



KEEPER
Cybersecurity Starts Here®

2022

US Cybersecurity Census Report

Foreword

Cybersecurity is now recognized as a key priority for U.S. businesses. However, cybersecurity threats are evolving as risks, and the responses necessary to mitigate them, change rapidly. Staying a step ahead of bad actors is a continuous challenge and businesses—despite their intentions to do so—aren't always keeping pace.

To solve this problem, IT leaders must understand why. They need answers to questions such as, how is cybersecurity transforming? How are cyberattacks harming businesses? Where must investments in preventative training and tools be focused? Is cybersecurity being prioritized by leadership? And how does cybersecurity fit within organizational culture?

In partnership with Sapio Research, Keeper Security analyzed the behaviors and attitudes of 516 IT decision-makers in the U.S. to answer these questions and more. This report, Keeper's second annual U.S. Cybersecurity Census, maps the transforming landscape of cybersecurity based on these expert insights.

It provides leaders with a forensic assessment of the threats their businesses face, and details the urgent strategies necessary to overcome them.

Executive Summary

Four key takeaways from Keeper's second annual U.S. Cybersecurity Census



SECTION 1

Cyberattacks

Cyberattacks Present a Growing Threat

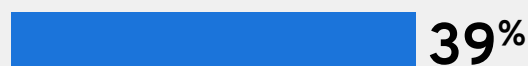
U.S. businesses face an onslaught of cyberattacks each year, with significant impact on their organizations.

The average U.S. business experiences 42 cyberattacks per year—between three and four each month. Over one-fifth (22%) are subjected to more than 251 attacks yearly, and 12% experience more than 500 attacks per year.

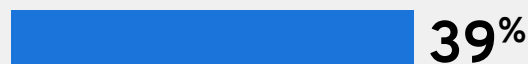
Of those, the average U.S. business faces about three successful cyberattacks each year. The overwhelming majority of respondents agree that the total number of attacks will increase over the next year, with 39% predicting that the number of successful cyberattacks will also increase.

How IT leaders expect the number of cyberattacks (successful and total) to change over the next 12 months

I expect both the total number of cyberattacks as well as the number of successful attacks to increase



I expect the total number of attacks to increase, but successful ones will not increase



I expect neither the total number, nor the number of successful cyberattacks to increase



I don't expect the total number of attacks to increase, but I do expect the number of successful attacks to increase



I don't know because we don't track how many cyberattacks we are experiencing



Most Organizations Say They're Prepared for Cyberattacks, but...

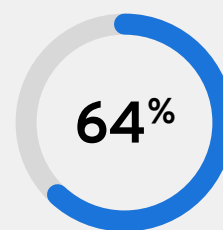
Most organizations in the U.S. feel they're prepared to fend off cyberattacks, with 64% of respondents rating their preparedness at least an 8 on a 10-point scale, with 28% rating themselves as a 10/10. Only 18% rated themselves at 5 or less. However, respondents weren't nearly as generous when grading other organizations' preparedness, with only 48% of respondents giving U.S. businesses in general at least an 8/10.

However, as discussed in the next subsection, the losses keep coming – and the time to address attacks is increasing. The majority of respondents (57%) say it is taking longer to respond to attacks, and only 8% say responses are getting faster.

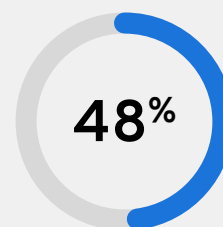
Darren Guccione, CEO and Co-Founder, Keeper Security

“This research demonstrates that cyberattacks present a profound threat. Preventative measures, in the form of investment, education, and cultural shifts, will be essential for businesses to drive resilience and protect their organizations from cybercriminals.”

How prepared to fend off
cyberattacks is your business?
How prepared do you think other U.S.
businesses are?



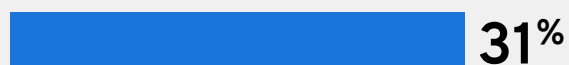
My business is prepared
(at least 8/10)



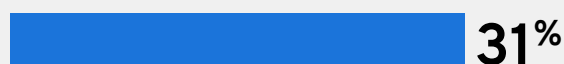
Other businesses are
prepared (at least 8/10)

Which of these has happened to your business as a result of a successful cyberattack?

