SecureLink®
an Imprivata company

Ponemon INSTITUTE

The state of cybersecurity and third-party remote access risk

Organizations are treading water when it comes to cybersecurity: What happens when the next wave comes?

A letter from SecureLink chief technology officer Joel Burleson-Davis

I wish I could introduce you to a report with better news. Organizations are facing an increase in cyberattacks and its financial impact is enormous. The areas of vulnerability found in 2021 seem to only be growing in 2022, with more organizations reporting cyberattacks caused by third parties. Software companies are facing this problem. Hospitals are facing this problem. Banks are facing this problem. We've reached a point where no one can afford to ignore the increasing threat of cyberattacks.

The good news is that organizations that are smart about strengthening their cybersecurity infrastructure can succeed in reducing vulnerabilities and fending off attacks. A few organizations were able to improve their security posture in the last 12 months, but it still wasn't enough to move the needle — and it's not for a lack of trying. Organizations have an average annual IT budget of $365 million, $78.5 million of which is spent on cybersecurity infrastructure. In the last 12 months, organizations have spent an average $9+ million to remediate the impact of cyberattacks, and yet, 54% of these organizations have experienced a cyberattack within the same period of time. It begs the question of how these investments became so misplaced.

Given the year-over-year increase in cyberattacks, it's striking that the majority of organizations continue to use manual controls to monitor third-party access when automated options are not only available but necessary. Organizations race to innovate within their competitive markets but forget that cyber risks are evolving just as quickly. According to this year's report, 48% of organizations don't have a comprehensive inventory of all third parties with access to their network, a decrease from 50% in the 2021 report. That might be why 49% of these organizations have experienced third-party attacks in the past 12 months compared to just 44% from the prior 12 months. That number will only increase if organizations continue to rely on manual infrastructure when cyber attacks are advancing every day. The same keen eye a company places on new developments within its industry needs to watch for emerging risks and do so with the most advanced tools.

Organizations' reluctance to update their security infrastructure might be due to budget or personnel. A number of companies choose to build their own security system because they don't know there are options out there that have already been built. Or they may look for a quick and immediate solution that won't have lasting effects. They'll become more and more vulnerable with each passing year that their security software remains the same.

When organizations finally recognize the need for automated tools, they still might not know where to start. The problem I often see is that the initial, fundamental questions aren't being asked: What would a successful framework look like? What would it solve? Organizations don't identify their own requirements before they begin poking around the internet looking for a software solution. They need a problem-first approach over a tool-first strategy. And before a company simply Googles it, they should recognize that there is value in talking to people and other trusted organizations as well. Companies may feel unique, but the problem of third-party security—or lack thereof—is ubiquitous.

Organizations need to prioritize critical access management to strengthen their cybersecurity infrastructure and protect their most important assets, which can only be done if there is an automated system that detects vulnerability and remains vigilant as new risks emerge. Developing automated infrastructure is a powerful form of insurance, especially when every company in the world needs to address cybersecurity.

The attacks won't stop coming, and no one is immune. But every company can be proactive in preparing for the worst, so it can emerge at its best.

Digital transformation is happening across industries. We see it with the emergence of “smart factories,” the streamlined payment methods and supply chain in the service and retail industries, and the use of artificial intelligence in everything from our smartphones to medical equipment. Changing and evolving technological trends create ease, efficiency, and convenience in our daily lives.

Businesses of all sizes — from the global enterprise to the home-based start-up — are integrating more technology into their workflows and processes. The COVID-19 pandemic drastically advanced this transformation. Within a moment’s notice, operations, workforces, and all means of communication became digital, and it’s impacted the business environment ever since.

Over the last two years, 59% of organizations have changed their cybersecurity structure to meet the new and evolving needs. However, organizations have barely moved the needle when it comes to the effectiveness of those security strategies.

The purpose of this second-annual research study, sponsored by SecureLink, is to understand how organizations are investing in their cybersecurity infrastructure to minimize threats and third-party remote access risk. Ponemon Institute surveyed 632 individuals who are involved in their organization’s approach to managing remote third-party data risks and cyber risk management activities.

An evolving digital landscape

The manufacturing sector is a prime example of this evolving digital landscape and the threats that come with it. For better or for worse, Industrial Revolution 4.0 has turned factories into “smart,” internet-connected businesses. The equipment and technology used in manufacturing was originally built for on-premise teams. In order for any malfunctioning PLCs or industrial control systems to be fixed, a vendor would have to drive or fly to the factory to repair any damage. Now, most repairs can be done remotely, without any physical presence needed. But what factories are gaining in efficiency they are losing in security. Factories aren’t prepared for this innovative change and it’s shown — 46% of industrial and manufacturing organizations have experienced a data breach or cyberattack in the last 12 months.

Complexity: In an evolving threat landscape, organizations want simple and effective solutions

SYSTEM COMPLEXITY AND EFFECTIVENESS ARE KEY FACTORS IN IMPROVING SECURITY INFRASTRUCTURE

67% of organizations look at how to solve system complexity issues when improving their cybersecurity structure.

What are the primary factors considered when making improvements to your cybersecurity infrastructure?

