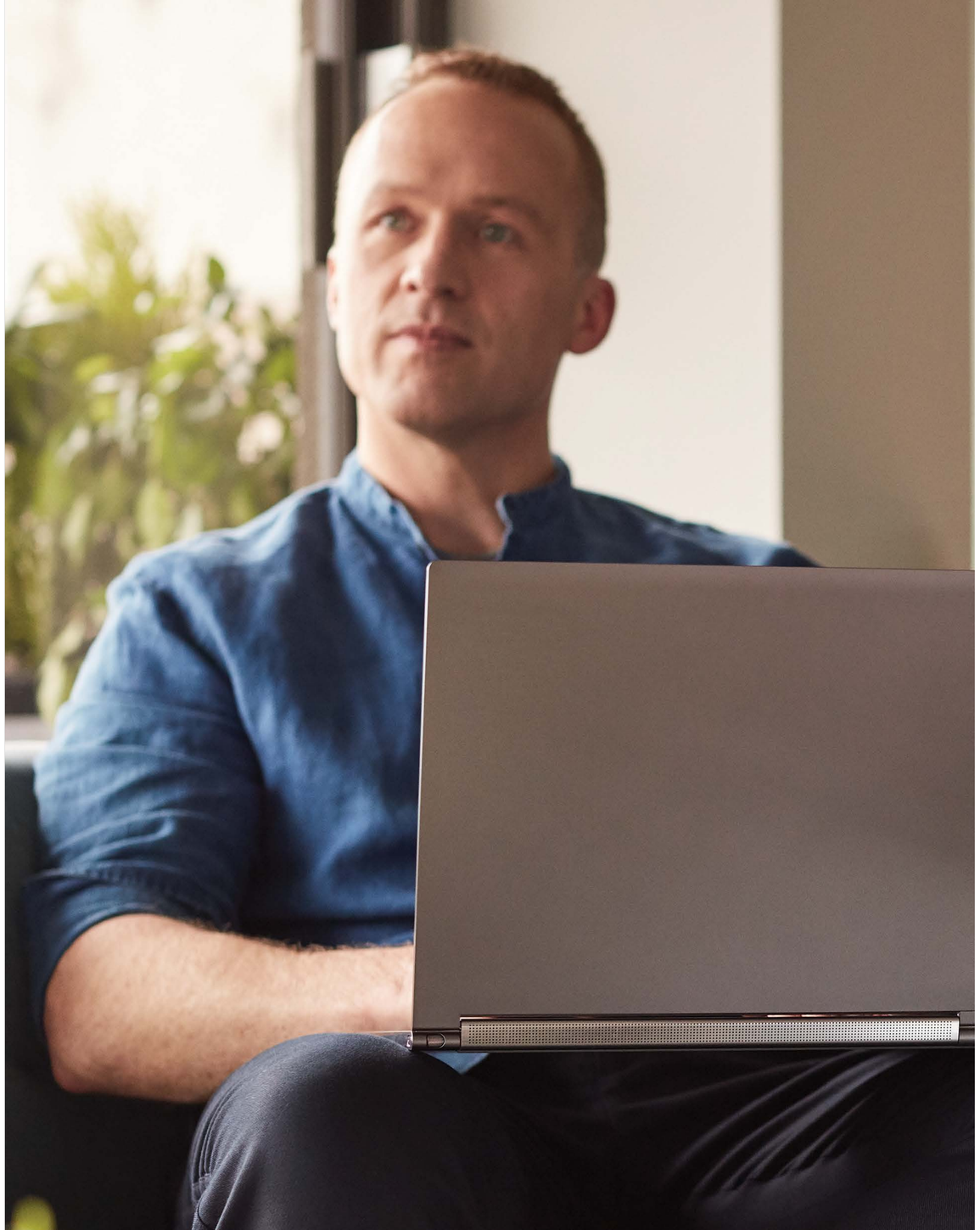

43% of cyberattacks target small and medium-sized businesses.[2]

I wish I had been more educated in what could happen … to think of me, middle of Small Time, USA; I just didn’t think that it could happen to me. I’m as vulnerable as any big corporation.

Business owner

Want to check your security readiness?