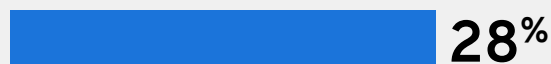
Disruption of partner/customer operations



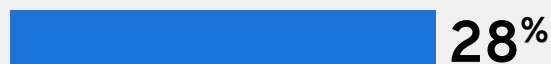
Theft of financial information (eg. bank details or payment card details)



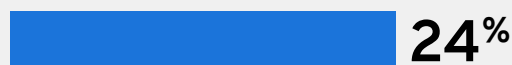
Reputational damage (eg. bad publicity/disgruntled customers)



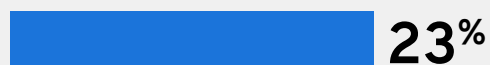
Theft of corporate information



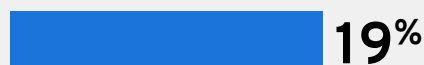
Disruption of supply chain



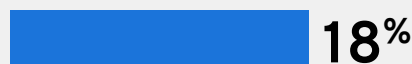
Disruption of trading/business operations



Loss of business or contract



Theft of money



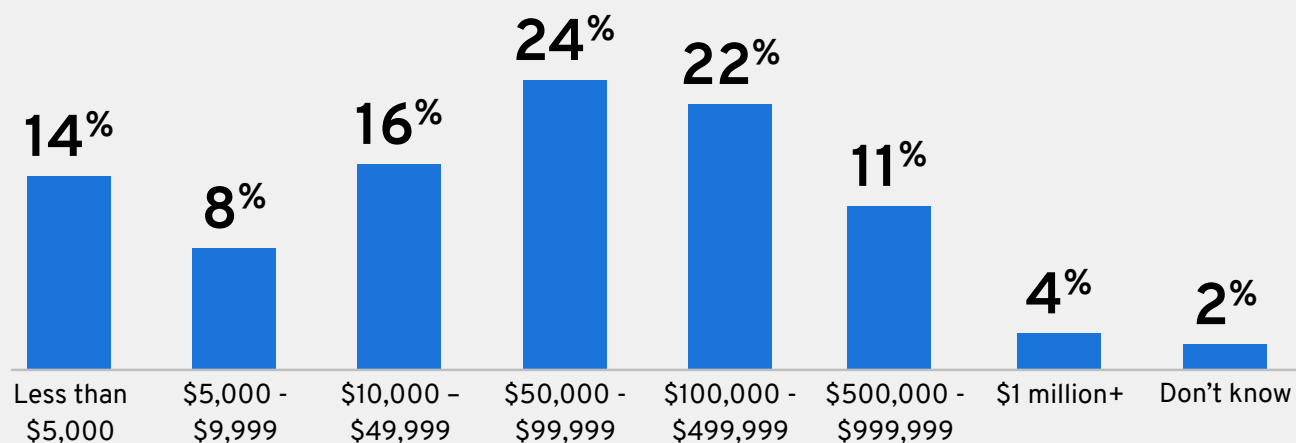
Cyberattacks are Causing Significant Harm to Businesses

Successful cyberattacks have the potential to seriously damage businesses. Nearly one-third (31%) suffered a disruption of partner/customer operations in the wake of a cyberattack, and the same percentage experienced theft of financial information, with 18% also experiencing theft of money.

The financial cost of cyberattacks is significant. Of those organizations that had money stolen as a result of a cyberattack, the average amount was more than \$75,000 – and 37% of organizations lost \$100,000 or more.



How much money was stolen if your business lost money in a cyberattack?



In addition to direct costs, cyberattacks can cause lasting damage to business perception, client trust, and the smooth running of future partnerships. More than one-quarter of respondents (28%) suffered reputational damage due to a successful cyberattack, and 19% reported losing business or a contract.