Hardware requirements	49%
In-house expertise	58%
Installation costs	40%
Interoperability issues	52%
Personnel issues (lack of in-house expertise)	33%
System complexity issues	67%
System effectiveness issues (high false positive)	60%
System performance issues (degradation)	48%
The licensing cost	19%
The maintenance cost	17%
Vendor support issues	39%
Visibility of core systems	15%
Other (please specify)	3%

When determining how to improve their cybersecurity structure, most organizations (67%) will look at the complexity of current systems and their effectiveness (60%). They need streamlined solutions that can integrate into their already existing systems, which is why over half also cite interoperability issues as a consideration when updating security tech.

BARRIERS TO ACHIEVING A GOOD CYBERSECURITY POSTURE

What are the most significant barriers to achieving a strong security posture?

Insufficient resources or budget	35%
Insufficient visibility of people and business processes	51%
Insufficient assessment of cybersecurity risks	43%
Difficulty in hiring and training which leads to a lack of skilled or expert personnel	48%
Lack of leadership	23%
Lack of oversight or governance	60%
Complexity of compliance and regulatory requirements	37%
Other (please specify)	3%

The biggest struggle to achieve a strong security posture is a lack of resources, whether that's budget, information, management, or staff. Unfortunately, this isn't an uncommon issue: cybersecurity is often deprioritized at an organizational level. 39% of organizations allocate 15% or less of the annual IT budget towards cybersecurity, and 52% said securing third-party remote access isn't a priority for their IT or security teams.

Lack of governance is what keeps most organizations from a strong security posture, but they also struggle to have clear visibility into the people and business processes that help determine what's needed for strong security. If you don't know the users or workflows that need securing, you can't put proper security protocols in place.

The Great Resignation has also made finding talent relentlessly difficult. To maintain a strong security posture, you need staff who are equipped to manage it, which is why so many participants indicated they need in-house expertise. But when hiring, training, and retaining skilled personnel is a roadblock in itself, organizations will start to look elsewhere.

THIRD-PARTY COMPLEXITY

More businesses are becoming reliant on third-party vendors for operational support since in-house talent is challenging to maintain and on-site premises have been replaced by the cloud — but third parties contain their own risks and complexity.

39% of organizations expressed that a primary factor in improving security frameworks is vendor support issues

48% of respondents don't have comprehensive inventories of their third parties due to the complexity in third-party relationships

So, what?

The looming problem for businesses is how to make cybersecurity less complex and more effective. As digitization builds momentum, organizations need to adapt to trends and technology that will not only solve their current issues but are built to adapt and endure a rapidly changing cybersecurity landscape. To keep up with sophisticated threats, security tools need to be streamlined and interoperable. Technologies need to “play well with others” if there are any hopes of creating a robust, comprehensive, and autonomous security infrastructure.

To start streamlining and simplifying security strategies, organizations can start by evaluating their current strategy, what system complexities they’re trying to solve, and how it should ideally be managed. As for the talent retention barrier, creating a more effective and streamlined security strategy will not only appeal to skilled personnel, but will also help shore up gaps found in security areas such as system maintenance, oversight, control, and monitoring.

Cybersecurity: Organizations are treading water when it comes to cybersecurity

Cybersecurity is not a constant. What constitutes "strong" cybersecurity is always evolving, and even then, it depends on the organization, the industry, and the threats of the day. In the past few years, there's been a shift, both in cyberattacks and how cybersecurity is viewed, designed, and implemented. And while many organizations and industries have seen the writing in the code and started to shift their cybersecurity strategies, threats continue to evolve as well. The truth is: organizations are barely treading water when it comes to staying safe and secure.

59%

of organizations say their cybersecurity strategy has changed over the past 2 years

ORGANIZATIONS ARE SHIFTING TO ACCESS MANAGEMENT MODELS AND MODERN CYBERSECURITY STRATEGIES

Alignment of goals among security and business leaders	16%
Deployment of cybersecurity compliance, risk management and privacy framework	29%
Emphasis on the remote workforce	49%
Expanded use of automation and AI tools for security operations	51%
Heightened awareness among employees about cyber hygiene	45%
Improved communications to customers regarding security issues	31%
Increased accountability among employees	54%
Integration of health and safety considerations as part of security operations	35%
Reliance on security in/from the cloud	48%
Reliance on third parties in achieving security goals	37%

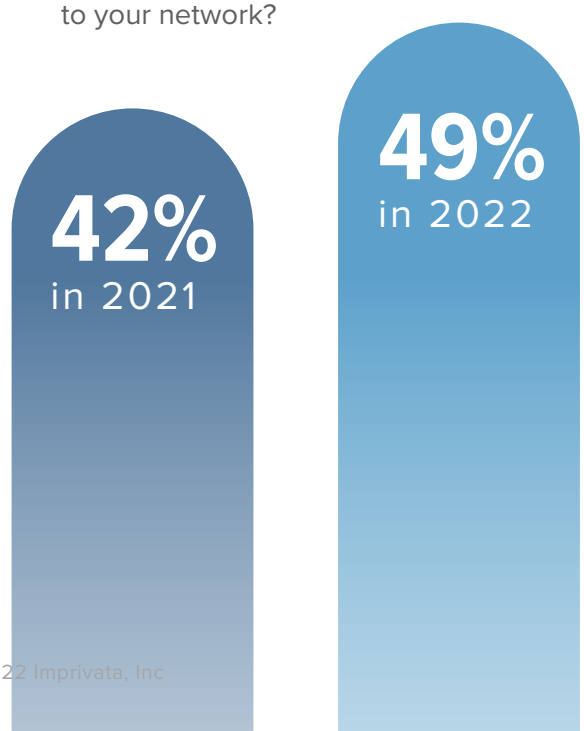
While organizations are automating security operations, demanding employee accountability, and have better awareness of cyber hygiene, we're also seeing a bigger reliance on third parties and remote work — both of which can introduce new cyber risks.

