The State of Cybersecurity for Mid-Sized Businesses in 2023:

Under-Staffed and Under-Resourced

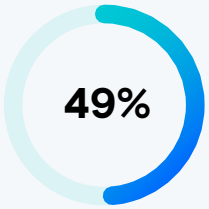
HUNTRESS

Table of Contents

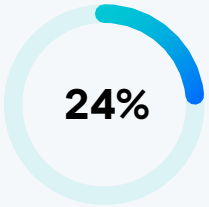
Key Findings

Cyber attacks are the greatest threat faced by mid-sized business.

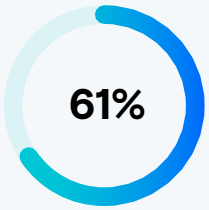
Some estimates place the potential losses faced by these entities at nearly $7 billion annually in addition to the operational disruption, loss of productivity and expense of recovering from an attack.



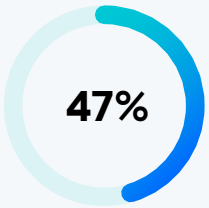
of mid-sized businesses **plan to spend more** on cybersecurity in 2023



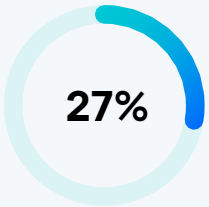
of mid-sized businesses suffered a cyber attack or were unsure if they **suffered a cyber attack** in the last 12 months



of mid-sized businesses do not have **dedicated cybersecurity experts** in their organization



of mid-sized businesses do not currently have an **incident response plan**

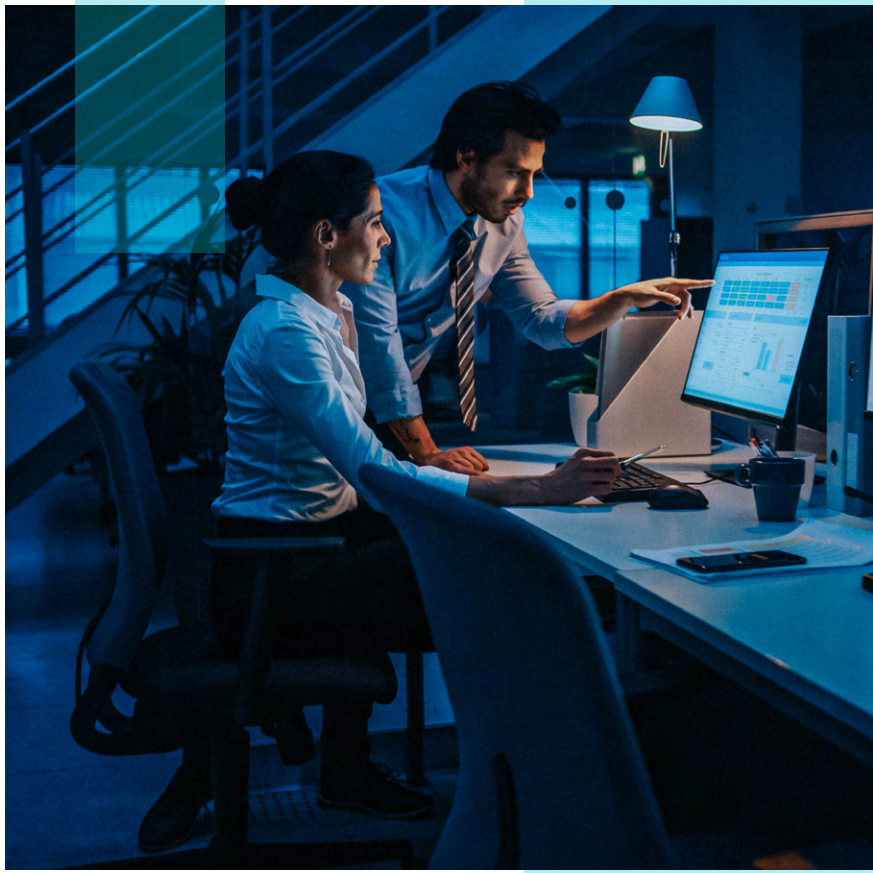


of mid-sized businesses reported having no **cyber insurance** coverage

Methodology

This research provides insights on the current state of cyber defense for this segment of the business market, including what steps organizations are taking to protect themselves against threat actors. Conducted by Virtual Intelligence Briefing (ViB) of Nashua, New Hampshire, the study was developed to gain insights into the organizational structure, resources and cybersecurity strategies used and required by mid-sized businesses. Mid-sized businesses are generally defined as companies with 250 to 2000 employees.

