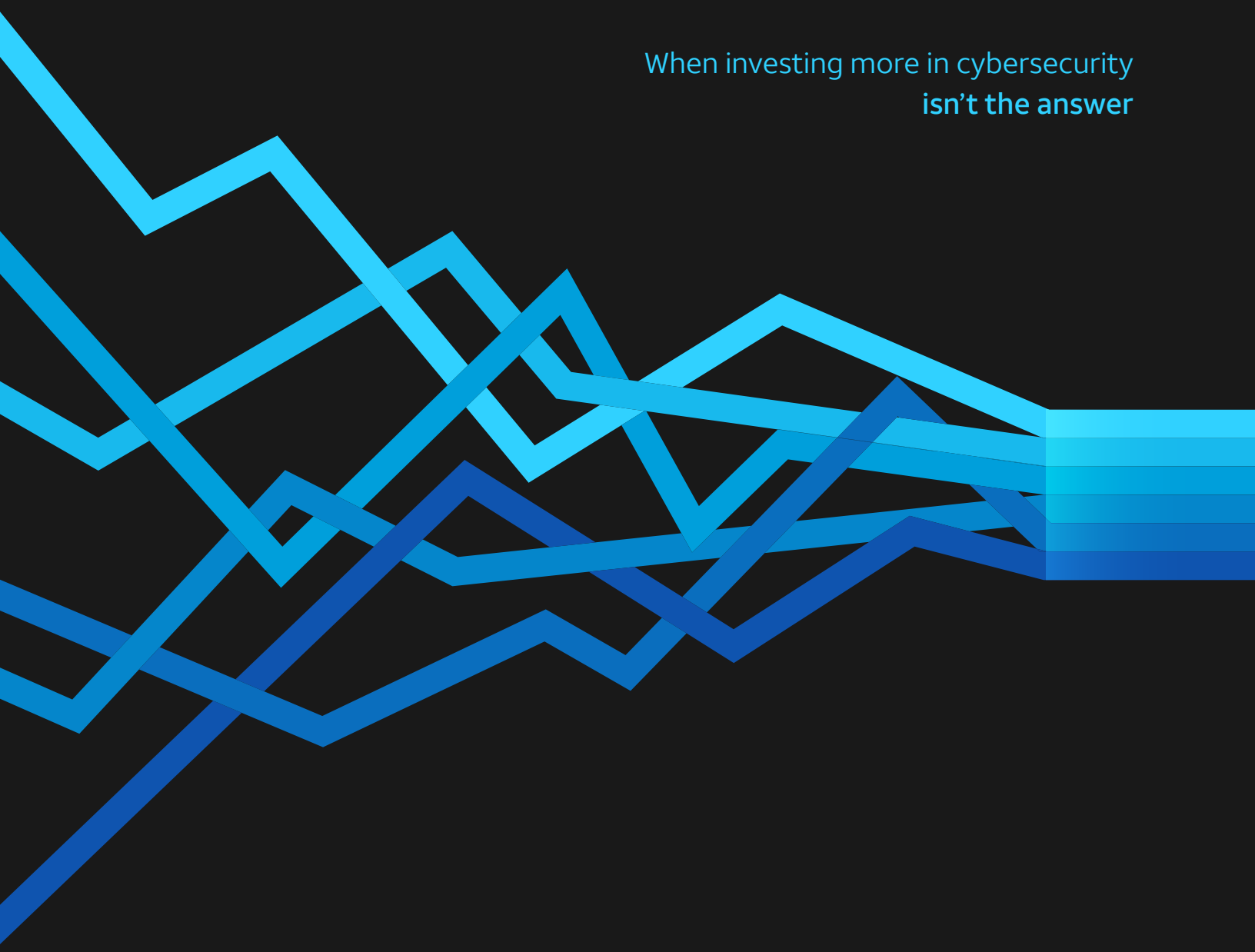
AT&T Business

Charting a new course

When investing more in cybersecurity **isn't the answer**



CYBERSECURITY INSIGHTS **VOL. 8**

Executive Summary

Are the organizations who are investing more in cybersecurity achieving better outcomes than those who aren't?

Our research suggests the answer is no. Rather, the key differentiator in achieving better cybersecurity performance is investing in a security strong risk management strategy.

In the summer of 2018, AT&T Business and Spiceworks performed a research study with 250 IT leaders. The research revealed that 99% of organizations have a security risk management strategy. However, there is a sharp performance divide between the organizations confident in their risk management strategies (*42% called the "Confident Investors"*) and organizations who are not (*57% called the "Unconfident Investors"*).[1]

Confident Investors are ahead on initiatives such as improving the customer experience (*25-point lead*) and boosting employee productivity (*16-point lead*). The reason, we conclude, is that Unconfident Investors place excessive focus on cybersecurity, which can drain resources needed for critical digital transformation projects. However, by turning to a managed security provider or a unified threat manager to tackle the everyday tasks of cybersecurity, organizations can be more strategic about cybersecurity risk management—as well as the future overall.

This report was written to help IT professionals chart a new course for their organizations by:

1. Aligning the organization around a security risk management strategy focused on business risk— and keeping it up to date.
2. Finding synergies that free up IT resources for larger digital transformation initiatives.