Enhanced physical controls (i.e., restricted control areas)	63%
Restriction of network access	65%
Enhanced identity and access management techniques	47%
Ensure access entitlement is appropriate to the job function	60%
Network segmentation/isolation	55%
Remove access credentials when appropriate	41%
Verification of a third party's need to have network access	36%
Education of privileged users	40%
Other (Please specify)	4%

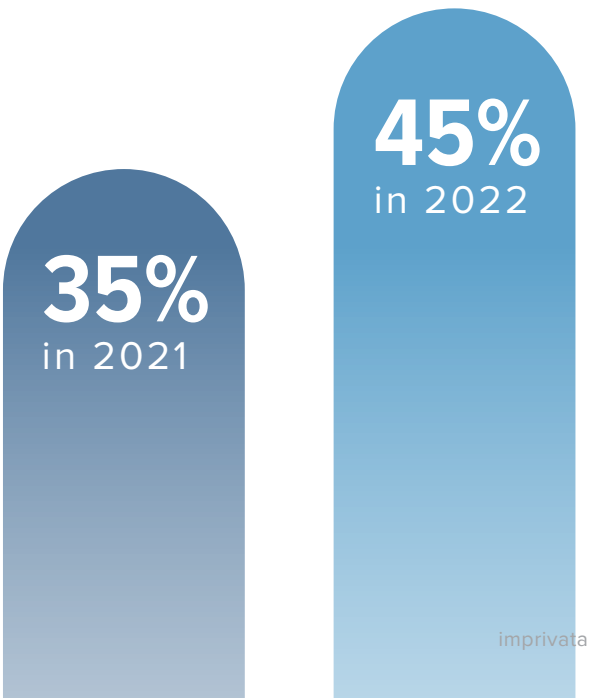
More than half of organizations are understanding the importance of (and implementing the practices of) limiting access by restricting network (and physical) access. However, they are still struggling to provision and deprovision access for both internal and external users.

Third parties introduce risk, but organizations are improving when it comes to third-party security.

Does your organization have a comprehensive inventory of all third parties with access to your network?



Does your organization have identification of all third parties accessing your most sensitive data?



But — the number of attacks has stayed the same.

- 54% of organizations have experienced a cyberattack in the last 12 months
- 52% say there is an increase in cyberattacks compared to last year
- Third-party attacks have increased from 44% to 49% year over year

Types of cyberattacks organizations have experienced in last 24 months:

49%
ransomware

48%
DDoS

THIRD-PARTY THREATS ARE STILL PREVALENT

Has your organization **ever** experienced a data breach caused by one of your third parties that resulted in the misuse of its sensitive or confidential information, either directly or indirectly?	FY2022	FY2021
Yes	56%	51%
No	42%	43%
Unsure	2%	6%
Total	100%	100%

In the past 12 months , has your organization experienced a data breach or cyberattack caused by one of your third parties, either directly or indirectly?	FY2022	FY2021
Yes	49%	44%
No	48%	52%
Unsure	3%	4%
Total	100%	100%

If yes, did any of these third-party breaches or cyberattacks result from giving too much privileged access to your third parties?	FY2022	FY2021
Yes	70%	74%
No	28%	23%
Unsure	2%	3%
Total	100%	100%

What industry is the most vulnerable to attack?

The data shows that every industry contains vulnerabilities and strengths, but there are a few standout points to consider.

- **Financial** sector and healthcare are the two top industries targeted by cybersecurity attacks. 58% of financial organizations and 55% of **healthcare** organizations stated that they experienced a third-party data breach in the last 12 months. This is not a surprise, as both industries rely heavily on third-parties and contain valuable data (like financial information and PHI) that hackers are after.
- In addition, neither of those industries feel their IT systems are making third-party security and access a top priority — 66% for financial services and 65% for healthcare.
- While those two industries are at a particular risk, more than 50% of **every industry** surveyed (financial services, healthcare, public services, infrastructure and manufacturing, and education), stated that managing third-party security is overwhelming and a drain on internal resources.

So, what?

What these data points tell us is both good news and bad news. Organizations are starting to understand what's needed to keep their critical access points (and data and systems) safe, but with attacks increasing in frequency and sophistication, not much headway has been made.

We're seeing the trend of organizations struggling to innovate their cybersecurity as quickly as other aspects of their operations (remote work, IoT, internal software), instead relying on outdated practices and software instead of implementing granular access management, especially when it comes to proactive measures like proper access governance and visibility.

