SMB CYBERSECURITY DISCONNECT

Uncovering the Risks, Challenges and Human Factors to Close the Gap for Small and Medium-sized Businesses

Presented by LastPass

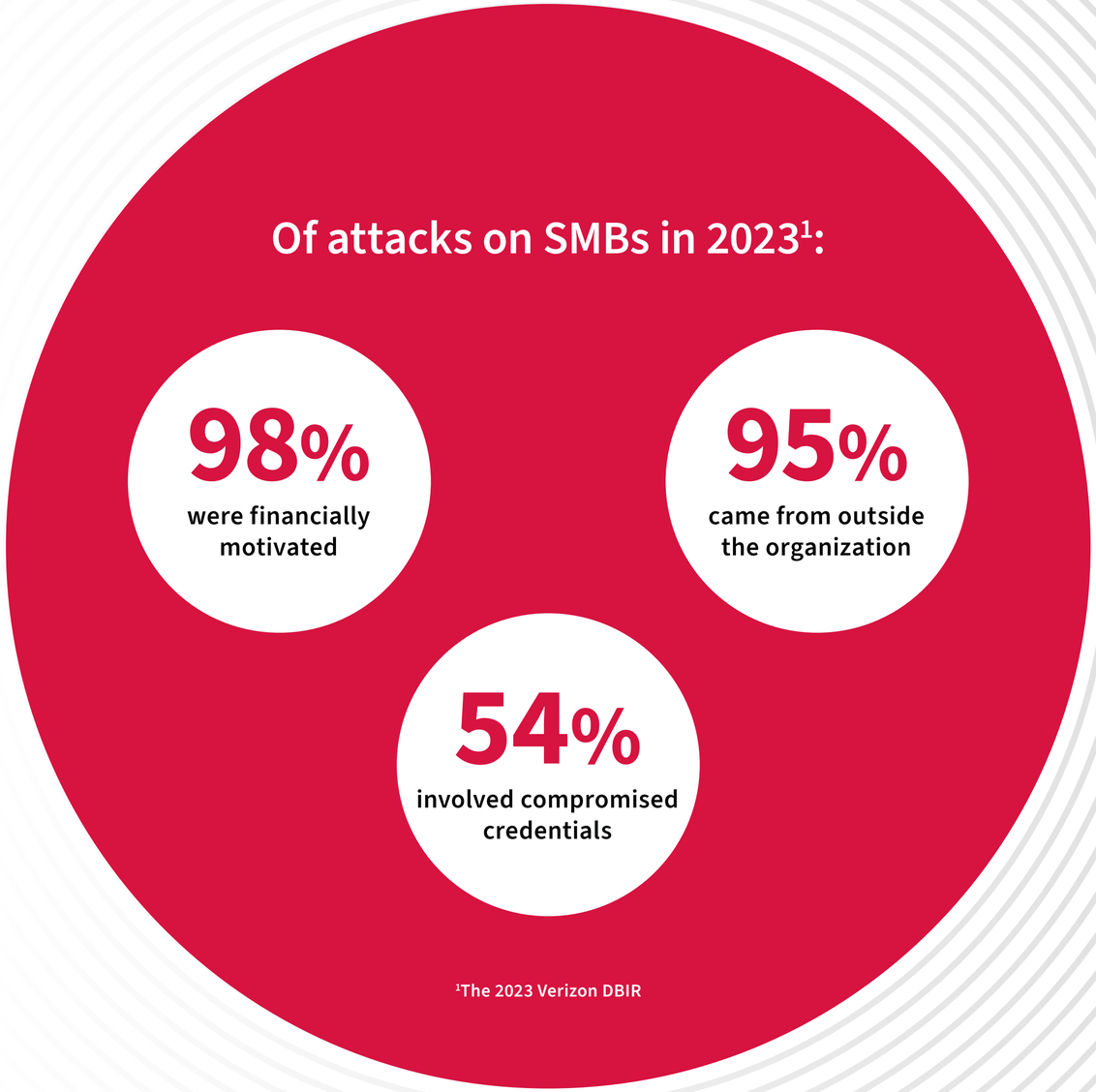
Small and medium-sized businesses are a growing target.

Cyberattacks directed at small and medium-sized businesses (SMB) have surged in recent years.

Why? There are two primary reasons:

First, cybercriminals have identified smaller entities as relatively easy targets, due to these organizations' relatively constrained resources and underdeveloped cybersecurity policies.

Second, small organizations can pose sizeable profits for cybercriminals. Bad actors are increasingly attacking SMBs in order to infiltrate larger organizations farther up their supply chain, as well as automated ransomware bots that can attack multiple organizations at once.



How are SMBs responding to these increasing threats?

The SMB Cybersecurity Report explores attitudes and behaviors around cybersecurity within these organizations.

LastPass commissioned research firm InnovateMR to conduct a survey of 633 US-based business and IT security leaders at SMBs. Small businesses were defined as having 10-499 employees, and mid-market as having 500-2,999 employees.