The report is the latest in our **ongoing cybersecurity insights series**, devoted to helping organizations protect against ever-changing security threats. This time, we've talked to IT professionals in small/mid-market organizations, along with AT&T cybersecurity experts, about best practices for protecting your operations from edge to edge, from the keyboard to the cloud.

"It's not about the number of dollars an organization spends that leads to them reducing risk. It's whether you have approached this from a business perspective and you have a risk management program that will not go stale."

—Todd Waskelis,
AVP with AT&T Cybersecurity Solutions

The security landscape:

Perceived risks and current practices

When AT&T Business and Spiceworks talked to 250 IT pros in the summer of 2018, the research revealed two categories of respondents—those who are confident in their cybersecurity risk management strategies (42%) and those who are not (57%). We then asked both groups about the business goals or outcomes, if any, they had fulfilled or experienced by having a formal risk management strategy in place.

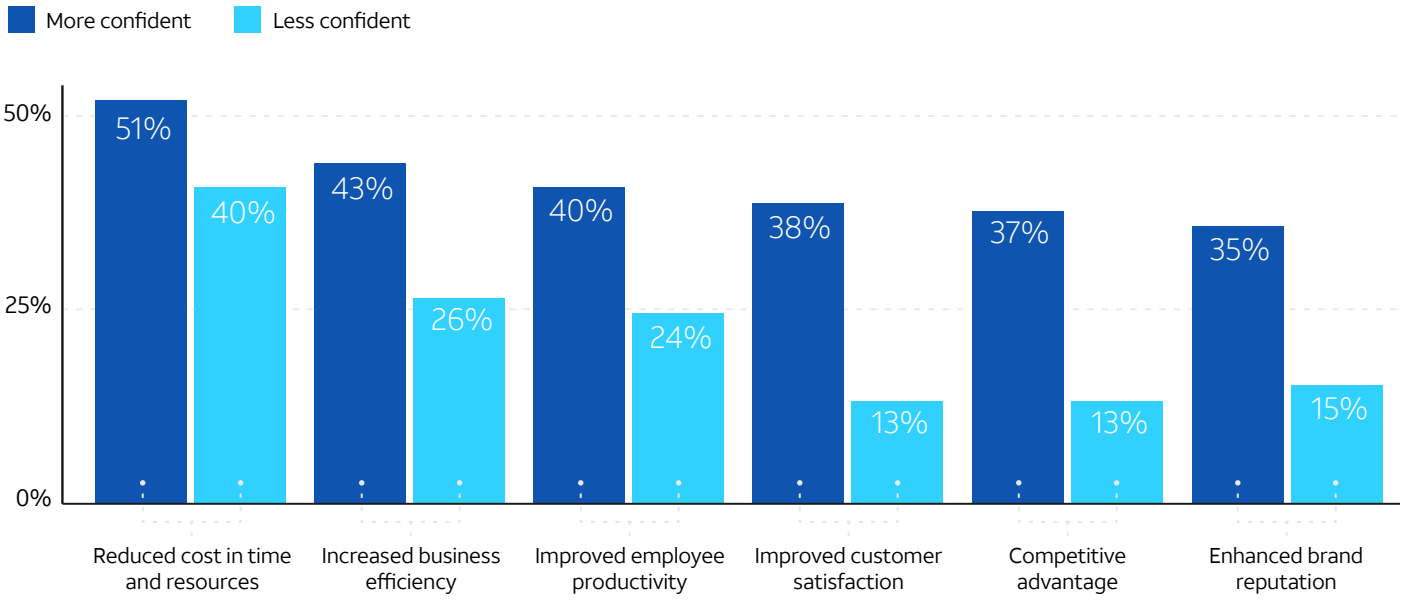
Here's what we found: organizations with a formal security risk management strategy not only experienced cost and time savings, increased business efficiency, and improved customer satisfaction—but all those outcomes were significantly higher for organizations with more confidence in their strategy.[1]

In fact, the need for a structured approach to the identification and management of risk has never been greater than in today's always-on, constantly communicating, cyber enabled business environment. With a realistic and disciplined assessment of worst-case scenarios, organizations can prioritize their investments for defending against cyber attacks.

"It's important to have a cybersecurity framework in place—with effective governance and reporting to make sure that you're following it"