When looking at third-party access in particular, organizations are still not treating those external parties as the security risk they are, and the results are devastating. It's not difficult to restrict access, but it was probably difficult, time-consuming, and costly for those 70% of organizations above to deal with the fallout of a third-party cyberattack. While there is a statistically significant increase in terms of identifying third parties, that number is hovering under 50% while the reliance on third parties and a remote workforce is trending upwards. And while there is an increase in those measures, organizations are still finding managing third-party access to be overwhelming. All those numbers add up to a major risk point.

Treading water is enough for today, but for tomorrow, organizations of all industries need to closely examine what threats are looming and take proactive measures to prevent the next cyberattack.

Access governance and access visibility: Every industry is struggling to gain access visibility and implement governance

There are two crucial components to a strong access management strategy: Access governance and access visibility. The data shows that organizations are struggling with both.

Organizations are struggling to implement governance

60% of organizations cite lack of oversight and governance as a barrier to achieving strong security posture

53% of organizations are not implementing enhanced identity and access management techniques for high-value data assets

43% of organizations are able to provide third parties with enough access and nothing more to perform their designated responsibilities and nothing more.

59% of organizations are not revoking credentials when appropriate

What is access governance?

Access Governance is the system and processes that make sure access policy is followed as closely as possible. Strong access governance includes established rules of which users can access what and the specific privileges those users have.

What is access visibility?

Access visibility is a component of governance and means that an organization knows the level of access and permissions that a user has within a given system.

ORGANIZATIONS HAVE VISIBILITY

- Only **36%** of organizations visibility into the level of access and permissions both internal and external users have
- When it comes to documentation of third parties and third-party access:
  - Only **38%** know what network access third parties have
  - Only **45%** have Identification of third parties that have the most sensitive data
- Only **15%** cited visibility of core systems as primary factor in making a security improvement.

So, what?

Strong access management begins with governance. Letting users into your organization's system, whether internal or external, "should not be a task taken lightly".

Strong access governance includes:

- Role-based access control (for internal users)
- Restricted user access that aligns to the principle of least privilege access
- Periodic user access reviews (that can lead to access adjustments, provisioning or deprovisioning).

Not having a strong understanding of who can access what, as well as policies that apply to an given user, is the equivalent of leaving every door and window wide open. Mismanaging access is a major cause of data breaches, and the numbers above highlight that, especially when it comes to third-party access. While the data showed that 60% of organizations are able to ensure that access entitlement is appropriate to job function, that number only applies to internal users. Third parties can't be treated the same as internal users. They have different titles, roles, and responsibilities, meaning implementing role-based access controls is not possible. Instead, organizations must utilize diligence and detail to make sure those accesses are not mismanaged.

If you can't see what a user is accessing, you have no way of knowing:

01 If they should have that access

02 What they are doing with that access

03 If that access is creating a security gap

If an organization can't answer those three questions when it comes to user access, they are essentially turning a blind eye to the risk and possible attack of their network, data, and assets. As stated previously, cybersecurity, especially in regards to access management, is not set in stone. Organizations need to be able to adapt to new threats, change access strategies, and learn and evolve over time. A lack of governance and visibility makes all of that harder to achieve, and leaves organizations open to a bad actor who will exploit those vulnerabilities.

Zero trust and access controls:

Learn to lock your doors

ORGANIZATIONS ARE GIVING TOO MUCH ACCESS TO THIRD PARTIES

What is access control?

Access control is the additional security layer on top of access governance that helps protect high-risk and high-value assets. Kinds of access control include:

- Access notifications
- Access approvals
- Time-based access
- An access schedule
- Zero Trust Network Access
- Multi-factor authentication
- Privileged credential management

What the data says about current access control methods:

of organizations state that a third-party breach came from granting too much access, but only 52% said that breach changed their cybersecurity practices.

of organizations are able to provide third parties with enough access to perform designated responsibilities and nothing more.

of respondents don't rate the use of multi-factor authentication as highly important in their access control standards.

