SECURELINK

Ponemon INSTITUTE

A crisis in third-party remote access security

A deep dive into the third-party lifecycle, its greatest point of risk, and the threat that comes with it

Sponsored by SecureLink | Independently conducted by Ponemon Institute LLC

A letter from the SecureLink CEO

The verdict is in: When it comes to managing third-party remote access risk, organizations don't just need new tools, they need a new mindset. While awareness about the threat posed by third-party remote vendors has been growing, recent high-impact data breaches have thrown an even greater spotlight on the scale and far-reaching impact of unsecured third-party relationships. A single data breach can expose hundreds of millions of records, resulting in fines, fees, lost revenue, and liability that lasts for years.

As this study points out, more than half of respondents say their organizations have experienced a data breach caused by a third party that led to the misuse of sensitive or confidential information. Unfortunately, that number isn't surprising when you consider how many organizations take what amounts to a "fingers crossed" approach to third-party risk management. Signed contracts, strong reputations, and compliance checklists are important starting points in protecting third-party relationships. But they're just not enough – especially at a time when hacker activity is surging thanks to new remote ways of working.

And if an organization takes a "fingers crossed" approach then it is most certainly not a question of "if," but "when" and "how" and "how much."

The goal of this report is to arm senior decision-makers with information about the third-party remote access landscape so that they can stay ahead of the threats that are inevitably coming. And it's to help them understand that the issue isn't just about protecting a single organizations' data but safeguarding data belonging to customers, partners, and entire communities.

The good news is that resources are scaling up to match the magnitude of the problem. Moreover, there are technology systems and Zero Trust programs that enforce compliance policy and prevent human mistakes. They provide tested, reliable protection against third-party threats. The first step is understanding the new reality of third-party remote access risk. We hope this report helps you begin that journey.

Joe Devine, SecureLink CEO

A crisis in third-party remote access security

A deep dive into the third-party lifecycle, its greatest point of risk, and the threat that comes with it

Crisis and risk. Not two words you want associated with your cybersecurity strategy. But in this fast-paced digital world, the sophistication of cyberattacks has advanced just as quickly as technology without skipping a beat. As the internet of things (IoT) grows and interconnectivity makes its way into our organizations and our homes, hackers are making the most of the intricately woven web that connects our lives and technology.

And hackers aren't just advancing technologically - they are getting smarter, too. Sophisticated hackers don't just stop at social media profiles, but are targeting large-scale corporations that house sensitive or confidential information that can be exploited. Further, instead of attacking just one enterprise at a time, they've developed a more methodical approach that starts with a common denominator between multiple organizations and enterprises - a third-party vendor.

Third parties offer specialty services to their customers (enterprises or organizations) that require remote access into an organization's network in order to fulfill the responsibility for which they are hired. Oftentimes, these third-party companies service multiple customers, providing much needed support for specific functions that require network access.

So when hackers see a third-party company, they see more than one target - they see several, dozens, or hundreds of bullseye at which they can aim.

This "hack one, breach many" methodology explains the more recent mega breaches, one of the most infamous being the SolarWinds supply chain hack in late 2020. A virus hidden within the SolarWinds software update exposed thousands of its customers to malware. Since then, several more breaches have occurred, which has consequently brought more attention to the necessity of third-party remote access security.

SHOULD THIRD-PARTY REMOTE ACCESS SECURITY BE A REAL PRIORITY?

Quite simply and fervently - YES. It's no longer a matter of if, but when a hacker will try to penetrate an organization's network and information systems. There's a pandemic in the remote access space and it's the ideology that third parties don't pose significant cyber risks and that commonplace security practices suffice for a comprehensive remote access security strategy.

> "It's no longer a matter of if, but when a hacker will try to penetrate an organization's network and information systems."

Third-Party Lifecycle

As evidenced in this report, **many organizations view third-party remote access as a security threat, but not a priority.** Organizations are not taking the necessary steps to reduce third-party remote access risk, and, as a result, exposing their networks to security and non-compliance risks. The findings in this report showcase the lack of security, management, and accountability that's needed to adequately secure third-party remote access.

This report was conducted by the Ponemon Institute and sponsored by SecureLink. Ponemon Institute surveyed 627 individuals who have some level of involvement in their organization's approach to managing remote third-party data risks. They were also instructed to focus their responses on only those outsourcing relationships that require the sharing of sensitive or confidential information and involve processes or activities that require providing access to such information.

The report will walk you through the six stages of the third-party lifecycle (see above for visual). When an organization engages with a third party, there's often a typical lifecycle they go through, from "sourcing and selecting" to "reporting and ongoing management". The purpose of this research is to understand organizations' approach to managing third-party remote access risk in each stage of the third-party lifecycle and to provide guidance on how to prepare for the future.

SOURCE AND SELECT

Filtering third-party options

The first stage of the third-party lifecycle is source and select. In the source and select stage, organizations sift through the myriad of third parties that could fulfill a need an organization cannot fulfill itself. In this stage, factors such as cost, return on investment, efficiency and time savings, and productivity are all considered to determine which third party is worth the investment. One factor organizations aren't really looking for is network security - the one factor that has the potential to take down an entire company.