This report reflects the key findings of that survey.

Small organizations, big disconnect.

There is an accountability disconnect at SMBs between executive cybersecurity investments and risky employee behavior.

The LastPass survey found that while SMB leaders report investing more time, attention, and budgets toward cybersecurity, human factors are getting in the way – including lack of awareness, training and inconsistent policy adherence.

Together with policy and technology gaps, these factors continue to create significant security and business risks.

Investments are increasing.

SMB leaders report increasing attention to cybersecurity in the past year:

90% of IT leaders

80% of non-IT leaders

Budgets are likewise increasing at SMBs:

82% report increased cybersecurity budgets year over year.

Pro tip:

While these ***quantitative*** investments are promising, leaders should spend more time making ***qualitative*** investments to improving cybersecurity at their organizations, including policy, education and culture.

Leaders perceive low risks.

Those at the top who are held accountable for cybersecurity -- executives and IT leaders -- believe cybersecurity is stronger because they are more focused on it, and they are spending more money on it.

30%

Only three in 10 leaders believe their company faces a very high risk (8+ out of 10) of having a cybersecurity issue.

But that doesn't mean broader employee awareness and behavior are on the same page with leadership and spending.

Cybersecurity education has to bring all employees into that circle of accountability for behavior to change.

Pro tip:

A threat intelligence-led security program is critical to understanding risk, rather than just guessing what's coming.

Leaders must have an understanding of their crown jewels, who is coming after them, and their most likely threats.

Executives and IT leaders are overly optimistic.

The vast majority of executives and IT leaders believe employees understand the security expectations for their jobs, while non-IT leaders are decidedly less confident.

IT leaders also tend to believe adherence to policies is higher than their general business, non-IT security peers.

Who believes employees understand the security expectations of their job?

92%
of executives

93%
of IT leaders

78%
of non-IT leaders

Pro tip:

Leaders across an organization should consult together to determine true understanding among employees as well as the best route to achieve organization-wide cybersecurity policy compliance.

Policies are still being broken.

Significant numbers of leaders and employees admit to breaking cybersecurity policies, with interesting disparities across job roles and age groups.

1 in 5

business leaders admits to circumventing security policies

1 in 10

IT security leaders admits to circumventing security policies

1 in 4

younger workers are more likely to break policies

36%

of Gen Z professionals write down passwords, as opposed to 16% of other age groups

Pro tip:

Leadership should take “carrot and stick” cybersecurity approaches, with incentives for employees who follow policies and consequences for employees who break them.

Easy and clear policy exception processes can also help employees get their work done without taking dishonest measures.

Password management is critical.

IT security professionals at SMBs say password management is critically important to cybersecurity strategy, with nearly half reporting recent breaches due to compromised passwords.

The majority of leaders also report using a password manager at work – either company provided or one of their choice.

72%
say password management is critical

47%
report recent breaches due to compromised passwords

81%
use a password manager

1 Reference Article Name | **2** Reference Article Name | **3** Reference

Compliance, at a glance:

Non-IT business leaders cited lack of understanding, lack of importance, and the hectic pace of business as the top three barriers to security policy adherence.

Leaders see employees from the Baby Boomer generation as least likely to comply with security policies, while millennials and GenX staff are seen as most diligent.

Leaders also have varying views of security compliance by employee category:

- Business leaders believe compliance varies by job function, employee age, and work-from-home status.
- IT leaders believe the main factors are job function, department, and title.

SMB leaders are looking forward.

Leaders reported the following as the top cybersecurity threats facing SMBs in the next twelve months:

Phishing attacks

Cloud vulnerabilities

Data loss from ransomware of malware

Pro tip:

SMB leaders should also consider the growing role of artificial intelligence in the cyber threat landscape, including AI-powered phishing attacks.

Small organizations have taken big steps.

At SMBs, cybersecurity awareness and investments are increasing. These are positive, encouraging developments.

However, cybersecurity culture and policy still have a long way to go at these organizations. Human behaviors are still leaving SMBs vulnerable to attack.

SMB leaders should be proud of their efforts and keep up this positive momentum. In 2024 and beyond, they should focus on **education and policy enforcement around password management** and other proven cybersecurity practices.

With a password manager like LastPass, these leaders can reduce their organizations' use of passwords and reliance on human behavior – as well as prepare for a passwordless future.

LastPass

LastPass is a leader in password and identity management solutions that helps 100,000 businesses and millions of consumers secure their credentials at work and at home. Since 2008, LastPass has made logins easier, more secure, and accessible across virtually any device. Today, LastPass innovates for a passwordless future by supporting next-generation security solutions that respond to human behavior, including biometric logins and beyond.

Learn more via www.lastpass.com and follow us on Facebook, YouTube, LinkedIn, X and Instagram. LastPass is trademarked in the U.S. and other countries.

Learn more