Zero trust

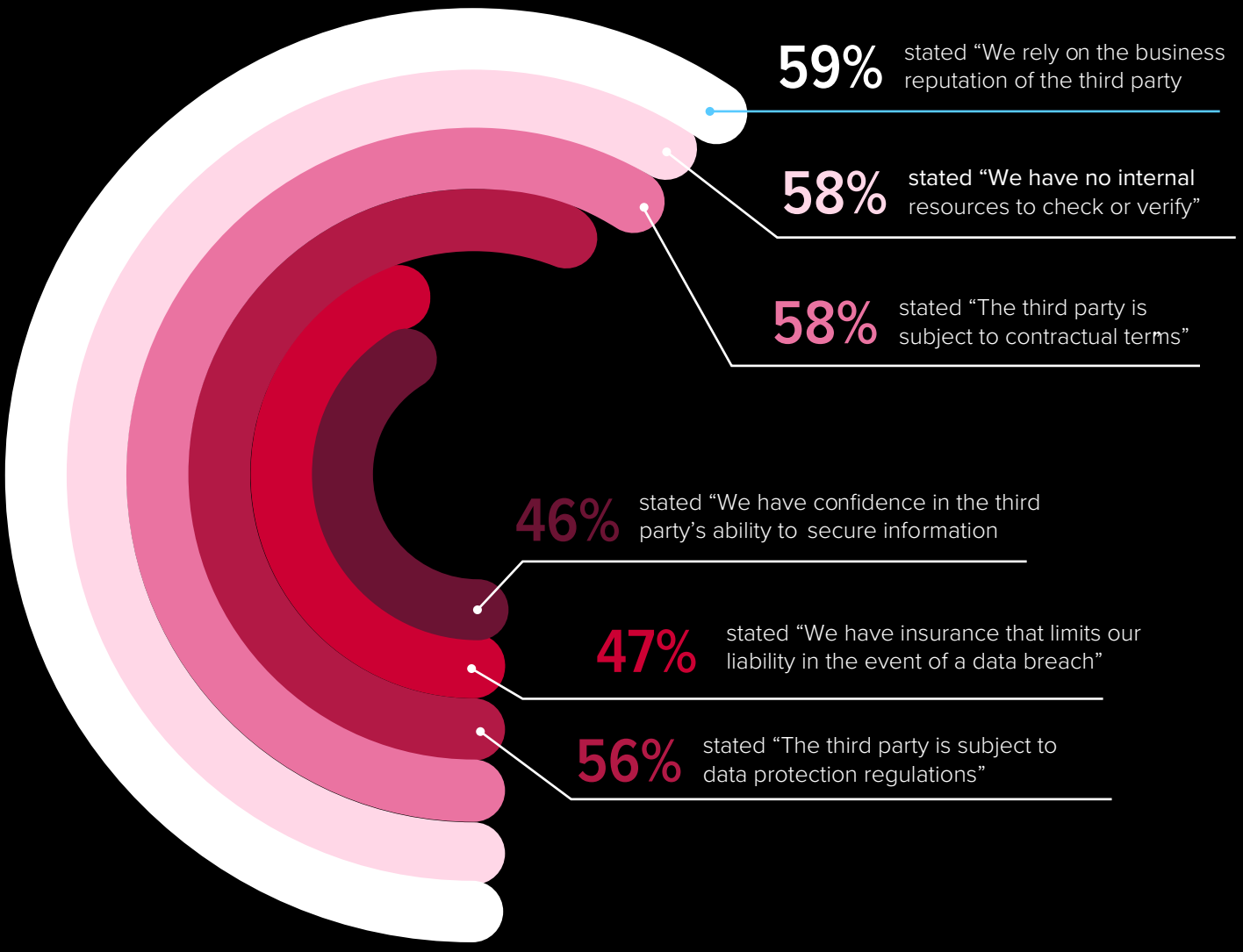
These percentages show that organizations are not implementing Zero Trust Network Access, especially in regards to third parties. Zero trust may be viewed as an overused buzzword, but the implementation of it is both real and critical to controlling access. Having ZTNA means taking a “never trust, always verify” approach to access and access rights. It includes (but not limited to) implementing multi-factor authentication for every user and using credential vaults to prevent access creep or credential theft, the latter of which was reported by 54% of respondents.

REPUTATION RELIANCE: TRUSTING THE UNKNOWN

In place of a zero trust system or strong third-party access controls, organizations often rely on trust or reputation when it comes to granting access.

.

Why doesn't an organization monitor third-party access to sensitive and confidential information?



Despite that reliance on trust and reputation, organizations remain as confident in their third-party vendors as they were in 2021, which is to say, not very confident.

61% of organizations aren't confident that their third parties would notify them if they had a data breach involving your organization's sensitive and confidential information.

So, what?

Think about the brakes on a car. When a moving car needs to stop, the driver applies brakes to add friction to the road and bring the car to a halt. The same can be said for access controls. When a user is moving through a system, access controls apply the brakes to stop that user from getting any further than they need to within a network. It's the figurative checkpoint and a literal method to reduce an attack surface and stop bad actors from reaching an organization's most critical assets. Yet, those brakes are squeaky, at best, for most organizations.

The majority of organizations are stating that yes, cyberattacks are increasing, and yes, breaches for them came from too much access and more than half originated from credential theft. But no, they state, we are not controlling access. The solution couldn't be clearer.

Benefits of access control include:

- Limiting the attack surface if a bad actor enters a network
- Prevention insider threats, like access creep
- Stops a third-party-based attack in its tracks
- Prevents user error that could result in compromised data or information
- Reduces the effectiveness of phishing and ransomware

Proactive security is better than reactive security, and access control (in its many forms) is a simple and effective form of proactive security that can prevent a great deal of damage.

Monitoring: Half of organizations aren't keeping tabs on user access

Monitoring user access is a core component of any access management strategy. Think of a home security system: it constantly watches for behavior that could trigger an alarm. Access monitoring tools accomplish the same goal of watching user access and triggering "alarms" when bad behavior is suspected.

What is access monitoring?

Access monitoring involves observing, recording, or documenting a user's behavior while they are logged in to a critical asset (network, software, database, etc.) and analyzing that behavior to prevent future security incidents or investigate anomalies in session activity.