These direct and indirect financial losses can be catastrophic, particularly for small and medium-sized businesses (SMBs), which employ 46.8% of all employees in the United States. Most SMBs are cash-strapped; only 40% are profitable, and only half survive at least five years.¹

SECTION 2

Cybersecurity Investment and Tools

Shortfalls in cybersecurity investment are leaving businesses exposed to threats. Visibility of users, password strength, identities, and permissions are baseline necessities regardless of business size or sector—but they aren't being met.

Leaders Admit Their Tech Stacks Lack Essential Tools

Nearly one-third of respondents (32%) lack a management platform for IT secrets, such as API keys, database passwords and privileged credentials. A whopping 84% are concerned about the dangers of hard-coded credentials in source code – and 25% don't have software in place to remove them.

More than one-quarter of respondents (26%) said they lack a remote connection management solution to secure remote access to IT infrastructures. With 58% of American workers being able to work remotely at least one day each week, and 35% being able to do so five days per week², this is a major security gap. As today's data environments grow more complex, with more devices, networks, operating systems, and authentication methods, the security risks spiral. IT leaders are struggling to keep up with the rapid shifts in how the world works and the subsequent impact these shifts are having on their security.

26%

of respondents said their organization lacks a remote connection management solution to secure remote access to IT infrastructures.



Security Investment is Planned, but Immediate Action is Needed

As discussed in Section 1, most U.S. IT leaders feel that their organizations are prepared to fend off cyberattacks. However, their responses to other questions reveal very serious weak points in U.S. companies' security postures.

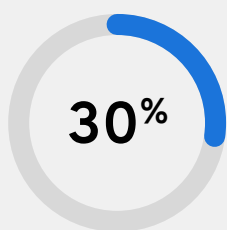
Passwords and credentials are a particular area that requires urgent investment. Fewer than half (44%) of respondents provide their employees with guidance and best practices governing passwords and access management.

Ensuring that all employees use strong, unique passwords for every account is a minimum best security practice. However, 30% of respondents allow employees to set and manage their own passwords – and admit that employees often share access to passwords. Meanwhile, only 26% have a highly sophisticated framework in place for visibility and control of identity security.

This laissez-faire approach to access management makes it clear that more must be done to keep organizations and their employees protected.

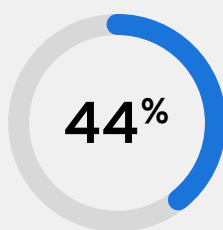
Despite these issues presenting a clear threat to businesses, fewer than half of respondents state they have plans to invest in password management, visibility tools for network-based threats, or infrastructure secrets management.

What is your organization's maturity with regards to visibility and control over identity security across on-premises and cloud systems?



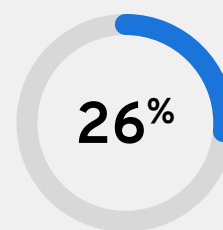
Low maturity

We leave it to employees to set their own passwords, and access is often shared



Average maturity

We provide guidance and best practices governing passwords and access management

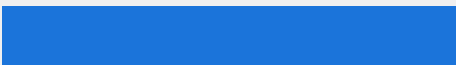


High maturity

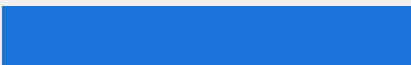
We offer a highly sophisticated framework to govern access to our system

Which of the following investments are you planning to make around cybersecurity within your organization over the next year?

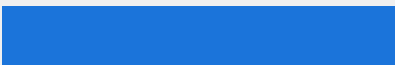
Employee security awareness training

**54%**

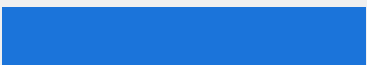
Creating a culture of compliance

**50%**

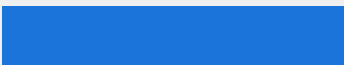
Password management

**48%**

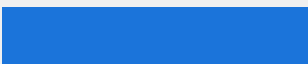
Greater control and visibility to help detect network-based threats

**44%**

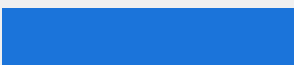
Infrastructure secrets management

**42%**

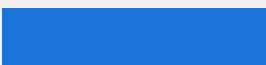
Passwordless authentication

**37%**

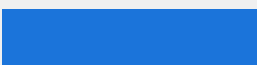
Establishing a stronger connection between access policy and access tools

**35%**

Adopting a zero-trust and zero-knowledge security approach

**32%**

Privileged access management to secure remote access sessions

**31%**

Cybersecurity is complex, with many moving parts and shifting priorities to manage, and this research shows that organizations could be doing more.