— Danessa Lambdin, AT&T VP of Cybersecurity Solutions

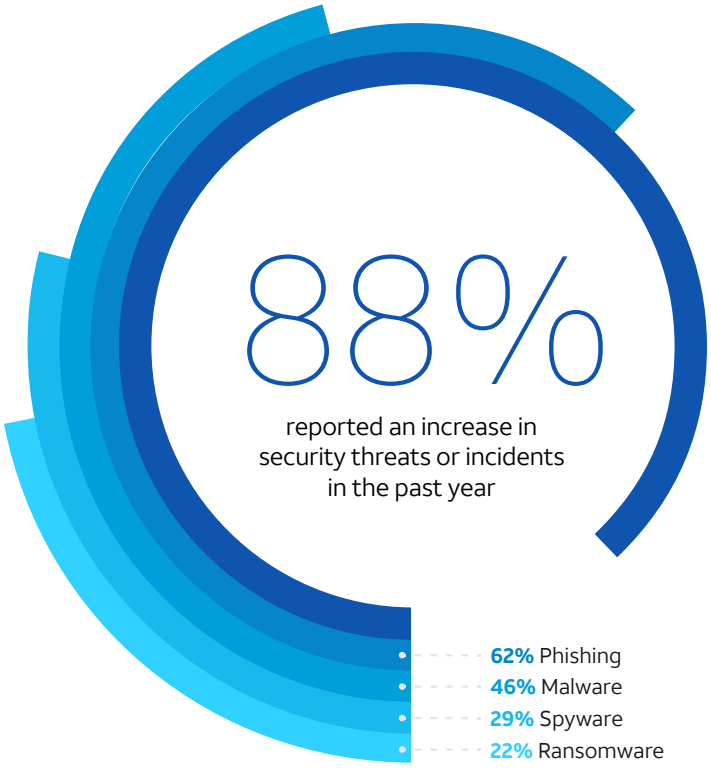
How confidence in your security risk management strategy ties to business outcomes:



Why is a security framework so important? Most organizations are getting attacked.

Eighty-eight percent of survey respondents reported experiencing at least one type of security incident or breach in the past year, with phishing attacks and malware being the most common.[1]

Organizations are taking a multi-layered approach to cybersecurity. And yet, only 38% of organizations say they feel completely or very safe from security threats or breaches.[1]

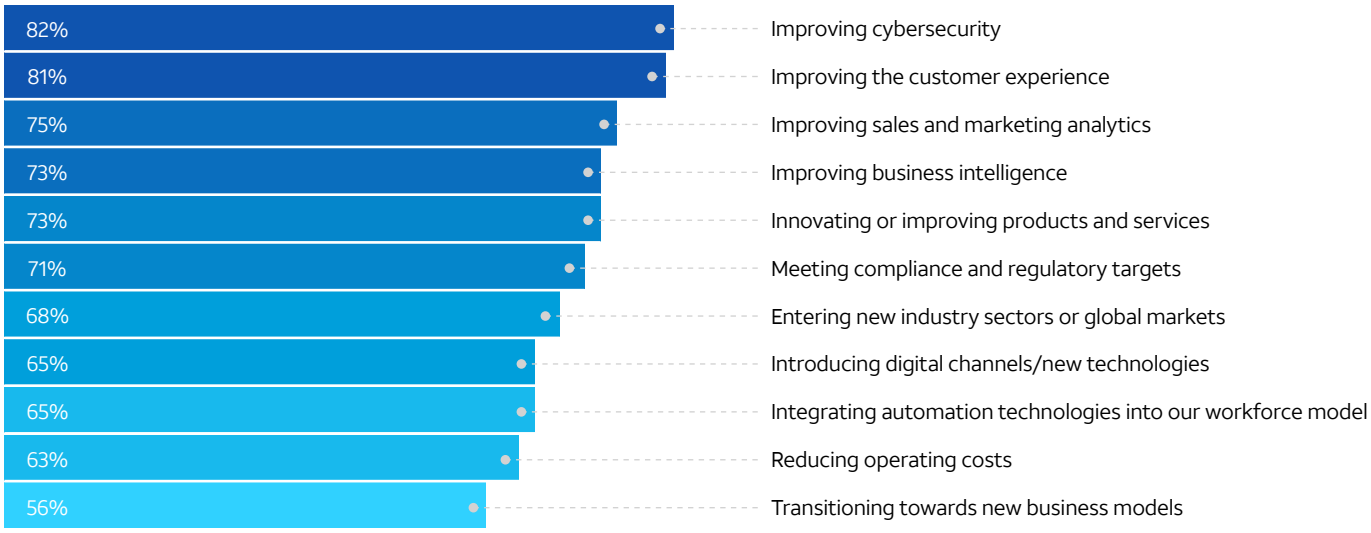


One of the main issues?

Our research shows that although cybersecurity was the top technology priority for the past year, organizations see it as the most underperforming IT area.