The problem is that, although businesses consider monitoring a crucial part of their security strategy, many are having trouble actually executing it across all users — especially third parties.

56% of organizations are tracking and monitoring all access to network resources and critical data

59% of organizations capture detailed audit logs of each vendor support session

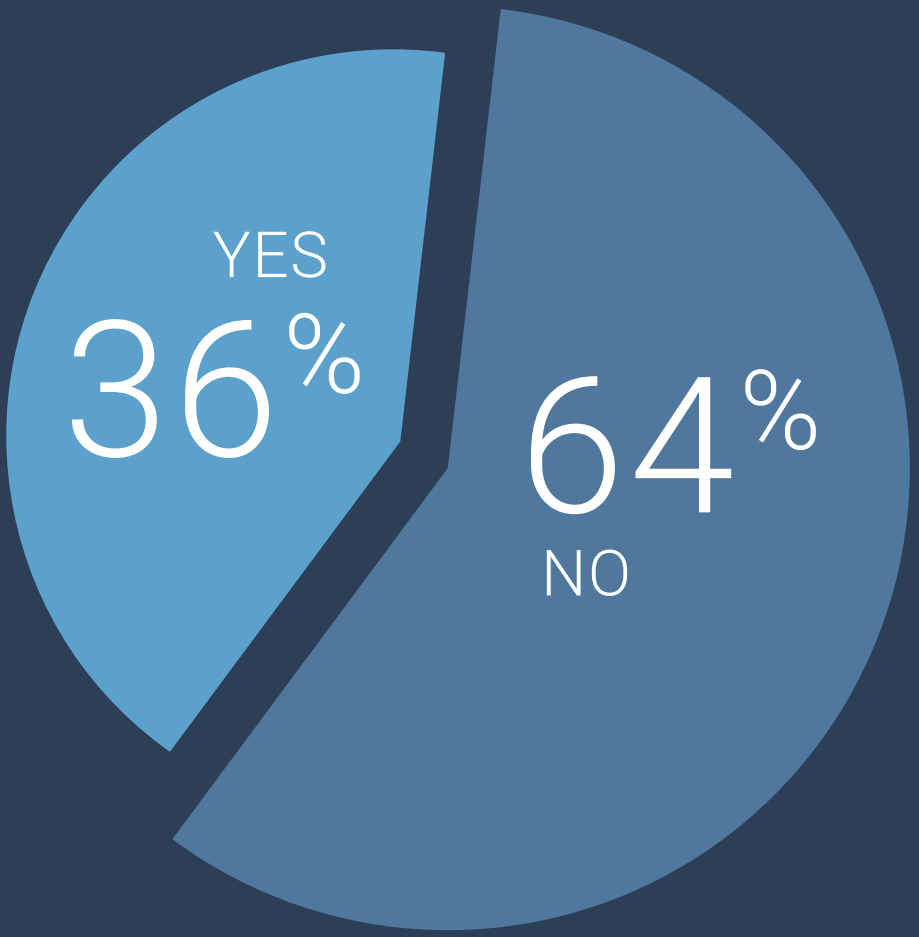
50% of organizations don't monitor third parties with access to sensitive and confidential information.

Businesses continue to struggle monitoring third-party access

Are third parties with access to your organization's sensitive and confidential information monitored?	FY2022	FY2021
Yes (please skip to Q35) 45% 46%	45%	46%
No (please skip to Q34)	50%	51%
Unsure	5%	3%
Total	100%	100%

If no, why doesn't your organization monitor the third parties' access to its sensitive and confidential information? Please check all that apply.	FY2022	FY2021
We don't have the internal resources to check or verify	58%	54%
We have confidence in the third party's ability to secure information	46%	47%
We rely on the business reputation of the third party 59% 61 %	5%	3%
We have insurance that limits our liability in the event of a data breach 47% 50%	100%	100%
The third party is subject to data protection regulations that are intended to protect our information	56%	59%
The third party is subject to contractual terms	58%	61%
The data shared with the third party is not considered sensitive or confidential	29%	30%
The third party will not allow us to independently monitor or verify their security and privacy activities	23%	23%
Other (please specify)	2%	3%

Third parties are opaque, transient, and bring risk to a business' digital environment, yet they still get overlooked in cybersecurity strategies. Year over year, the numbers still show staggering confidence in reputation or contractual terms as the reason why organizations don’t monitor third-party network access.



Does your organization automate the monitoring process of third parties?

Businesses are working harder, not smarter, with their monitoring practices

HOW MUCH TIME IS SPENT WEEKLY ON MANUALLY MONITORING THIRD-PARTY ACCESS?

Real-time	19%
1 to 4 hours	25%
5 to 10 hours	27%
More than 10 hours	29%
Total	100%
Average	7.00

So, what?

We said it last year, and we'll say it again: reputation, contracts, and sheer confidence don't secure your critical assets or provide real-time monitoring and insight into your systems. When a bad actor exploits a third-party connection, a solid Google review or the clause in section two of the service agreement aren't going to stop the attack.

47% of respondents say they aren't highly effective in detecting third-party threats. With the lack of monitoring and automation that's taking place, it's easy to see why.