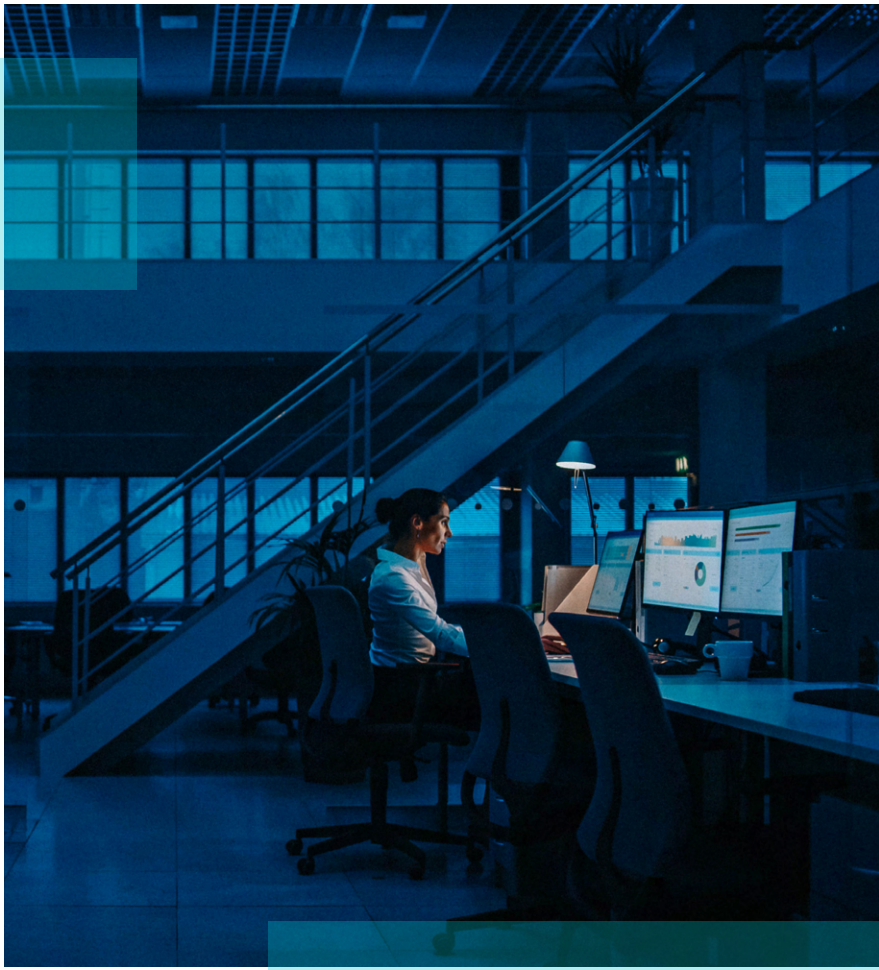
The research targeted private-sector businesses in the U.S. and Canada across all industry sectors. Respondents were IT professionals at the manager, director and c-level within these organizations. The survey was conducted over two weeks in January 2023, with 256 companies participating.



Introduction

Cybersecurity has become an increasingly critical concern for businesses of all sizes, however, there are significant vulnerabilities extant for those with less than 2000 employees.