Take the Microsoft Security Assessment





# Strategy 02

## Take small steps on security today, bigger steps as soon as you can

If you're worried about spending money on cybersecurity today, consider this: you might not have the budget for recovery from a cyberattack. Of businesses that lost access to their data for three months or longer, only 35 percent remained profitable.[3] The truth is that some of the most powerful security moves you can make don't cost anything. And you don't have to be an expert to implement them.

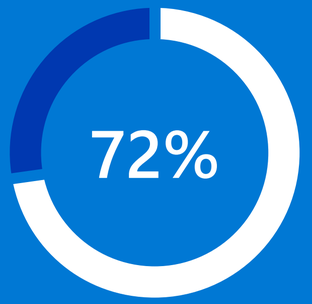
## Take action

**We're not saying you shouldn't invest in your company's cybersecurity. You absolutely should. But there are some low- or zero-cost things you can do to strengthen your defenses immediately.**

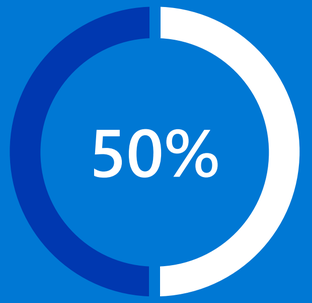
**01** Educate your people on smart password best practices, and ensure they're enforced. That means making sure passwords are longer than eight characters, not writing down passwords, and making sure they're different than personal passwords.

**02** Update software regularly. Those prompts for software updates should never be ignored. Many involve security patches that you wouldn't otherwise get. Make sure anyone working on a company computer enables automatic updates, and doesn't delay them when the updates are prompted.

**03** Review usernames and passwords for the more public devices in the office—routers, copiers, and other Wi-Fi connected devices. Hackers often know the default passwords.




72% of businesses agree that it typically costs more to recover from a cybersecurity attack than it does to prevent one.[1]