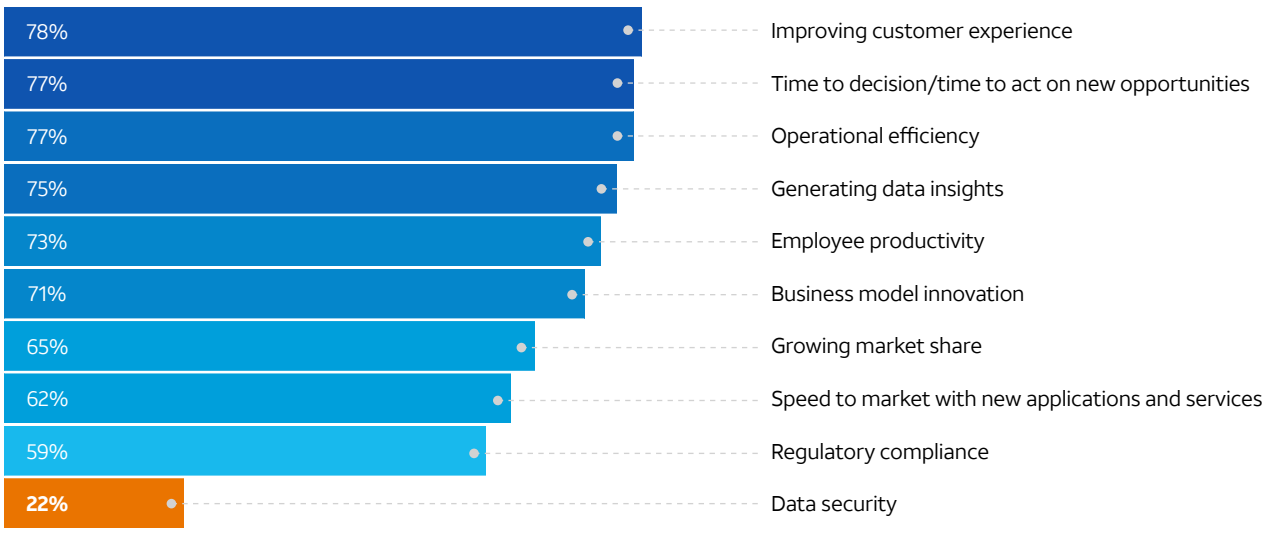
In fact, there's a disconnect in how security investments are viewed by top executives, compared to IT/security teams actually implementing them. [2]

Business leaders think their investments in technology infrastructure will deliver the performance needed to achieve strategic priorities



And yet, the same research shows that improvements in data security are lagging behind other business areas.[2]

Areas where performance over the past 12 months has improved significantly



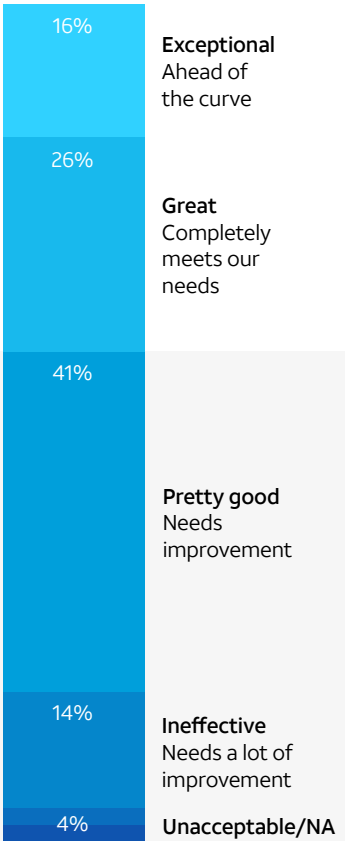
The outlook on security risk management strategies

Just 42% of organizations rate their strategy as exceptional (ahead of the curve) or great (completely meeting their needs).[1] This means 58% say their security risk management strategy needs improvement, a sentiment that is particularly prevalent among organizations that procure and deploy security solutions using only their own in-house teams.

"Enterprises probably spent a ton of money on technology because they were sold on the idea that they needed the 'next silver bullet,'" Waskelis says. "Instead, they should step back and say, 'Well, maybe I don't need all of that technology over here because my risk is really over there; I can limit how much I spend and mitigate my risk better by moving those controls around.'"

Organizations can invest as much in cybersecurity as they want, but if they don't understand where to best direct their investments, they will likely be wasting money, points out Bindu Sundaresan, Strategic Solutions Practice Lead with AT&T Cybersecurity Solutions. "An average organization tends to get around 50 to 60 security point products, and these tools don't work with each other. You don't get the full bang for your buck in terms of your investment."

> "Even when all seems well, and the network seems secure, there's the creeping fear: 'What am I missing? And what's it going to cost me in the end?'"
>
> *— Director of Technology Services, Financial Firm*



58%

say their security risk management strategy needs improvement

Old-school thinking can't defend against new attacks

Many organizations are still applying old security strategies and solutions to new security problems.

Anti-virus, anti-malware, and anti-spam software are the most popularly deployed tools.[1] However, deployment of advanced solutions is not widespread.

In interviews with IT professionals across various industries, we found that many organizations tend to react to security issues—rather than being ahead of the curve.

Explore their sentiments here:

Finance

Visibility can be a constant concern.

"There's always the fear of the unknown. Just because we've done a good job in the past, that doesn't mean something won't change and catch us off guard."
—Director of Technology Services, Financial Firm

Energy

Security can fall on the back burner for small teams.

"It's a 24/7 job, and there's only so many hours in the day… Our biggest challenge is trying to stay current with what we're protecting against or warning people about."
—Senior IT Systems Administrator, Energy Company

Manufacturing

Often, end users are on the frontlines to tell IT teams when something is wrong.

"I don't really have an automated way to see everything on the network to see if there are any anomalies."
—IT Director, Manufacturing Company

Healthcare

A security strategy can help with every decision.

"The most important thing we need to do for 2019 is to adopt a cybersecurity framework."
—Network Director, Healthcare Organization

The many challenges of threat detection and response

One of the biggest mistakes organizations make, Waskelis says, is not making security a risk management discussion. "They can list the security controls they have in place, but they can't really tell you what value those security controls are giving them in terms of overall risk mitigation. It is also very difficult for them to tell you how each control aligns to protect their critical data as it moves through the organization."