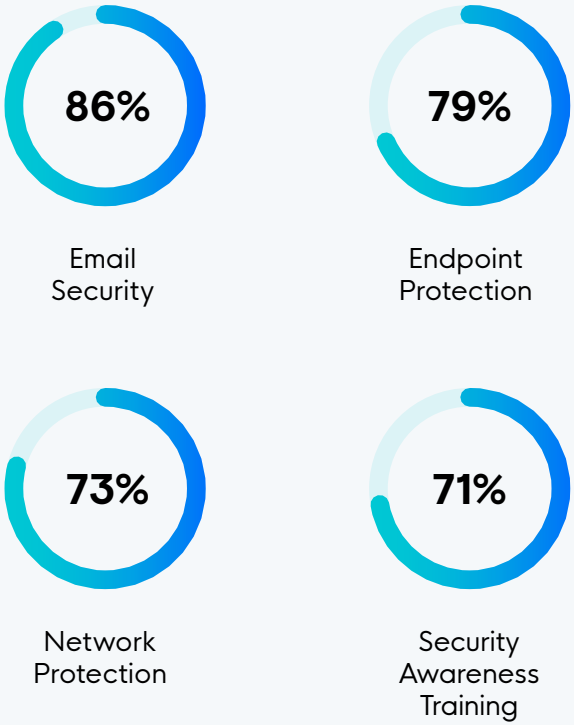
The research revealed that a significant number of these businesses feel either unprepared, understaffed and/or under-resourced for responding to evolving threats, and a significant number face challenges in securing cyber insurance coverage and proper security awareness training for their workforces. Survey responses also highlighted a wide range of cybersecurity issues and considerations, including how prepared mid-sized businesses are for today's threats, what security tools are being used and the obstacles they face in establishing a robust security posture.



Current Cybersecurity Solutions, Resources and Obstacles

The data shows that mid-sized businesses are aware of the need for multiple cybersecurity layers, which is driving the adoption of security tools and techniques. Notable gaps exist in their current tools and planning processes, and mid-sized businesses are also facing resource challenges when it comes to cybersecurity.

A majority of respondents reported deploying a wide range of solutions to counter threats, the most prevalent of which were **email security (86%), endpoint protection (79%), network protection (73%) and security awareness training (71%).**