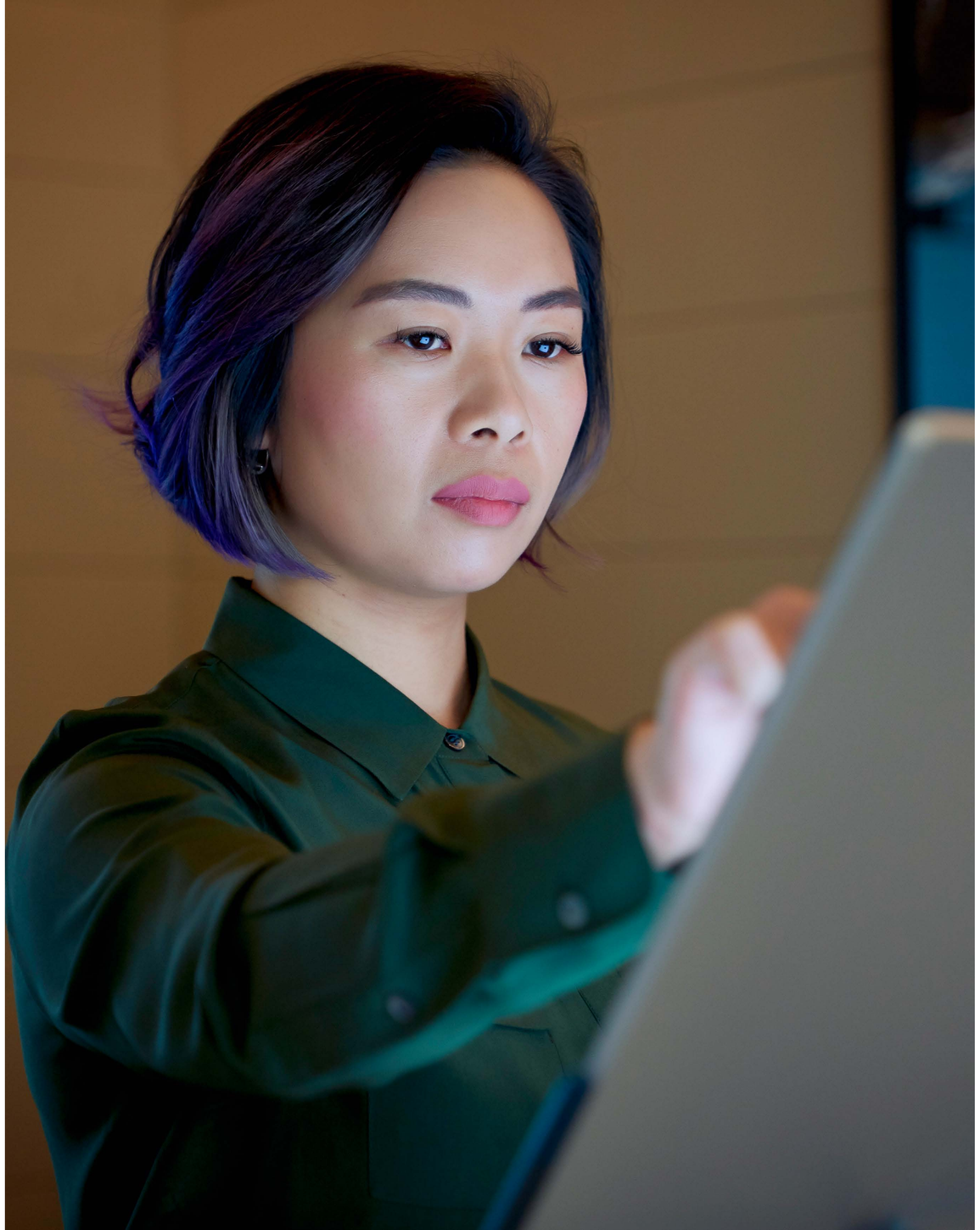

More than 50% of respondents had less than $5,000 per year for IT security, and half of those had less than $1,000 per year.[4]

**We've learned a couple of important things. One is to outsource as many things as you can. I'm a clothing store. I am not a technology security company. If I can find providers to take that piece that's not my specialty, and handle it for me in a secure, correct way, I'm going to do that.**

**Robin,**
*Small business owner*

**Interested in a security consultant that's the right size for your business?**

Search Microsoft's partner program





# Strategy 03

## Understand the threat from within

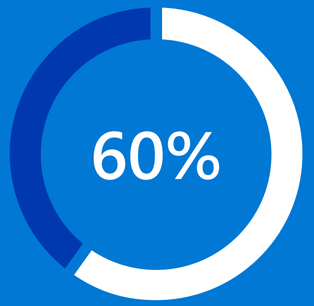
Smaller businesses prioritize defense against outside threats.[4] This is appropriate. But given the number of security events tied to employees, you run the risk of underestimating the threat from within. Not all internal breaches are intentional, and we can't always predict how an employee will behave. In fact, 30 percent of security events are attributed to careless or uninformed employees.[5]

# Take action

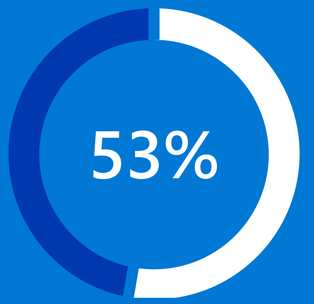
**Preventing accidental or intentional breaches from the inside takes a two-step effort.**

**01** Since many threats come through email, it's easy for an employee to unknowingly share a virus with coworkers. Make sure your software provides comprehensive protection against malware, spyware, and viruses across email, applications, the cloud, and the web.

**02** Use an identity and access management solution, such as Azure Active Directory (also part of Microsoft 365), which supports single sign-on and gives employees a single, secure identity for accessing network resources.




60% of breaches stem from compromised endpoints like a laptop or phone.[6]