As shared in our **previous cybersecurity insights report**, "The underlying IT services strategy and framework need to evolve as you chart your course toward next-generation transformation, whether it be virtualization, cloud, or SDN (software-defined networking)," says AT&T VP Lambdin. "One of the big challenges we always see is a business attempts to do some planning up front, but their technology planning framework rarely gets updated. That framework must be part of the tapestry and evolve with the organization as the network topology changes to stay aligned with the goals of the company."

In fact, our research shows that many organizations treat their security risk management strategy as a "checkbox item," but don't really enforce it. Many have deployed a compliance initiative that includes some degree of risk management—but they never intend for it to drive any meaningful decisions.

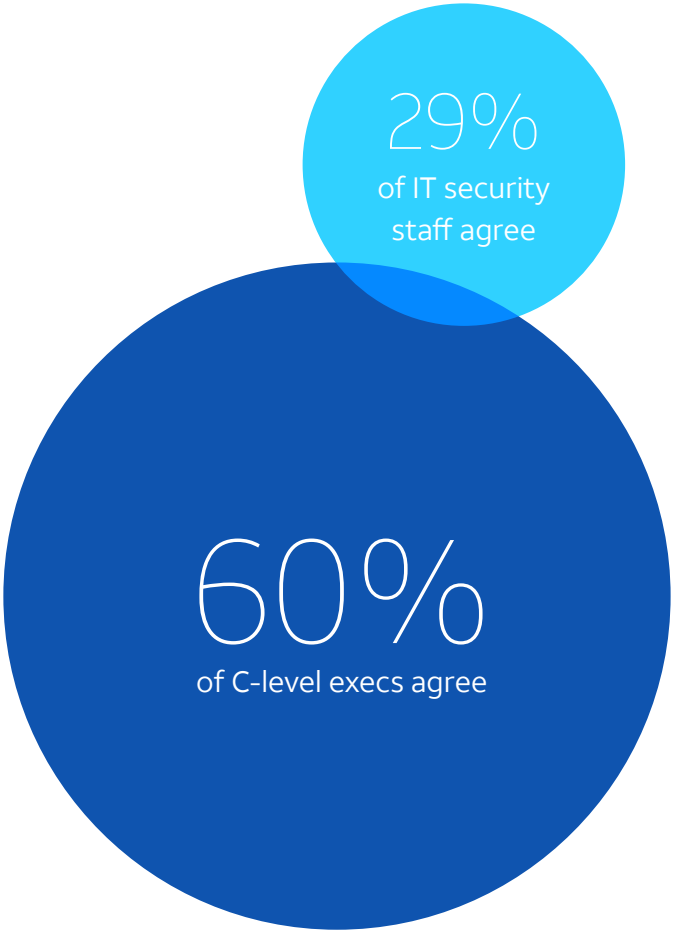
> "It's hard to get to the point where you're more progressive… I can play whack-a-mole all day long—block certain URLs and blacklist things—but that's reactive, not proactive."
>
> *— IT Director, Manufacturing Company*

Other challenges organizations see as they try to implement better security solutions and practices include: end-user resistance, inadequate budget for security, and a lack of true appreciation for the problem from C-level executives. In fact, 60% of C-level executives felt the security solutions already in place are keeping them completely or very safe—compared to 29% of IT security staff. Further, just 53% of IT decision-makers felt business leaders understand the importance of security in all aspects of the business—and for those organizations with in-house-only security management, it was just 39%.[1]

We heard from IT professionals that they have to work hard to convince C-level executives that threats are real.

"There's a big disconnect between me as a technology person and the board as business people," says the director of technology services for a bank. "It's my responsibility to help them understand the risks, and then they reluctantly spend money on cybersecurity."

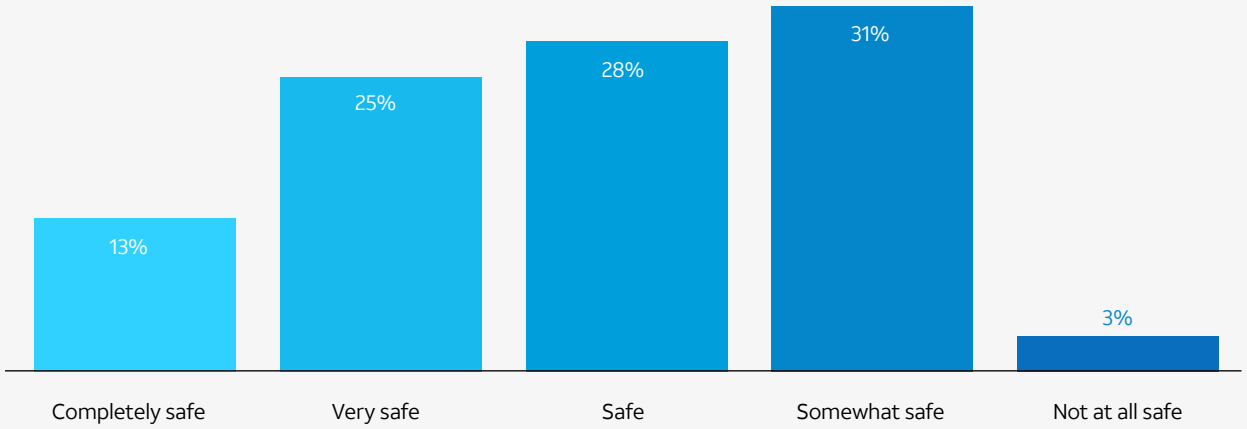
As Chuck Brooks, Adjunct Professor of the Graduate Applied Intelligence Program (Risk Management) at Georgetown University puts it, "As an advisor to the C-suite, you basically have to communicate how these threats impact profit and loss. Because now, you're dealing with the whole image of the company… and how emerging threats can impact their operations."