Cybersecurity Solutions That Mid-Sized Organizations Currently Have

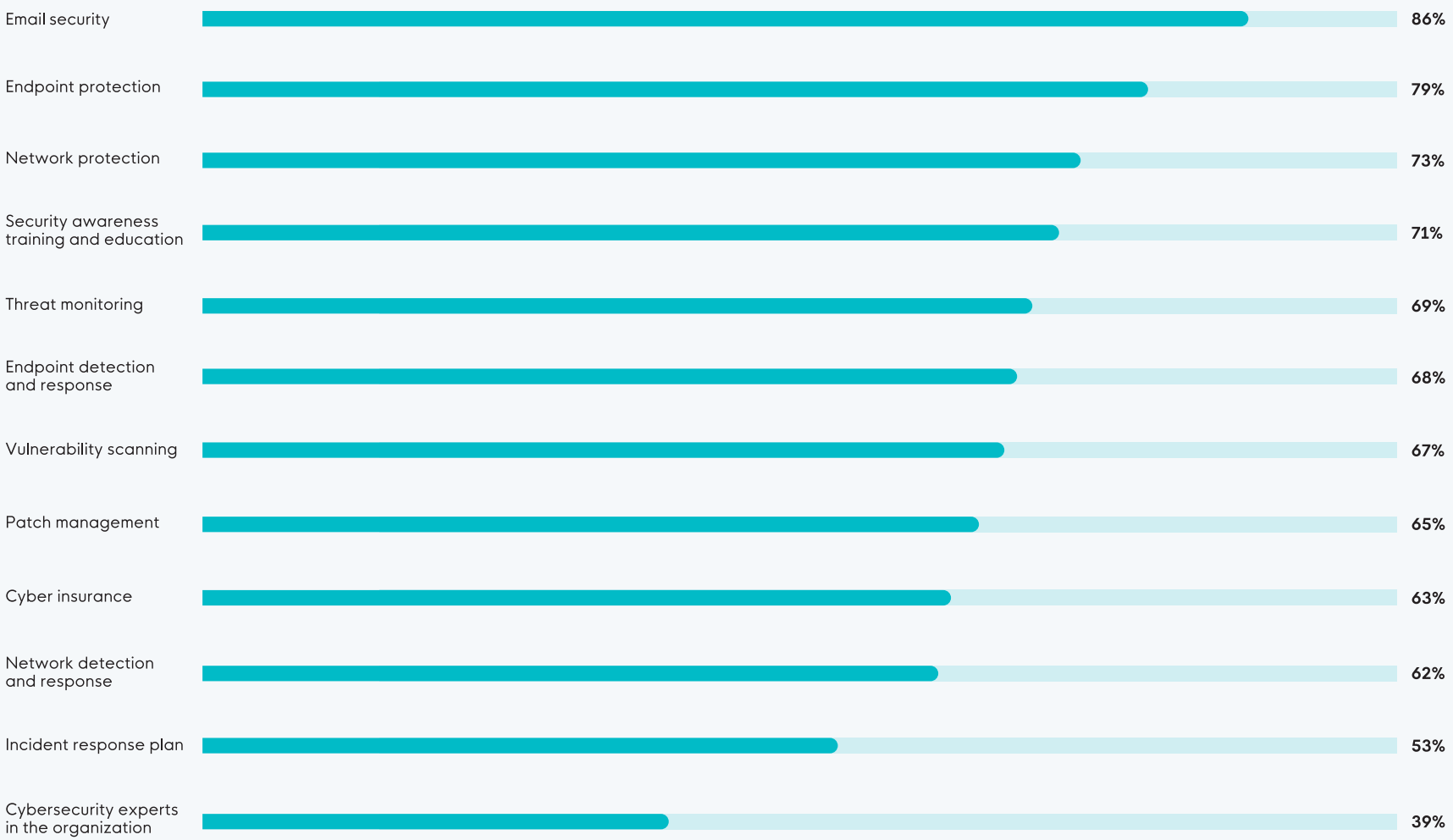


Figure 1: Analysis of the cybersecurity solutions that respondents' organizations currently have, not showing all answer options, asked to all respondents (Base: 276)

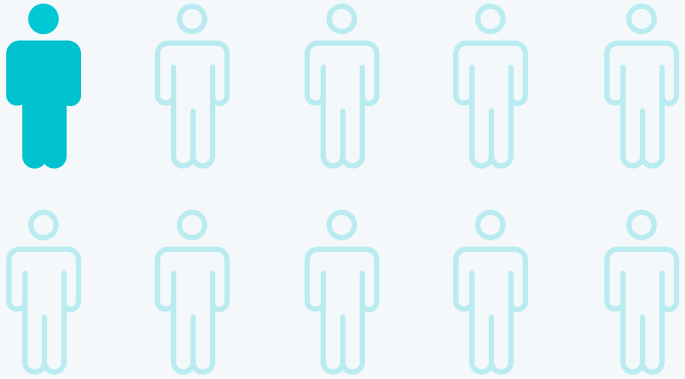
The research indicated high awareness and usage of security tools deployed by mid-sized organizations, a significant portion of respondents are not taking some of the most basic defensive measures available.

Almost one-third of respondents indicated they were not deploying threat monitoring, endpoint detection and response, vulnerability scanning, patch management or network detection and response. An alarming 47% of respondents reported their organization does not currently have an incident response plan.

61%

OF RESPONDENTS SAY THEY DO NOT HAVE DEDICATED CYBERSECURITY EXPERTS IN THEIR ORGANIZATION.

In the discussion of resources, respondents identified gaps in budgeting, staffing and skill sets as obstacles to deploying a robust security program. Many mid-sized businesses lack the necessary personnel and expertise to deal with the growing threat landscape. Based on respondent data, for every 10 employees in IT there is only 1 dedicated to cybersecurity. Additionally, 61% of respondents say they do not have dedicated cybersecurity experts in their organization.



Budget and resource constraints combined with a shortage of cybersecurity talent means that mid-sized businesses struggle to scale their cyber defenses and find the right employees with the necessary skills and expertise to effectively manage their cybersecurity posture—leaving them vulnerable to new threats. **Half (49%) of respondents claim they will spend more for cybersecurity in 2023, another 43% will maintain their current cybersecurity spending, and 7% will plan to spend less in the coming year.**

According to the FBI's Internet Crime Complaint Center, there were 847,376 complaints filed in 2021 representing an estimated $6.9 billion in losses. Research firm Gartner is predicting an 11.7% increase in risk management spending in 2023 to $79.5 billion.