IT leaders are conscious that their defenses are limited and are voicing concerns as to where those weaknesses can be found. While many organizations are considering future investments, they face being outmatched by rising external threats and demands created by existing gaps.

Analyzing how cybersecurity ranks in terms of leadership priorities can help demonstrate the resources necessary to meet those changing demands.



SECTION 3

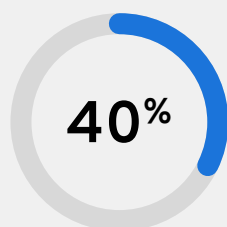
Cybersecurity Leadership

Protecting businesses from cyberattacks in the face of growing threats is no small task. IT leaders are under immense pressure from stakeholders, particularly as cybersecurity concerns compete with wider digital transformation and hybrid working priorities.

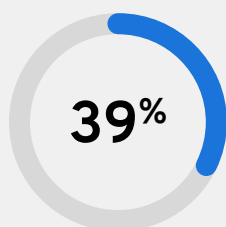
Cybersecurity is a Key Concern for the C-suite

As more employees work remotely, businesses must rethink their investments to maintain security. In fact, 40% of respondents highlighted remote and hybrid work as a top concern, with rising external threats close behind (39%).

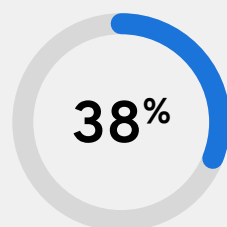
What are the top 3 concerns for you and your organization when it comes to cybersecurity?



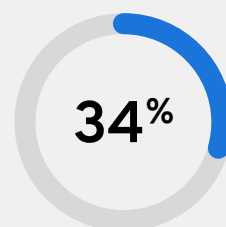
Remote and hybrid work



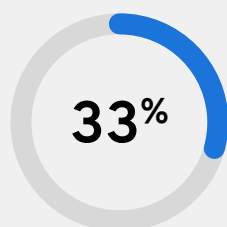
Rising external threats



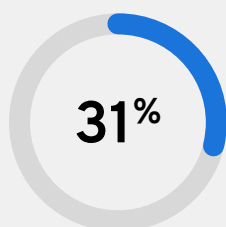
Contractors, interns and unsophisticated users



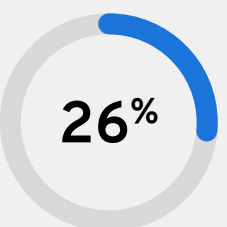
Digital transformation



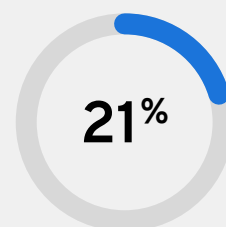
Password hygiene



Breach of secrets, such as API keys



Lack of training/skills shortage among staff



Lack of investment

On a positive note, lack of investment was the least common concern (21%), which is consistent with the fact that 60% of respondents said their C-suite's commitment to cybersecurity was of significant importance. Only 3% said that cybersecurity is not important to senior leaders at their organization.

However, 37% of respondents stated that their C-suite is either committed to only small investments as required or planning to make investments in the future. With cyberattacks rapidly increasing in frequency, sophistication and cost, organizations must invest in proactive security measures now, not at some undefined point in the future.

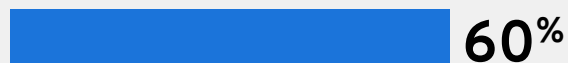
How Leadership is Shaping Cybersecurity within Organizations

U.S. business leaders are scrambling to source the necessary talent to keep their organizations secure. Nearly three-quarters (71%) of respondents have made new hires in cybersecurity over the past year, and 58% say they've increased cybersecurity training in that time.

