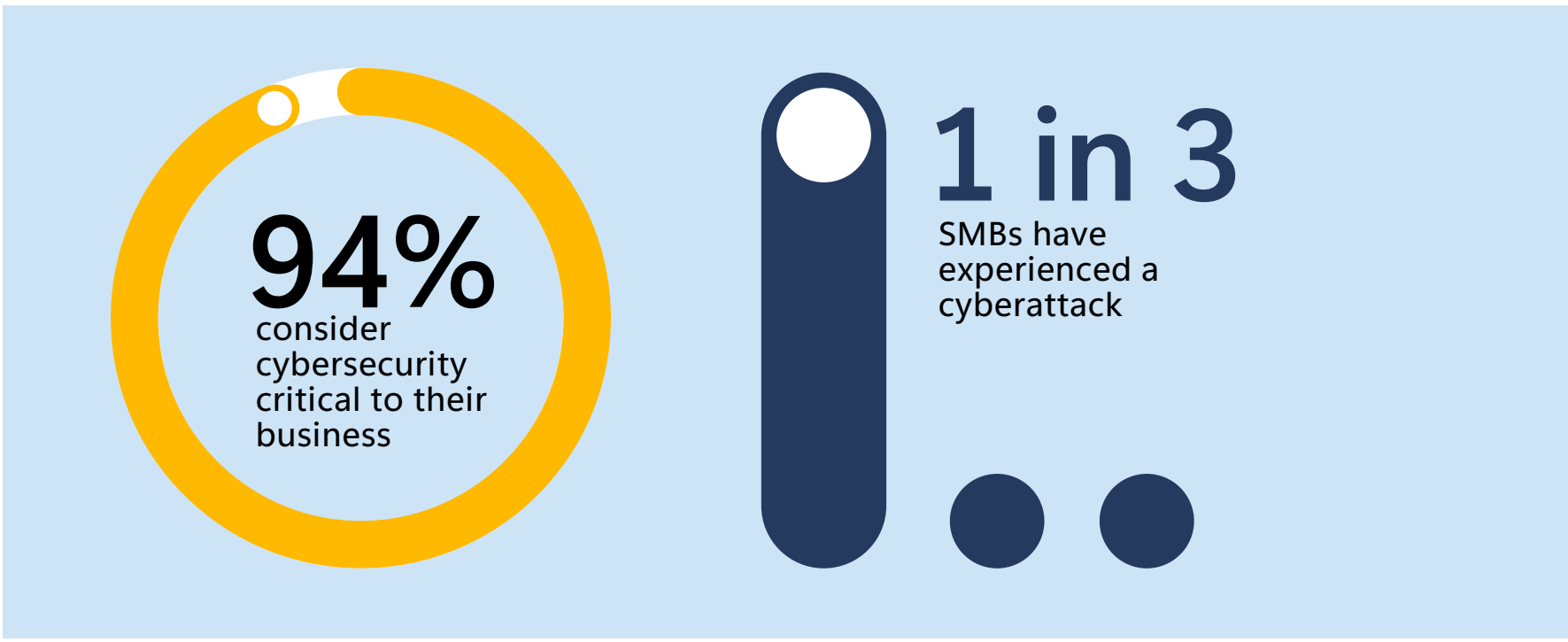
Microsoft Security

New research: Small and medium business (SMB) cyberattacks are frequent and costly

Safeguarding against escalating and evolving threats is now considered key to business success

Remote work, personal device use, and a lack of employee security training are escalating cybersecurity vulnerabilities for SMBs. A new survey* of 2,000 U.S. and U.K. IT security product decision-makers/influencers shows that SMBs understand the risk and are experiencing it firsthand.

This report shares findings from SMBs with 25-299 employees and reveals that a full 94% consider cybersecurity critical to success. One in three have experienced a cyberattack in the past year.



SMBs are susceptible to cyberattacks and aftereffects since they typically lack the tools and internal IT expertise that large companies use to prevent, detect, and respond quickly.

This new research, gathered in partnership with Bredin, makes it clear that SMBs understand the threat. SMBs are prioritizing cybersecurity and recognize that protection is a key business success factor.

In this report, you'll discover:

- How cyberattacks can cost SMBs millions of dollars
- The mindset that puts some SMBs at high risk of an attack
- That 81% say AI increases the need for additional security
- Why personal device use on company networks is a top challenge
- That 80% of SMBs intend to increase their cybersecurity spending
- Why 8 in 10 say lack of staff security awareness is a concern

SMBs are prioritizing cybersecurity; read on to learn why this is trending and how businesses are protecting themselves.