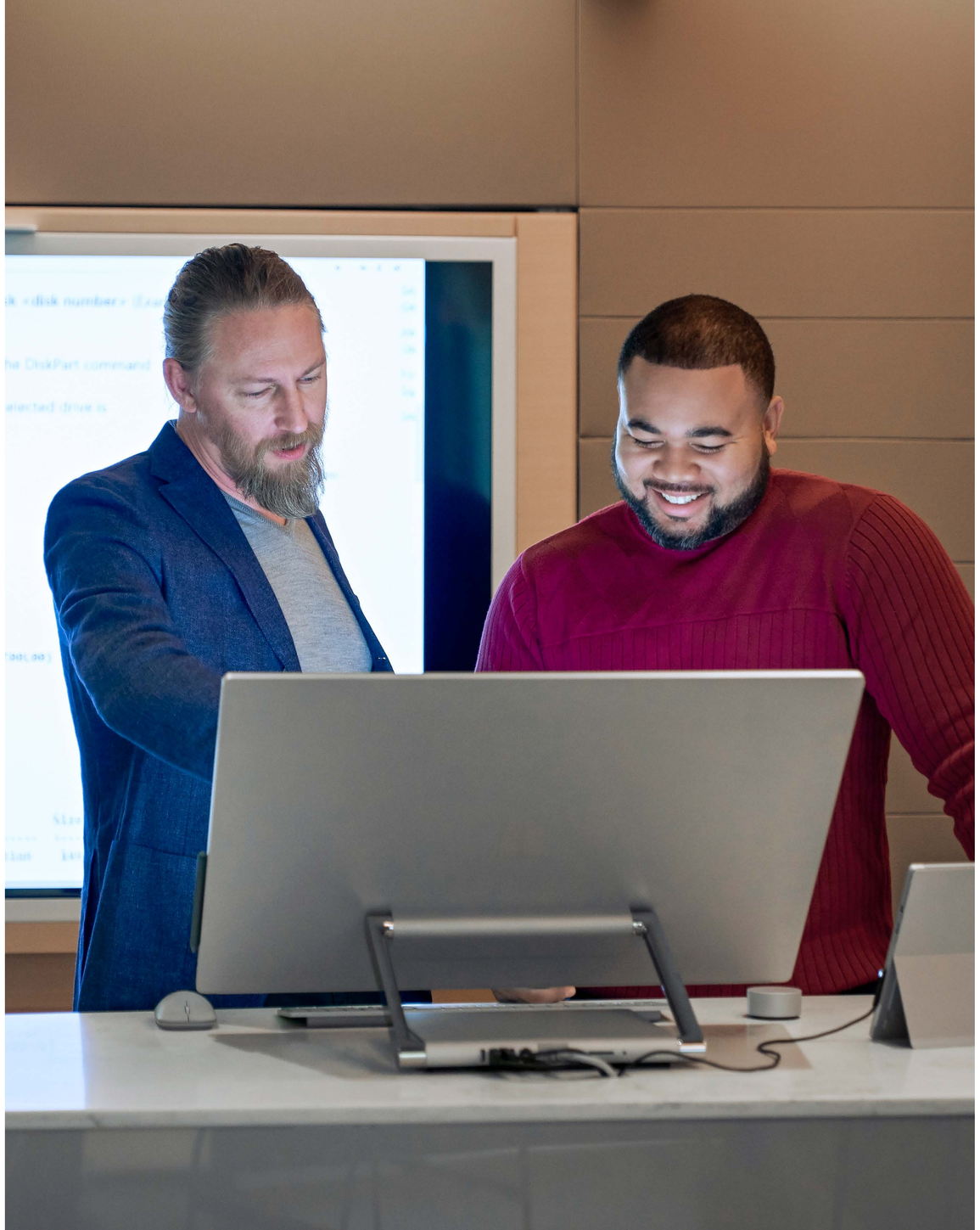

In the past 12 months, 53% of organizations have experienced insider attacks against their organization.[7]

**Our business is still unsure to this date if the incident was caused [purposefully] by an employee or some type of phishing attack. The end result was the business was completely shut down for a day, including access to any file and purposefully taken offline, corrupted.**

Medium-sized business owner

Want to find out how secure your users and accounts are?

Take the Microsoft Security Assessment





# Strategy 04

## Be vigilant

It's hard to imagine a cyberattack going unnoticed. Surely it would be obvious if data was breached or a hacker gained access to secure files. But it takes an average of four months to recognize that a cyberattack has taken place.[3] Malicious actors have become increasingly sophisticated, so it's not uncommon for them to stay hidden for weeks or months—continuously stealing more and more data and slowly increasing access to your accounts, devices, and files.