"Our current solutions keep us completely or very safe"

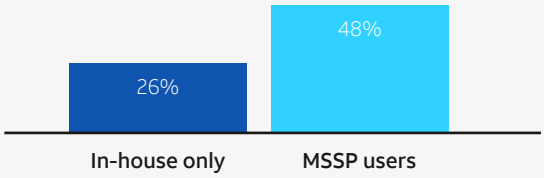
Explore the following graphics to see how perceptions on cybersecurity vary by organization size, job, and whether an organization is using a managed security services provider (MSSP) or going it alone.

How safe do organizations feel overall?



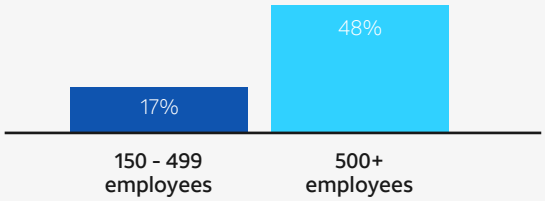
Security risk management approach

Completely/very safe



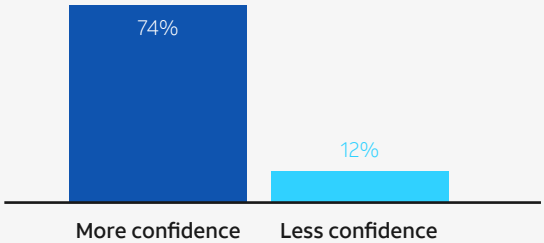
Company size

Completely/very safe



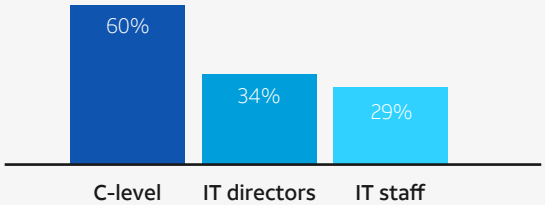
Security risk management strategy

Completely/very safe



Job role

Completely/very safe



MSSPs in the current landscape

Some organizations —typically those with deeper pockets and a cybersecurity strategy that has been embedded over a longer timeframe—are plotting a successful course by allocating their investments in technologies in a more balanced way. It's an approach that smaller organizations can also benefit from; it would help them consistently and intelligently invest in a diverse array of technologies, so they can be both better protected and well-positioned to maximize growth opportunities.

That's where managed security solutions can really help. Nearly half (49%) of organizations that partner with an MSSP rank their security risk management strategy as exceptional or great, and 48% feel safe from threats or breaches.[1]

Together, the organization and the MSSP can create a cost-efficient and centralized security strategy that supports and scales business operations—instead of hindering them. This approach also enables the business to focus on new technologies and innovation while the MSSP manages the ongoing cybersecurity strategy.

> "Top MSSPs can provide improved threat intelligence with highly specialized skills, helping organizations bridge the skills shortage... They also help remove the pressure from your IT/ security teams, freeing them up to focus on core operations."
>
> *—Bindu Sundaresan, Strategic Solutions Practice Lead with AT&T Cybersecurity Solutions*

Edge-to-edge security:

Protecting against vulnerabilities, from the keyboard to the cloud

Effective security requires proper controls to be incorporated into every aspect of the network. That can be problematic, however, if the controls don't work on all endpoints, such as IoT devices. So, edge-to-edge security needs to be deployed one step earlier, in the network design itself.

"The harsh reality is that no number of security systems can stop an attack; they can only reduce the risk. The severity of an attack is therefore determined by how quickly a company can detect and respond to threats as they occur."

— Barmak Meftah,
President of AT&T Cybersecurity Solutions and CEO of AlienVault

"It's important for security to be baked into that network design initially, from the ground up," Waskelis says. "As networks evolve, the goal is to virtualize security functions and make them on demand and scalable across networks. You're going to find that a lot of endpoints, especially IoT devices, don't even support typical security functions. So, it has to be done in the network. It can be done faster and much more cost-effectively on the network, instead of going out and buying box after box and stacking them in your data center."

Advanced security solutions, such as virtual firewalls, are a way to extend the value of security investments. They are designed to adapt to future needs. "So will we see a greater degree of virtualization? Absolutely," explains Josh Goodell, AT&T VP of Edge Solutions. "Is it possible to completely address all the security issues and all the security concerns with virtualized security today? Absolutely not." After all, network security is a critical piece of the puzzle, but it's still only one component of a complete risk management strategy.