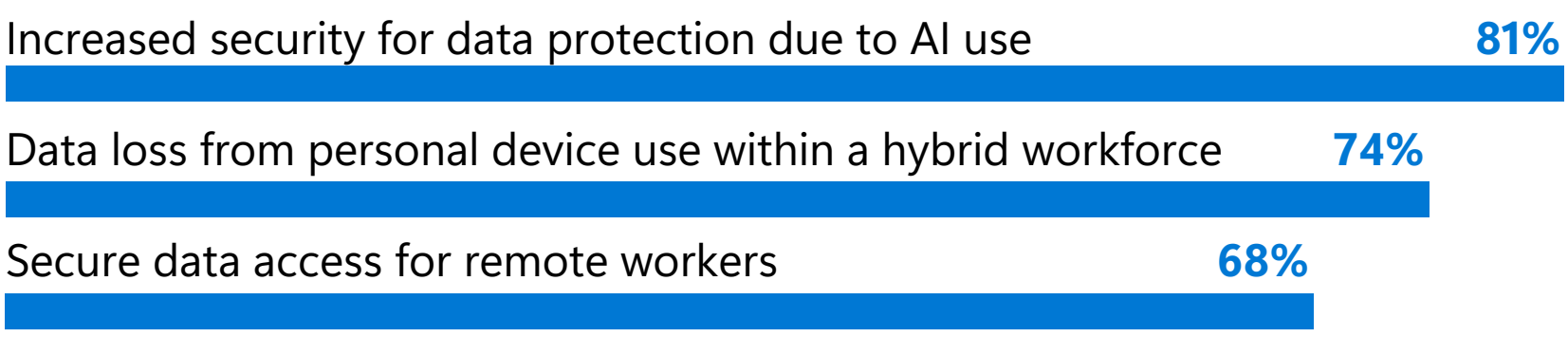
The real cost of cyberattacks

Nine in ten SMBs agree that cyberthreats are an increasing peril. Many have learned from experience about the financial, reputational, and productivity costs of an attack. The research shows the average total cost of an attack is $254,445, but ran as high as $7 million.

Average and high end of cyberattack costs:

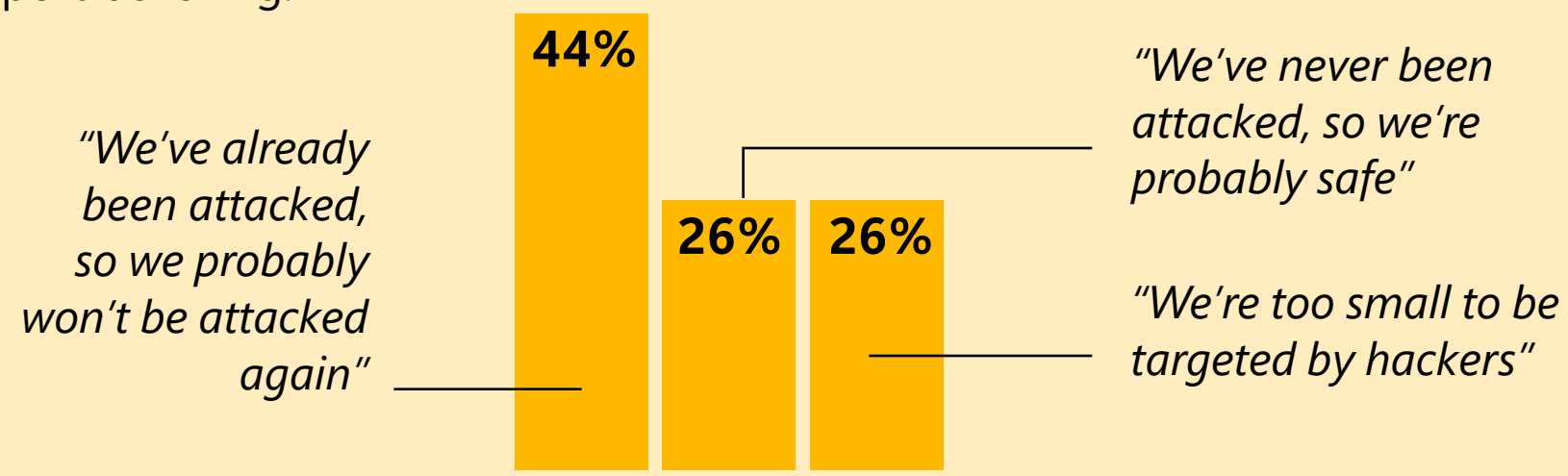
	Average costs	High end of costs
Investigation and recovery	$77,957	$3,930,000
Fines	$20,623	$655,000
Cost to reputation	$73,393	$1,310,000
Missed opportunities	$23,806	$6,550,000
Other costs	$58,666	$3,275,000

Businesses are aware of the impact and SMBs are focused on:



Among SMBs not using AI security tools now, 53% will deploy them in the next six months.