It takes real monitoring processes, like software that can capture the activity in all third-party user sessions, record desktop sharing sessions, and keep text-based logs that show what each third-party user is physically doing. It's a baseline proactive defense that can pick up on any anomalous behavior and provide the evidence or documentation needed if a cyber incident occurs. And when used to its optimal potential, monitoring technology can detect, thwart, and prevent threats before they even begin with innovations like detection technology, AI, and machine learning.

51% of organizations have expanded the use of automation or AI into their cybersecurity strategy over the last two years

There's a learning opportunity here for organizations that are manually keeping tabs on third parties. Manually conducting access monitoring is laborious, time-intensive, and very prone to human error. Implementing adaptive and automated technology that can monitor user access will save organizations time (so IT teams can attend to other high-priority projects) and money (like the costs incurred from a data breach).

Cost: Organizations aren't investing in cybersecurity. It's costing them.

WHAT RANGE BEST DESCRIBES YOUR ORGANIZATION'S ANNUAL IT BUDGET?

What range best describes your organization's annual IT budget in the current fiscal year?	FY2022
Less than $1 million	3%
$1 to $10 million	6%
$11 to $25 million	11%
$26 to $50 million	12%
$51 to $100 million	13%
$101 to $250 million	17%
$251 to $500 million	17%
Total	100%

Despite many organizations, a plurality of respondents allocating over $500 million to the IT budget, the numbers tell a more realistic story: IT budgets vary from company to company and will depend on the size of the business, its revenue, and its specific IT and infrastructure needs. A small company with a $10 million IT budget could have an equally streamlined and digital environment as a large corporation with $300 million dedicated to IT expenses.

But how those IT budgets are used is a different story.

IT BUDGETS ARE ALLOCATING A FIFTH OF THEIR BUDGET TOWARDS CYBERSECURITY AND IT'S NOT ENOUGH

What percentage of your company's annual IT budget is dedicated to securing the cybersecurity infrastructure?	FY2022
None	0%
Less than	3%
5% to 10%	11%
11% to 15%	25%
16% to 20%	28%
21% to 30%	16%
31% to 50%	10%
More than 50%	7%

Over half of organizations are spending between 11% and 20% on cybersecurity, but despite this investment:

35% say insufficient budget or resources are barriers to achieving a strong cybersecurity posture

52% of organizations are tracking and monitoring all access to network resources and critical data

54% have experienced a cyberattack in the last 12 months

49% of organizations have experienced a data breach caused by a third-party vendor in the last 12 months

50% of organizations don't rate their organization as highly effective in mitigating remote access risks

Nearly half of respondents don't feel their organization is effective in detecting remote access risks, responding to a third-party cyber incident, or controlling third-party access to its network

A BIG BUDGET DOESN'T SAVE ORGANIZATIONS FROM COVERING THE COSTS OF CYBERATTACKS

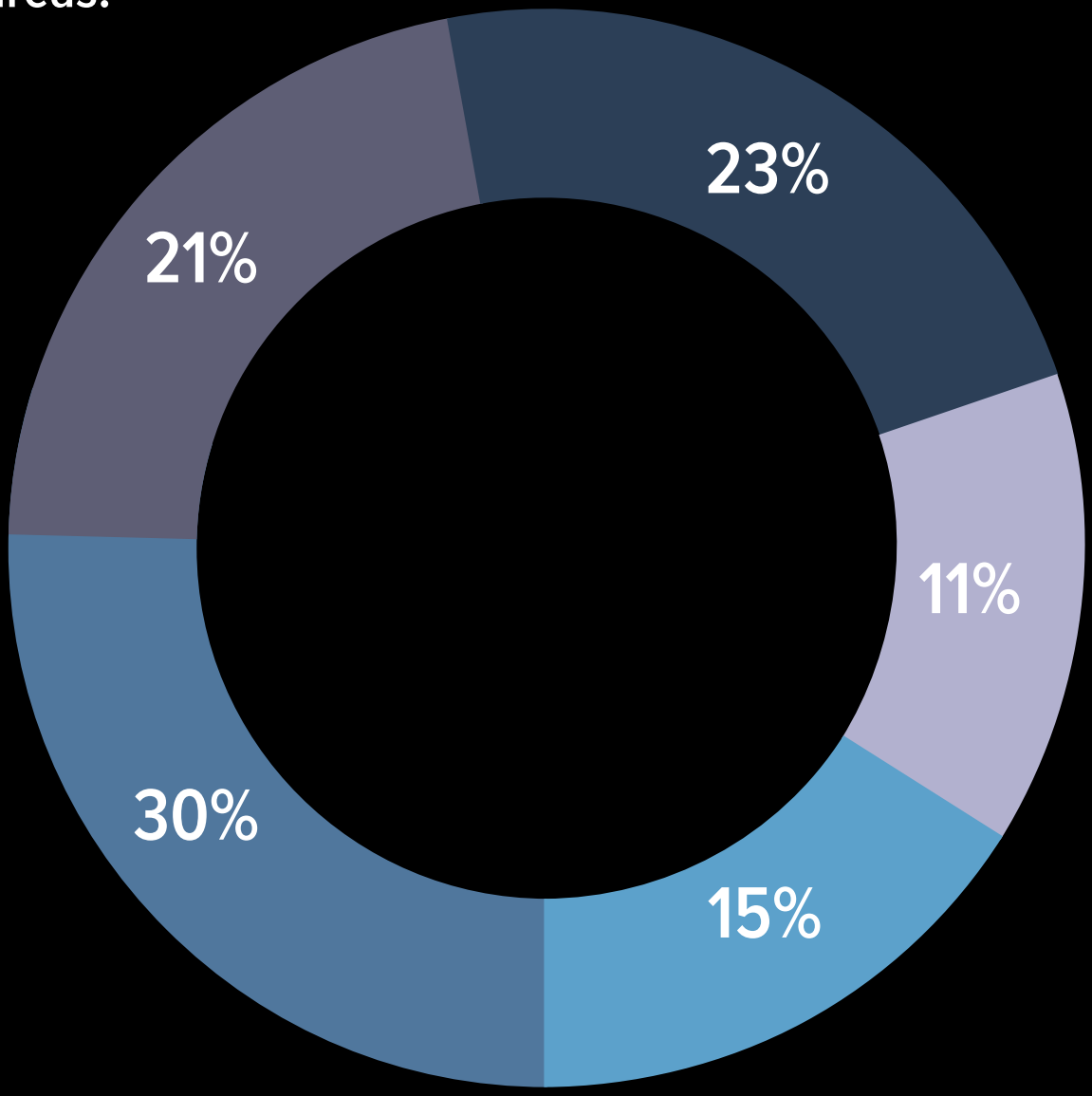
What's the estimated financial impact a cyberattack has had on your organization?