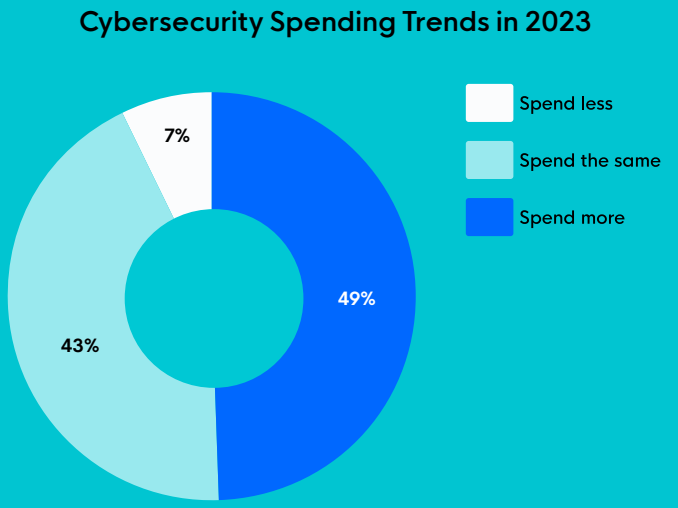


Figure 2: Analysis of how organizations expect cybersecurity spend to trend in 2023vs. 2022, asked to all respondents (Base: 274)

When budgeting for cybersecurity, many mid-sized businesses are approaching it proactively. 38% budget for cybersecurity based on business needs and priorities, 34% budget to address gaps in their security posture, and another 34% budget based on compliance requirements. However, some of this budgeting is still happening reactively—either on a case-by-case basis (24%), if a cyber attack happens in their industry (9%), or only if there's room left in their budget (9%).

In addition to changes in spending, mid-sized businesses are also turning to outside resources to help close critical gaps.

41%

OF RESPONDING ORGANIZATIONS' CYBERSECURITY IS OUTSOURCED OR MANAGED BY A THIRD-PARTY VENDOR, ON AVERAGE.

The most common factors driving these businesses to outsource their security needs include the lack of expertise, staff and resources. However, it is important to note that the risk associated with cyber attacks remains with the business itself.