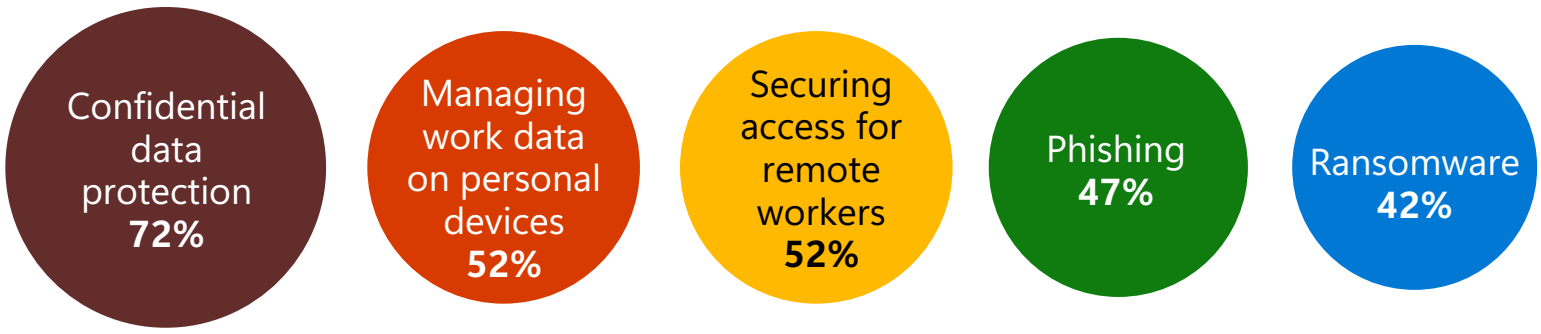
Despite cybersecurity awareness, the survey also uncovered some SMB mindsets that may put companies at increased risk of an attack. Some SMBs in the survey report believing:



The need to secure SMBs

Ninety-four percent of SMBs consider cybersecurity critical, but without the tools and internal expertise to keep people, data, and devices secure, SMBs are vulnerable.

As SMBs manage the threat landscape, their top challenges include:



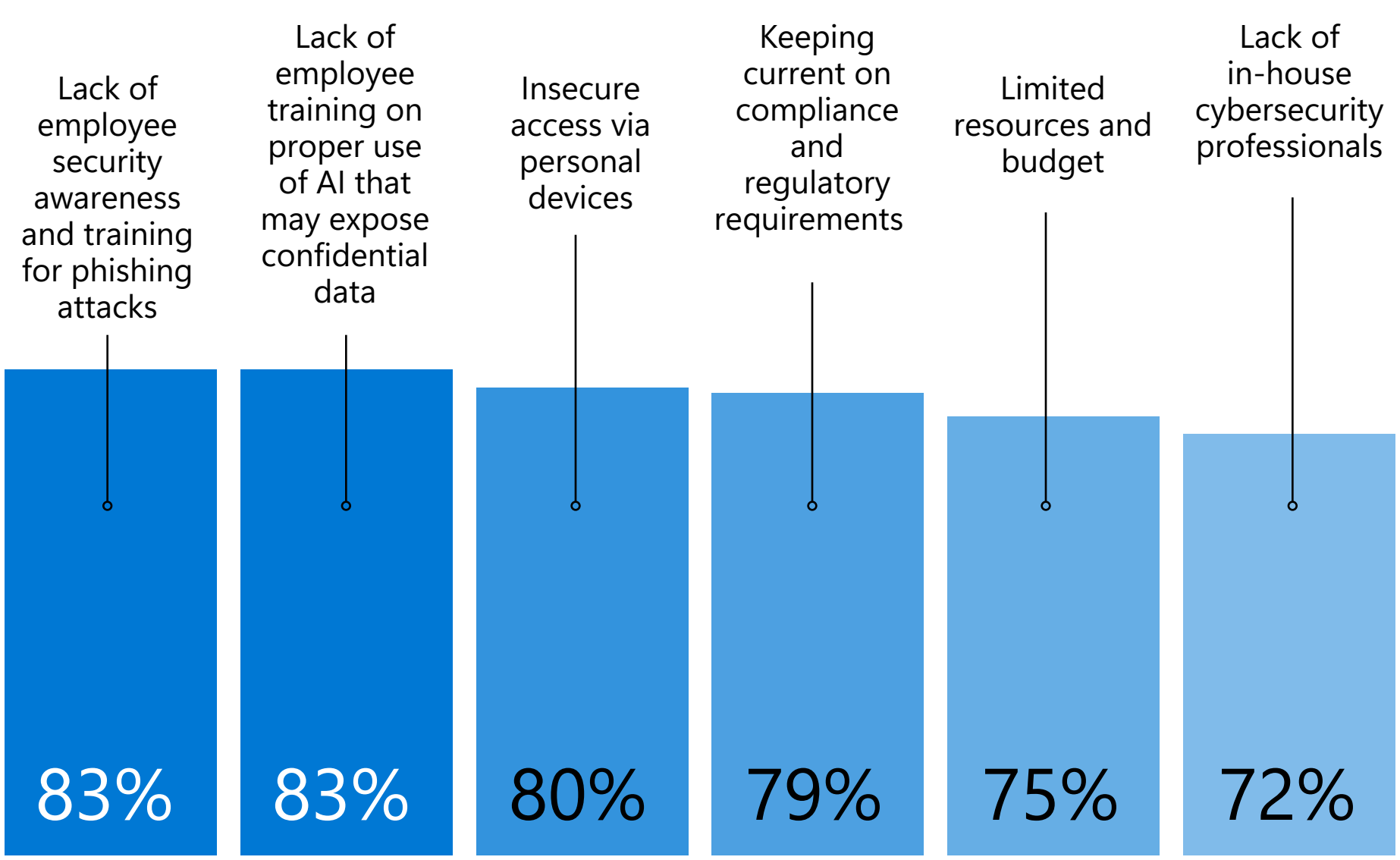
When you ask SMBs about protecting against threats, roughly one in five say their business is only somewhat effective at the following security practices:

- Protecting company network with firewalls, encryption, and other measures
- Using multi-factor authentication (MFA) wherever possible
- Ensuring employees use strong, unique passwords
- Implementing policies to manage secure password/PIN access to mobile devices and securing work data on personal devices
- Implementing robust data backup with offsite storage and periodic testing
- Implementing access control to limit employee system and data access to an “as needed” basis
- Enabling automatic software updates ensuring all systems are patched and up to date
- Maintaining and updating a cybersecurity incident response plan
- Conducting regular security audits
- Conducting regular employee cybersecurity training

Less than 30% of SMBs manage their security in-house. When it's time to research and select a cybersecurity solution, the top five go-to sources are:

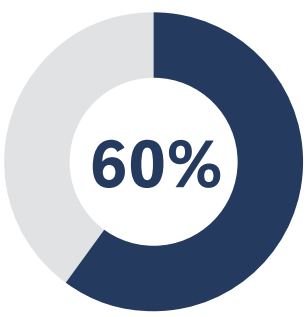
1. IT consultant/ Managed Services Provider (MSP) recommendation
2. Cyber insurance recommendation
3. Web search
4. Analyst reports
5. Rating/ review sites

Beyond choosing and acquiring the right security tools, SMBs say they face other security struggles:

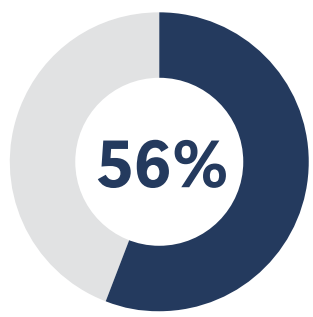


SMB cybersecurity plans

SMBs are juggling a need to modernize and support their staff with an imperative to protect company health and assets. It's a significant undertaking and can include securing access to emails and files; protecting data while allowing for collaboration; safeguarding against phishing, spam, and malware; and securing mobile devices. Approximately 80% of business leaders surveyed intend to increase their cybersecurity spending. The two motivators for improving or upgrading SMB cybersecurity measures are:

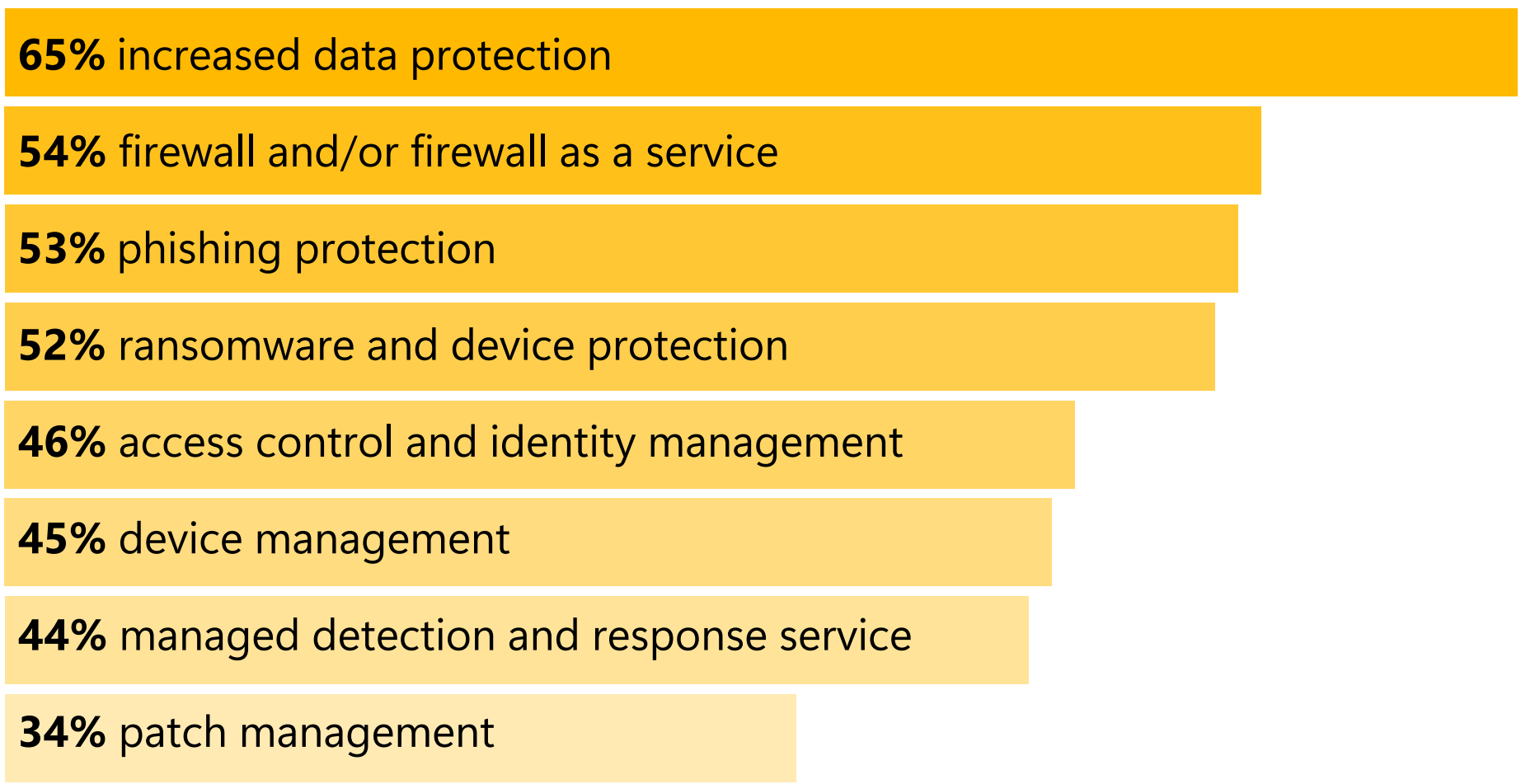


Protecting company from financial losses **60%**



Safeguarding client/ customer data **56%**

Where will SMBs focus their spending?



Microsoft Security

SMB technology leaders understand that cybersecurity risks are increasing.
Real SMB vulnerabilities exist in the form of fewer tools and less in-house technical expertise to thwart cyberattacks than in larger companies. The cost in expenses, reputation, and productivity if an attack occurs are significant. Savvy SMBs are taking steps to shore up protection for precious company and customer data and other assets. Putting tools and technical expertise in place to prevent attacks has become a key success factor.

To learn more about Microsoft Security solutions for SMBs, including Microsoft 365 Business Premium and Microsoft Defender for Business, please visit our website.

Methodology
*An online survey of 2,000 IT Security product decision-makers/influencers at U.K. and U.S. businesses from September 10-26, 2024. Data in this report focuses on SMBs with 25-299 employees.