The value of vulnerability management

How do you know if security controls are leaving some endpoints vulnerable? You can find out through a well-executed vulnerability threat management program, the bedrock of a strong security risk management strategy. In fact, we found that organizations that prioritize vulnerability management feel more confident about their security posture.[1]

The top factors that contribute to endpoint vulnerability include:

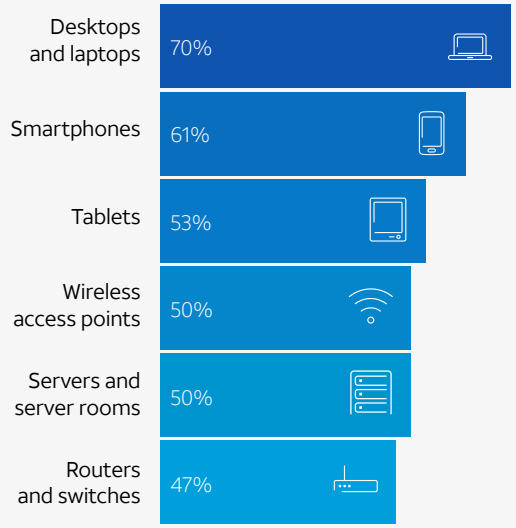
1. End-user practices
2. Lack of security patches to protect all endpoints
3. Inability to protect all endpoints
4. Inability to effectively identify vulnerabilities

"In my opinion, users are the weakest link," says the IT director for a mid-sized manufacturing company. "I see this over and over again. The spam, the phishing schemes, they get more intelligent and better every day. People are busy… and not thinking about security. They're just doing their job and trying to get things done."

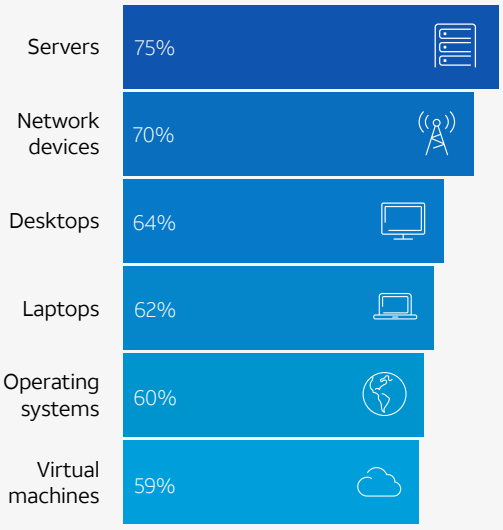
In fact, most IT pros consider end-user devices to be the most vulnerable. According to our research, desktop and laptop computers were considered to be the most at-risk for a security threat or breach, followed by smartphones, tablets, and wireless access points.[1]

Yet, organizations perform vulnerability assessments more commonly on network infrastructure devices, rather than on the end-user devices that they view as higher risk.[1]

Level of risk for security threat/breach



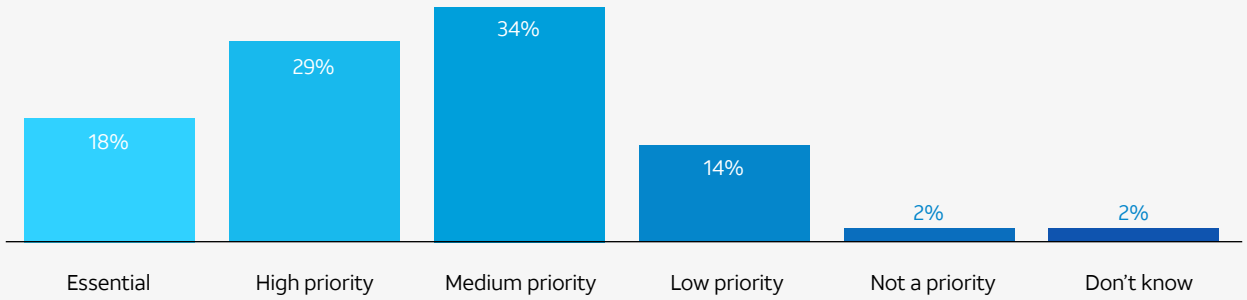
Vulnerability assessments performed



Forty-seven percent of organizations feel a vulnerability assessment is essential or a high priority to the IT security strategy.

That value is especially high among larger organizations (those with 500 or more employees).[1]

Importance of vulnerability assessment to IT security strategy



"Organizations cannot just think, 'Oh, we'll be lucky and not get breached.'"

"Everyone really needs to have a plan for security breaches and be sure that they're resilient. How can you be resilient? Only by planning for them. And that includes testing the incident response plan," Sundaresan says. "We're all evolving. If you're digitally transforming, why isn't your security transforming, too?"

And then there's cloud migration: as organizations move from on-premises systems to cloud-based services, they need to realize that even though the cloud provider offers security, there are a lot of controls that they're probably not covering. Cloud initiatives need to be folded into a broader security risk management discussion.

For many organizations, implementing vulnerability management presents them with challenges: they lack the skills or training for internal staff, the solutions are too costly, there isn't enough time to conduct such assessments, or they simply do not have the ability to scan devices that are not online all the time, such as laptops.