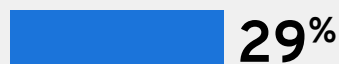
The lack of cybersecurity expertise available in the organizations surveyed reflects a broader skills shortage across the country—a key risk to the macro security of businesses.

What best describes the C-suite's commitment to your organization's overall security posture

It is of significant importance, and they dedicate resources to our security strategy



They are committed to making small investments as and when required



They acknowledge cybersecurity and plan to make some investments at some point in the future



Cybersecurity is not important to the C-suite

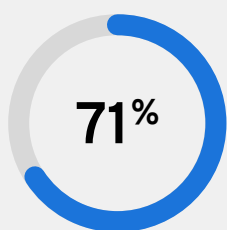


The U.S. cybersecurity skills gap

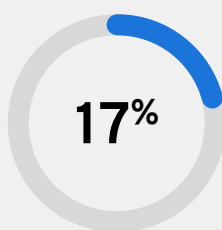
According to Cyberseek, there are only enough cybersecurity workers in the U.S. to fill 68% of the cybersecurity jobs that employers have open. On average, cybersecurity roles take 21% longer to fill than other IT jobs.³



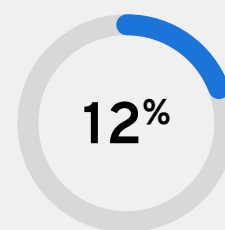
Have you made any new personnel appointments within your organization in the past 12 months to bolster your cybersecurity expertise?



Yes, we have made investments in the cybersecurity personnel within the organization



No, but we have plans to hire a cybersecurity specialist in the future



No, we have the right personnel in place already

Half of respondents (50%) have increased their spend on cybersecurity software. Just 8% state they haven't made any changes to their tech stacks in the past year—demonstrating a broad commitment across U.S. businesses to continue iterating and evolving their security tech stacks.

While incoming economic headwinds could present challenges to all businesses in the next year, 73% of respondents expect their cybersecurity budgets to increase.

However, as the following section explores, fiscal commitments are just one part of the cybersecurity picture. Cultural attitudes to cybersecurity present an emerging challenge.

Craig Lurey, CTO and Co-Founder, Keeper Security

“Cybersecurity is now firmly recognized as a foundational priority for senior business leaders. In the coming year, we need to see that positive sentiment translated into not only budgets, but a solid base of skills and solutions which will keep US companies secure in the face of ever-changing threats.”

SECTION 4

Cybersecurity in Company Culture

Lack of Transparency into Cyberattacks Could Fuel Culture of Mistrust

Despite budgetary commitments and a clear prioritization of cybersecurity from the C-suite, IT leaders themselves admit a concerning lack of transparency in cyber incident reporting within their organizations.

Nearly half of respondents (48%) admitted to being aware of a cyberattack but keeping it to themselves, suggesting they didn't report it to any relevant authority. This figure must act as a wake-up call to businesses and IT leaders alike.

Within a business, IT leaders must be able to share news of cyberattacks. If attacks aren't reported, businesses will fail to respond to them. The scale of threats becomes unclear, and ultimately the business becomes less secure. A shortfall in trust in the organization or fear of reprisal may be fueling this lack of transparency.



48%

of IT leaders have been aware of a cyberattack but kept it to themselves.

Meanwhile, the vast majority (79%) of IT professionals are concerned about a breach from within their organization, and 47% of those respondents have suffered a breach. This suggests that more must be done to educate teams and ensure everyone is following cybersecurity best practices.

Has your company ever experienced a breach from within your organization, and is it something that worries you?