Estimated financial impact	FY2022
Less than $10,000	0%
$10,001 to $50,000	6%
$51,000 to $100,000	4%
$100,001 to $250,000	12%
$250,001 to $500,000	16%
$500,001 to $1,000,000	15%
$1,000,001 to $5,000,000	13%
$5,000,001 to $10,000,000	12%
$10,000,001 to $25,000,000	9%
$25,000,001 to $50,000,000	8%
More than $50,000,000	5%

The minimum companies are spending on recovering from a cyberattack is $10,000. Does your organization have an extra $10,000 to recover from a data breach? Investing in cybersecurity proactively and budgeting for stronger security tools could save your organization tens of thousands (and possibly millions) of dollars of cyberattack clean-up.

No company is spending less than $10,000 recovering from a data breach. When you look at the various issues that need addressing once a cyberattack happens, the costs add up fast, and it's a cost IT teams might not be prepared to handle — financially or operationally.

How much of total cyberattack clean-up cost goes to different areas:



- Remediation & technical support activities, including forensic investigations, incident response activities, help desk and customer service operations
- Users' idle time and lost productivity because of downtime or system performance delays
- Disruption to normal operations because of system availability
- Damage or theft of IT assets and infrastructure
- Reputation loss and brand damage

So, what?

There's a disconnect between what an organization budgets for cybersecurity and what's needed to fully secure a business' mission-critical systems and assets. Even though it seems like organizations have substantial IT budgets, security is still average at best. It's consistently enough to prevent threats or give organizations confidence that their existing security solutions can handle the risk that comes from user access and third-party remote access.

It's time to see the writing on the wall — organizations aren't investing in the right security solutions that can reduce risk, prevent threats, and give the confidence businesses need in their cybersecurity systems. This is, again, where automation and streamlining security technology can save organizations financially and operationally. The investment upfront, no matter how heavy, will prove its worth when previously manual or siloed workflows (like manually tracking access permissions or third-party vendor identities) are made efficient. That's also why interoperability between systems is critical when investing in cybersecurity initiatives. If you're going to invest in security technology, make sure it covers all vulnerabilities, secures all access points, and integrates with existing technology to shore up the gaps that are leading to these rising and troubling cyberattacks.

Conclusion

Year over year, the stats continue to tell the same unsettling story. Cyberattacks are on the rise, especially those caused by third parties, and the financial impact is significant. While technology has advanced to allow for more secure infrastructures, organizations still aren't implementing best practices that could detect, prevent, and respond to these threats in a highly effective way.

KEY TAKEAWAYS :

- The future of cybersecurity is in protecting access points and identities. Hackers are looking for the path of least resistance into mission-critical applications and assets, whether that's a vulnerable access point or a poorly secured credential.
- Automation and efficiency are key factors in a successful cybersecurity strategy. Using security technology to streamline operations creates efficiency, which in turn, will be more effective in mitigating threats and pulling in/retaining talent to manage cybersecurity.
- Internal resources are valuable and needed. The biggest challenge businesses face is having the manpower to manage third-party identities and cyber risk. With more streamlined systems and automated workflows, access is more manageable and less burdensome on employees.
- Do research and invest. An investment in cybersecurity is one of the best proactive steps organizations can take to protect their future success — but that investment needs to be in the right technology.
- Take the next step. One of the biggest causes of cyberattacks that isn't listed in this report? Doing nothing. Use the information in this report to assess your current cybersecurity strategy, find where you can improve or fill gaps, and see what organizations are doing — or not doing — to secure access.

For more information, please contact us at 1 781 674 2700
or visit us online at www.imprivata.com