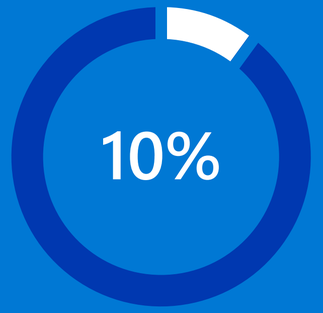
# Take action

**For businesses that don't have a big budget for cybersecurity, automation and intelligent solutions can increase your efficiency in detecting and thwarting attacks. Your security solution should:**

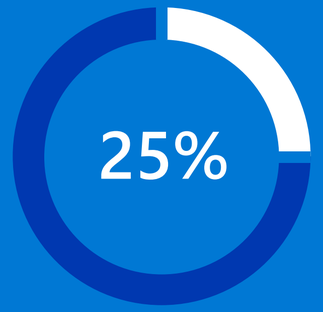
Have real-time reports on suspicious activities

Have automated and intelligent alerts that don't require a lot of tech expertise to decipher

Integrate across your business assets, such as your routers, hardware, software, laptops, and mobile devices




10%+ of businesses never even realize they've been attacked.[3]



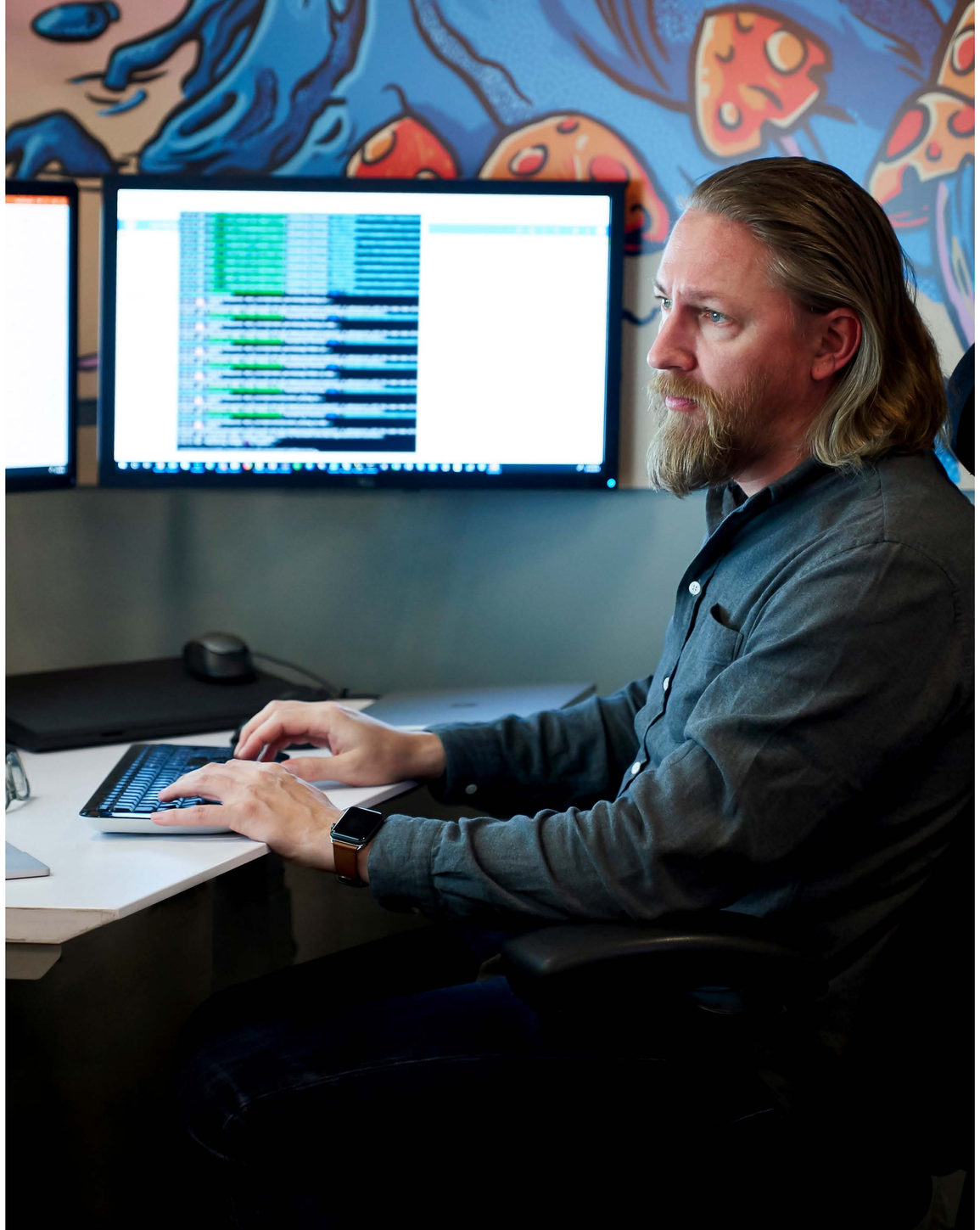

Less than 25% of small and medium-sized business owners invest in solutions to track the incoming signals, security alerts, and recommendations they receive.[3]

# You have to be diligent in keeping an eye on what is going on out there. You have to be proactive. If it looks suspicious, assume that it is.