Deploying a managed security solution or a unified threat manager can help solve those problems—and help minimize risks for your organization.

Moving forward:

The case for managed security solutions and unified threat management

Today's organizations understand the importance of investing in security solutions, with 67% of them saying it is very important or critical—double the percent that said it was important in their organization three years ago.[1] And this importance will continue to gain prominence: 82% expect it to be very important or critical for their organization in another three years.[1]

However, IT professionals still face an uphill battle in convincing C-level executives to invest in advanced security solutions, such as a managed security solution. The case for MSSPs—or at the very least, an integrated threat management platform—begins with emphasizing their ability to understand environments, perform vulnerability assessments, and support a risk management strategy. By using an MSSP or integrated platform to manage the tactical response to cybersecurity issues, your company can be more strategic about security *and* other initiatives.

The right MSSP can:

Create a cost-efficient, centralized security strategy that will support business operations, not hinder them

Enable the company to focus on new technologies and innovation, while the provider manages the cybersecurity strategy (if required)

Offer a raft of other benefits, including 24/7 threat monitoring and support, the latest insights on emerging security threats, and access to enhanced network security features

These benefits align with the perceived needs of organizations: we found that 52% of organizations struggle to keep up with rapidly evolving security threats. And, separately, just 48% have the necessary resources in-house to keep the organization secure.[1]

Although these issues affect organizations of all sizes, small organizations especially feel the struggle. Many don't have access to the resources needed to create and maintain a cohesive cybersecurity strategy. Here, MSSPs can apply expert-level solutions to problems where in-house teams may not be able to address issues with the same level of expertise, as well as adapt quickly to the ever-changing landscape and keep pace with evolutions and permutations.

While mid-sized organizations often have an in-house security team, they don't expect to manage all their security processes, so they may offload their monitoring and response capabilities to a security provider. Through this hybrid model, the company and MSSP work together to formulate a response when a breach occurs and to help find ways to prevent it from happening again.

Large enterprises typically have the funding and resources to implement a full cybersecurity program; but an MSSP can offer access to data and information outside the networks of these enterprises. MSSPs can also offer threat feeds with intelligence that customers can digest into their environment, rather than just act on them individually.

"Organizations that don't have cybersecurity as a core business differentiator, or as a core business function, are often struggling to adapt modern cybersecurity practices," says Kayne McGladrey, Director of Information Security Services for Integral Partners LLC. MSSPs can have the technology and breadth of knowledge to extend a company's overall security. "A good managed security provider has the right technology, addresses compliance issues, and most importantly, knows how to adapt. They will constantly up their security expertise to keep you protected," says Sundaresan.

> "The reason to use an MSSP was simple. We didn't have the expertise on staff… We could use the MSSP to watch for threats and actively respond and mitigate them 24/7."
>
> *—Network Director, Healthcare Organization*

Security is a company-wide issue

Cybersecurity has traditionally been viewed as an IT issue, but in today's digitized world, that thinking is dangerous. Organizations need to eliminate silos and prioritize collaboration so that business operations are transformed, and cybersecurity is placed front and center.

Because MSSPs have a broader view of a client's environment, they can help ensure that the client is not investing blindly. After all, 51% of organizations say their current investment in security solutions is adequate to keep them protected—but only 38% feel they're secure from a security threat or breach.[1]

Clearly, investment doesn't equal confidence. So, a new approach might be necessary.

> "Not all investment is good investment. You need to know what your data security priorities are first. Without this understanding, you could be chasing a shiny object of little value."
>
> *—Todd Waskelis, AVP with AT&T Cybersecurity Solutions*

Conclusion

To be truly comfortable in your organization's security approach, you need an effective security risk management strategy built on the concept of edge-to-edge protection. You need to know what your data security priorities are, and policies actually have to be enforced. Without that understanding, you could be throwing money into cybersecurity with very little return or benefit, strangling your business operations rather than supporting them. An MSSP can help solve those problems, and build confidence in your defense against cybercriminals.

About AT&T Cybersecurity Solutions

AT&T cybersecurity solutions business division combines the strengths of AlienVault's foundational **Unified Security Management** platform and the **Open Threat Exchange** with the AT&T suite of managed cybersecurity services, solutions and network visibility to better protect businesses. The focus of AT&T Cybersecurity Solutions is on making security capabilities and technologies accessible to businesses of all sizes around the globe.

Ready for your own cybersecurity risk assessment?

Find out how well your organization is doing with cybersecurity risk management.
Get a FREE assessment from AT&T Cybersecurity now.

Learn how AT&T security solutions can help you at:
att.com/security

Browse previous reports at:
att.com/cybersecurity-insights

About the Spiceworks Survey

AT&T commissioned Spiceworks to conduct an online survey in July 2018 to gain insights on cybersecurity practices in midsized organizations. There were 250 respondents in the U.S. The IT decision-makers were required to have involvement with security decisions and purchases at organizations with 150+ employees.

Sources

[1] Spiceworks "Voice of IT" survey of 250 IT decision-makers in the United States, July 2018.

[2] "The Intelligent Business: Bold moves, priorities, and barriers to cross the turning point," AT&T Business, September 2018.