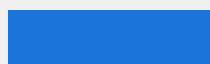
Yes, I have experienced a breach from within my organization, so it is something I am concerned about

**47%**

Yes, I am concerned about the threat of a breach occurring from within my organization, but I am yet to experience it

**32%**

No, I haven't experienced a breach from within my organization, and it's not something that I am concerned with

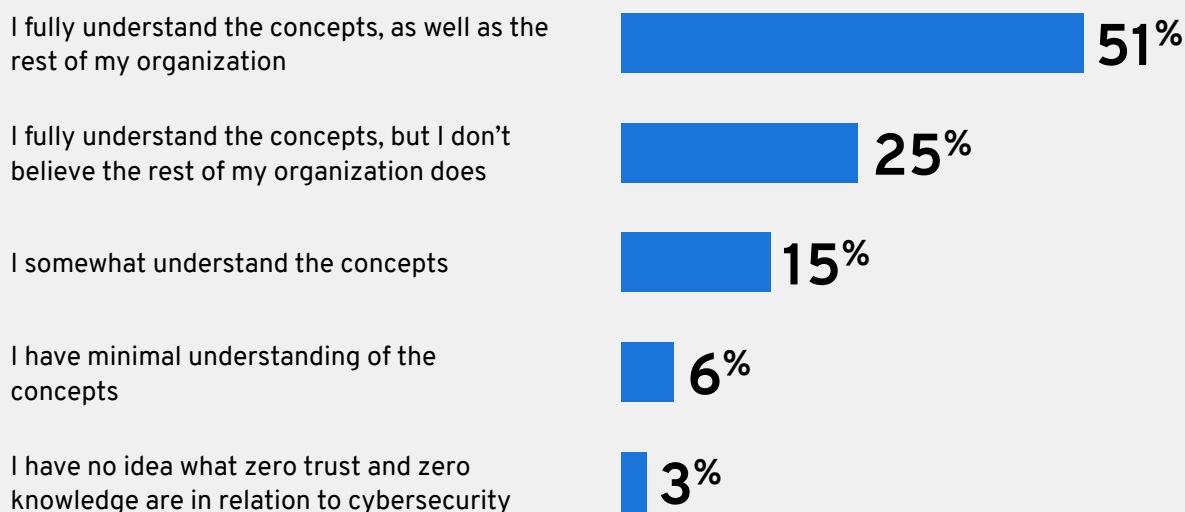
**21%**

More Robust Cybersecurity Education, Training and Planning are Needed

Despite the complexity of the cybersecurity landscape in terms of vendors and technologies, nearly 9 out of 10 respondents (89%) find it manageable or easy to build a cybersecurity roadmap. Just 11% find the process confusing or impossible.

However, while IT professionals themselves feel able to build roadmaps, there are clear gaps when it comes to understanding key concepts in security—both among IT teams and the wider business.

Do you understand the concept of zero trust and zero knowledge in relation to cybersecurity?



What are Zero trust and Zero knowledge in Cybersecurity?

- **Zero trust** assumes that all users and devices could potentially be compromised, and everyone, human or machine, must be verified before they can access a network.
- **Zero knowledge** is a security model that utilizes a unique client-side encryption and data segregation framework that helps support zero trust by protecting against data breaches.



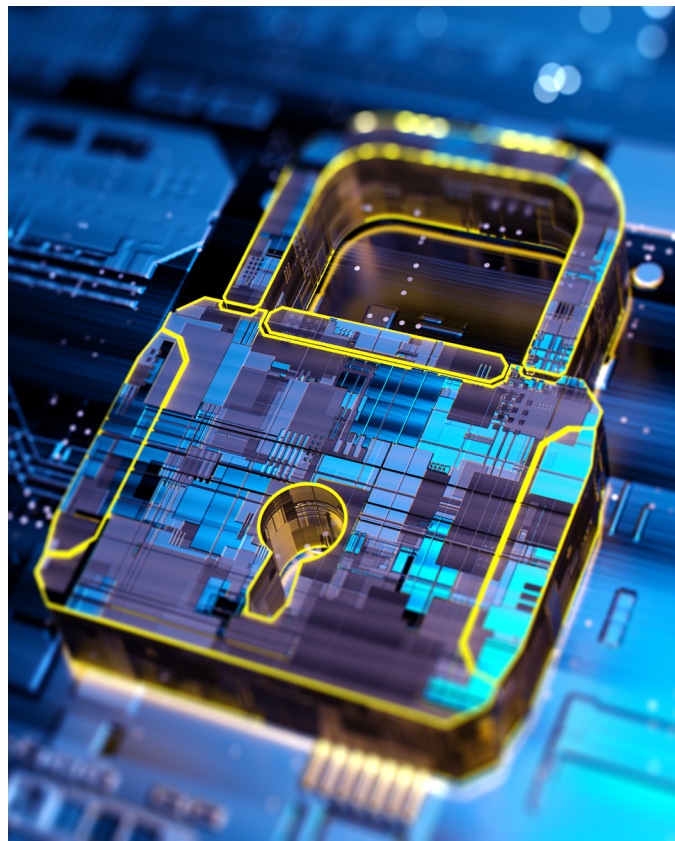
If the zero-trust tagline is “Trust no one,” the zero-knowledge tagline is, “We know nothing, and we can’t access your data.”