**Rachel,**
*VP of operations in the catering industry*

**Want to see how protected you are from threats?**

Take the Microsoft Security Assessment





# Strategy 05

## Prepare for the worst

Whether your business has suffered a security event or not, uncertainty about what kind of attack might come and the scope it might have can keep you up at night. In the most extreme cases, businesses have closed due to an attack. But  you can recover, and if you’re prepared, you can limit the losses.

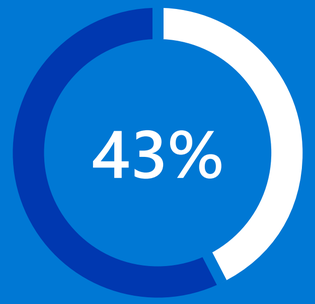
# Take action

**There are nearly endless actions you can take to be absolutely prepared for any cyberattack scenario. But some of the simplest actions can give you the protection and defense you really need:**

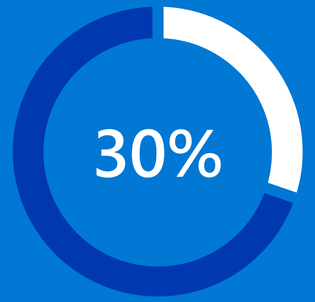
Back up critical data, preferably in the cloud, and have a system in place to do so regularly.

Schedule regular employee education on basic cybersecurity practices.

Implement a detection system to make sure you are getting a comprehensive and real-time view of useful security data and activity.




Of the small businesses that were attacked, 43% took longer than a week to recover.[1] The average cost of an attack that takes more than a week to recover from is $79,841.[7]




Only 30% of small and medium-sized businesses use technology that protects against the most advanced threats.[1]

**The impact of the Cryptolocker (type of ransomware attack) was pretty heavy. We were down for two and a half days. You're talking about all the areas from design to pre-production to production, shipping, orders. I would say about $50,000.**

**Alan,**
*IT director in the fashion industry*

**Want to see how effectively you're managing security?**

Take the Microsoft Security Assessment

## Protect, detect, and respond easily

**Technology that protects against the most advanced threats, such as those included in Microsoft 365, gives you the following critical features:**

Defend against cyberthreats with Office 365 Advanced Threat Protection, Microsoft Defender, and Azure Multi-Factor Authentication.

Protect business data with Office 365 Data Loss Prevention, Azure Information Protection P1, and Conditional Access.

Manage your devices with Microsoft Intune, Office 365 Shared Computer Activation, and Windows Virtual Desktop.

## State of security report

**We surveyed 2,000 small and medium-sized businesses from four countries (the United States, United Kingdom, Germany, and Brazil), interviewed 12 business owners, and reviewed the existing literature to gain a holistic understanding of attitudes and approaches toward security. This e-book, "State of security for small and medium-sized businesses," includes data from that research. Interested in the details?**

Get e-book

# See how you're doing on cybersecurity

To get a strong understanding of your security position, take the Microsoft Security assessment. You'll get specific recommendations to make your business more secure.

Take the assessment

Microsoft



[1] Microsoft's Global Security Survey for Small and Medium-Sized Businesses.
[2] Cybersecurity Statistics – Numbers Small Businesses Need to Know.
[3] "2017 State of Cybersecurity Among Small Businesses in North America," Council of Better Business Bureaus, 2017.
[4] "2018 SMB IT Security Report," Untangle, 2018.
[5] SMB Security Qual.
[6] "Top Five Security Threats Facing Your Business and How to Respond," Ann Johnson, Microsoft Security Blog, 2016.
[7] "Insider Threat 2018 Report," Crowd Research Partners and Cybersecurity Insiders, 2018.