Driving Factors for Cybersecurity Budget Decisions

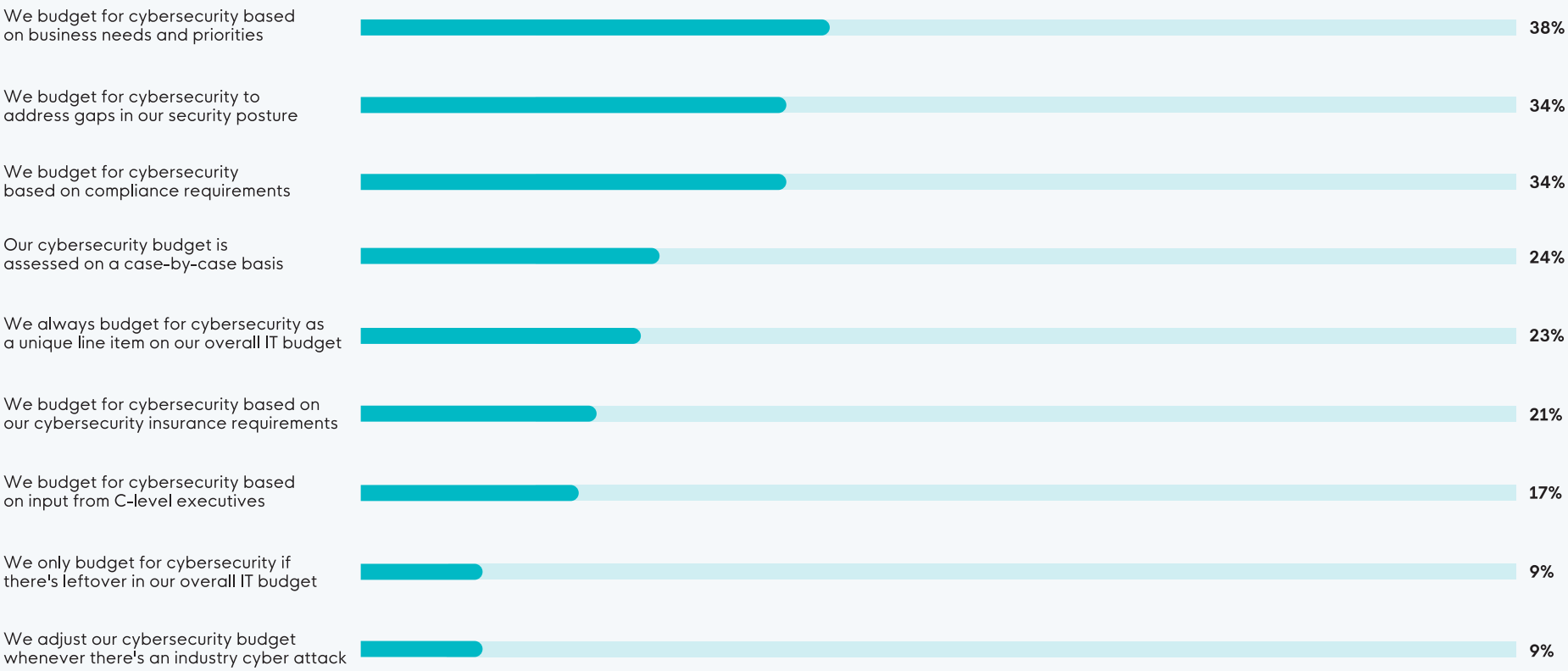


Figure 3: Analysis of the main factors that go into respondents' cybersecurity budget decisions, not showing all answer options, asked to all respondents (Base: 276)

Facing Today's Threat Landscape

Cybersecurity remains a top priority for a majority of mid-sized businesses; however, readiness to fend off today's threats is one of their most pressing challenges. The research highlights how a sizable portion of responding organizations is inadequately resourced to meet today's threat landscape—creating gaps that can be exploited by even the least sophisticated of hackers.

In self-assessing their resource vulnerabilities, respondents identified time (43%) and skills (34%) as gaps in properly dealing with security issues. And when it comes to deploying a robust security posture, the ability to detect advanced threats (34%), faster threat protection (32%) and budget (29%) are their top obstacles.