Organizations should also explore how they can use insight from third-party sources to build a robust cybersecurity culture. By far, respondents trust industry analysts, such as Gartner and Forrester, the most for cybersecurity guidance (59%).

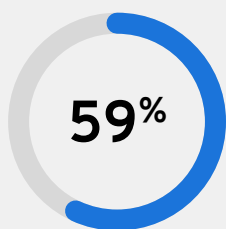
Tapping into that expertise and creating learning groups to delve into findings could be one way to start building cybersecurity into an organization’s culture.

As cybersecurity threats rise, IT leaders must lead by example.

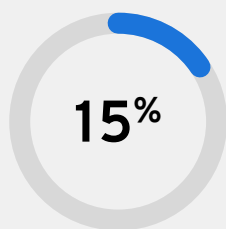
Being open with other leaders about attacks is a first step. An open dialogue on these issues is essential to recognizing the scale of the cybersecurity challenges organizations face. Only with that recognition can resources be devoted to education and truly embedding a cybersecurity mindset into an organization’s culture.



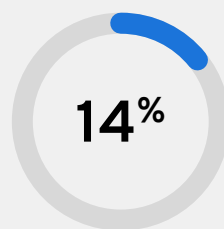
Who do you trust the most for cybersecurity guidance?



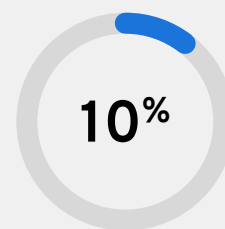
Industry analysts



Vendor white papers



Peer groups



Media

Conclusion

Businesses across the U.S. are making cybersecurity a priority. However, despite efforts and investments, clear gaps remain. Our research shows that there have been small steps, but no giant leaps.

The volume and pace at which threats are hitting businesses are increasing, and leadership can't afford to wait. If they do, the financial, reputational, and organizational penalties will be severe.

Likewise, as work has transformed dramatically over the past two years—with hybrid and remote working normalized—companies need to rethink how they are building cybersecurity resilience.

As we enter a new moment of economic uncertainty, we must not lose focus. The pace of cyberattacks is not going to decrease, even if the budgets to address them come under pressure. Preventative measures are always less costly in the long-run. It is essential that organizations deploy defensive solutions to protect against cyberattacks and their impacts.

Yet, for U.S. businesses to become truly secure, perhaps the biggest change that must be made is cultural. Nearly half of IT leaders admitted to keeping a cyberattack they were aware of to themselves (suggesting they did not report it to any relevant authority). This figure should shock business leaders. Without a culture of trust, accountability, and responsiveness, cybercriminals will thrive.

As we move forward, businesses and IT leaders need to not only voice commitments to cybersecurity, but also act on them. They need to acknowledge how our workplaces have evolved and respond to new ways of working with revised tech stacks.

Most importantly of all, they must make cybersecurity a part of organizational culture. Cybersecurity needs to be a pillar of every good business, but understanding, accountability, education, and progress must start at the top.

¹ Lawstarter Small Business Statistics & Trends 2022

² McKinsey American Opportunity Survey 2022

³ Cyberseek