Internal Cybersecurity Challenges

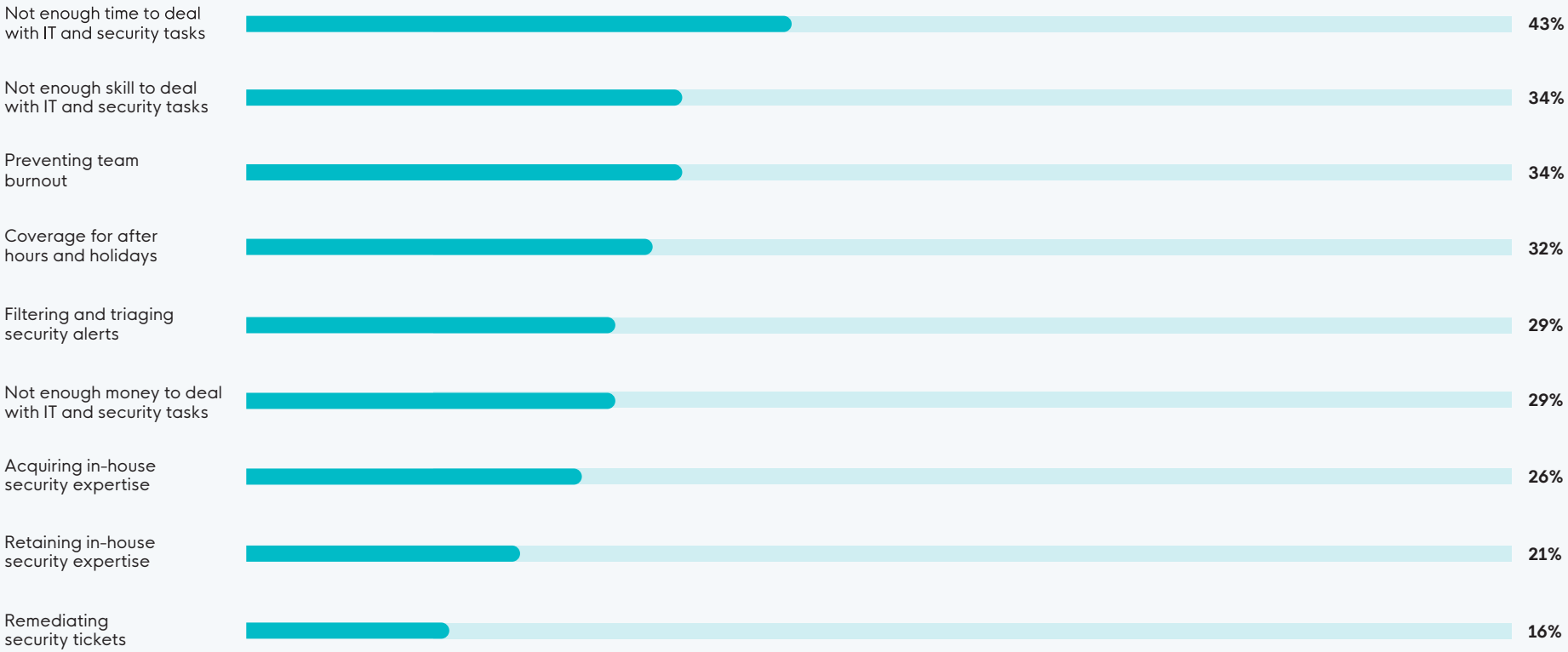


Figure 4: Analysis of the areas in which respondents' teams need the most help, not showing all answer options, asked to all respondents (Base: 276)

Cybersecurity Readiness Challenges

Figure 5: Analysis of the areas in which respondents' security posture needs the most help, not showing all answer options, asked to all respondents (Base: 276)

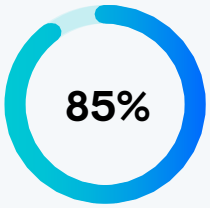
Due to these gaps in people, processes and technology, many mid-sized businesses are struggling to keep pace with the evolving security landscape. This leaves them vulnerable to potential attacks and hinders their ability to properly defend themselves when hackers eventually strike.

One-quarter of survey respondents reported either a form of cyber attack on their organization or did not know if their organization had been attacked in the past twelve months.

10%

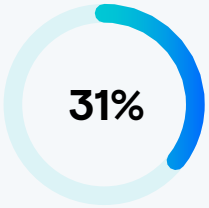
DID NOT KNOW IF THEIR ORGANIZATION HAD BEEN ATTACKED AT ALL.

For those reporting a cyber attack, the impacts were significant:

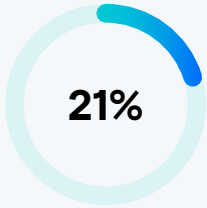


Reported a cost in time and resources

Reported a financial impact from the attack



Changed their security tools



Reported data losses

Employers Face Challenges in Security Awareness Training

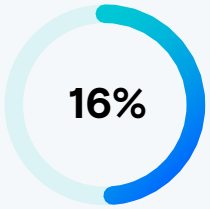
Training remains a challenge for a significant number of respondents. While 59% reported conducting regular formal security awareness training, only 9% say their employees adhere to security best practices, underscoring the complexity of implementing even the most basic of security protocols.

More alarming, more than 40% of respondents do not conduct regular formal security awareness training, exposing their organizations to higher cyber risk.

16% reported doing occasional ad hoc training and 15% reported having no training at all. 9% of respondents indicated they only raise awareness when a security incident occurs in real time.

Employees are the front line of defense in an organization's cybersecurity posture. Mid-sized businesses have an opportunity to introduce formalized cybersecurity awareness training to reduce their risk. Educating their employees about how to recognize threats and avoid them is a critical element of any robust cybersecurity program.

of respondents do not conduct regular formal **security awareness training**



reported doing occasional **ad hoc training**

of respondents indicated they only raise awareness when a **security incident** occurs in real time

Cyber Insurance Challenges

Carrying cyber insurance coverage was a key issue for respondents. While 69% of respondents are required to carry some form of cyber insurance, 35% find it extremely difficult to obtain coverage.

27%

HAVE NO INSURANCE COVERAGE AT ALL.

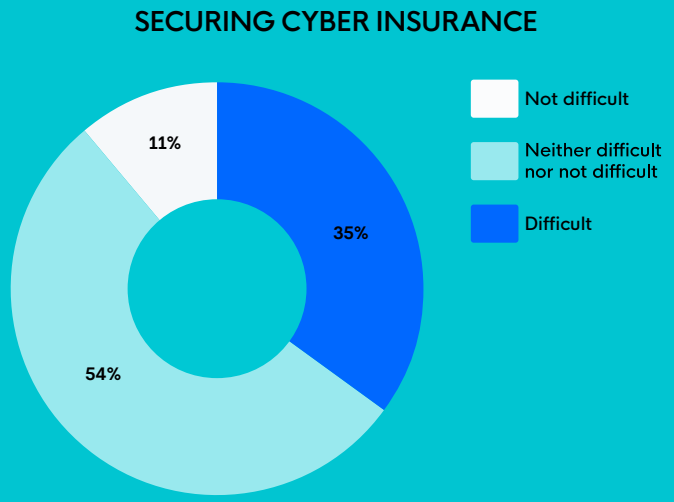
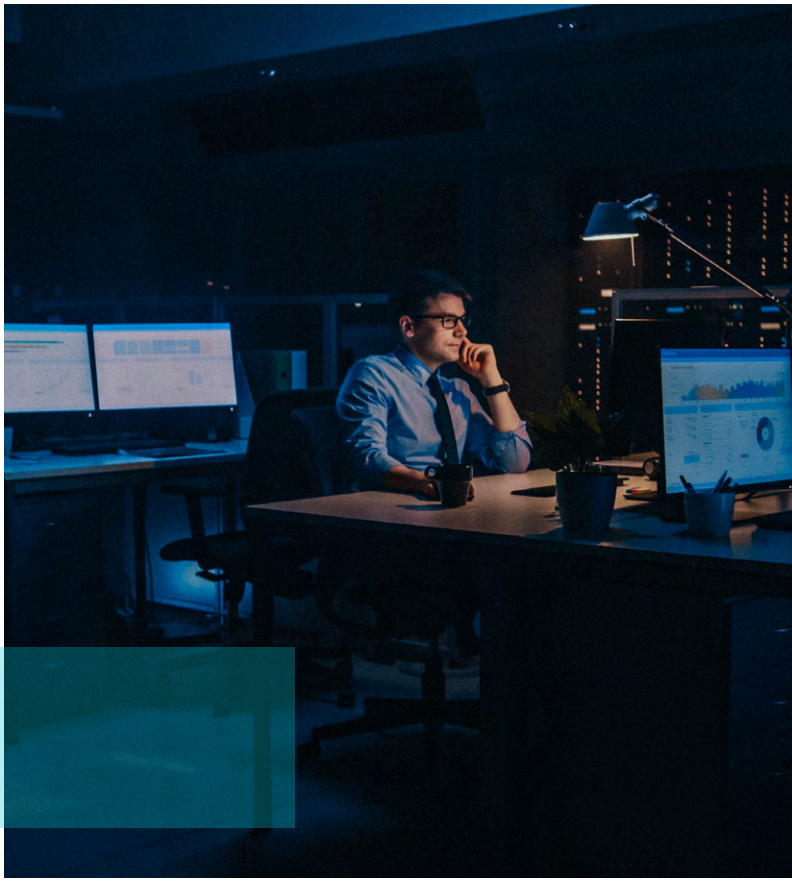


Figure 6: Analysis of how organizations rank the difficulty of securing cyber insurance, asked to respondents whose organization currently carries a cyber insurance policy (Base: 188)

Conclusion

This data confirms in stark terms that the businesses that drive most innovation, economic and employment activity in the U.S. and Canada are also at the most risk from cyber attacks. SMBs and their IT vendors have made decent strides in shoring up their cyber defenses in recent years, however huge gaps of vulnerability remain, posing significant economic and operational risks to themselves and the broader economy. In many cases, these companies are not aware that the same resources larger business enterprises access for protection are available to them at a scale and value that fits their company size.



About Huntress

Huntress is the managed security platform for the 99%—the small and mid-sized businesses that drive the economy. Founded by former National Security Agency (NSA) cyber operators, Huntress offers a powerful suite of managed endpoint detection and response (Managed EDR) and security awareness training capabilities backed by a 24/7 team of dedicated threat 'hunters' who are on a mission to defend businesses from today's determined and persistent cyber criminals.

VISIT WEBSITE

HUNTRESS