In reality, this part is often overlooked, as most organizations are not evaluating the security and privacy practices of third parties before they are engaged. Over half of respondents (51%) say their organizations are not assessing the security and privacy practices of all third parties before granting them access to sensitive and confidential information.[1]

Of these respondents, 59% say their organizations rely on signed contracts that legally obligate the third party to adhere to security and privacy practices[2], which means no evaluation was done before access was granted, and accountability for security protocol is dependent upon a signature.

A signature is not the only thing organizations rely on for a third party's security practices. **Reliance on reputation is the most common reason that organizations are not evaluating the privacy and security practices of third parties, according to 63% of respondents**[3]. But to what degree is reputation reliable? America saw what happened when thousands relied on the reputation of former American financier Bernie Madoff. Investors trusted Madoff's financial savvy and respected reputation as a Wall Street investment advisor, only to be duped in his Ponzi scheme, costing thousands of investors tens of billions of dollars in the largest financial fraud in history.[4]

Again...to what degree is reputation reliable?

> "Over half of respondents (51%) say their organizations are not assessing the security and privacy practices of all third parties before granting them access to sensitive and confidential information."

INTAKE AND SCORE

Assessing third-party risk

The second stage of the third-party lifecycle is intake and score. Once a third party is selected, engaged, and under contract, an organization will conduct risk assessments and scoring to determine the safety of on-boarding a new third-party vendor.

However, most organizations are in the dark about third-party risk because most do not evaluate risk before a third party is engaged. 65% of third parties are not required to fill out security questionnaires,[5] and shockingly, even more - 74% - are never asked to conduct remote or on-site assessments.[6]

To an even more shocking degree, third-party risk is not defined or ranked in most organizations. **61% of respondents say their third-party management program does not define or rank levels of risk**.[7] If risk is not defined or ranked - meaning all threats are categorized as a risk and rank the same - that means a spam email would fall in the same rank as a virus acutely installed in a software update that's pushed out to thousands of people. Defining and assessing risk provides insight into the levels of security needed to defend against a breach or hacking attempt.

4. Bernie Madoff, Britannica, https://www.britannica.com/biography/Bernie-Madoff.

Missing these critical steps in the intake and score stage leaves organizations unaware of a third party's protocol if the network were breached on account of the third party. Over half (52%) of respondents say their organizations are not aware of their industry's data breach reporting regulations[8] and do not have confidence in the third party's ability to secure information[3]. This means that if a breach did occur due to a third-party remote access connection, an organization may be left unaware of the intrusion, or it would take longer to discover the breach because of the lack of preparation in the intake process.

IDENTITY AND ACCESS MANAGEMENT

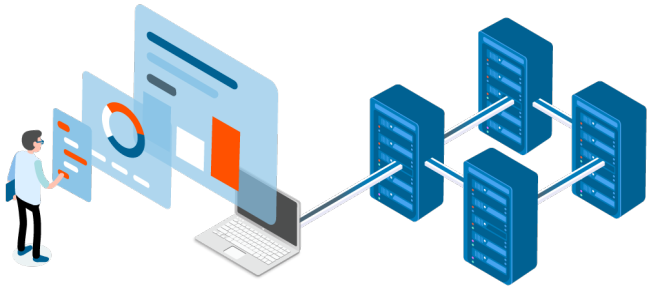
Controlling third-party permissions

After assessing risk and on-boarding a new third-party vendor, an organization enters the identity and access management stage of the lifecycle. As the name of this stage implies, this is where an organization identifies the access requirements of the recently hired third party and specifies what access it needs within the network to provide the services it was hired to do. An organization should do this with every third party they have engaged, creating a centralized repository for all identities and any associated access.

Depending on the third party and its responsibility to the organization, it will be granted a certain amount of access into the network, which should be transparent to the organization for granular control and visibility into a third party's activity.

Unfortunately, this isn't the case for most. Many organizations do not know all the third parties with access to their networks and lack visibility into the level of access and permissions for both internal and external users. In fact, **65% of respondents have not identified the third parties with access to the most sensitive data of the organization**[9], leaving the door for access to an organization's private information wide open for intruders.

Imagine you decide to throw a dinner party with a small, exclusive group of friends. Seems harmless, right? But what if each person separately decided to invite ten other people? Then those people also each invited ten people to the dinner party. Not so harmless anymore. On the night of your party, you'll have no insight as to who is attending and where in your house they might end up. Doors are left open and unlocked, and your entire home is vulnerable to guests you may or may not know or trust. Without prior knowledge of who will be there, you don't know how much of your home to make available and more importantly, what areas to block off. The same is true for third-party remote access - leaving those doors (access points) unmonitored, unidentified, and unmanaged leaves them unlocked and open to potential hackers that can make their way in and make a mess of an organization's network.

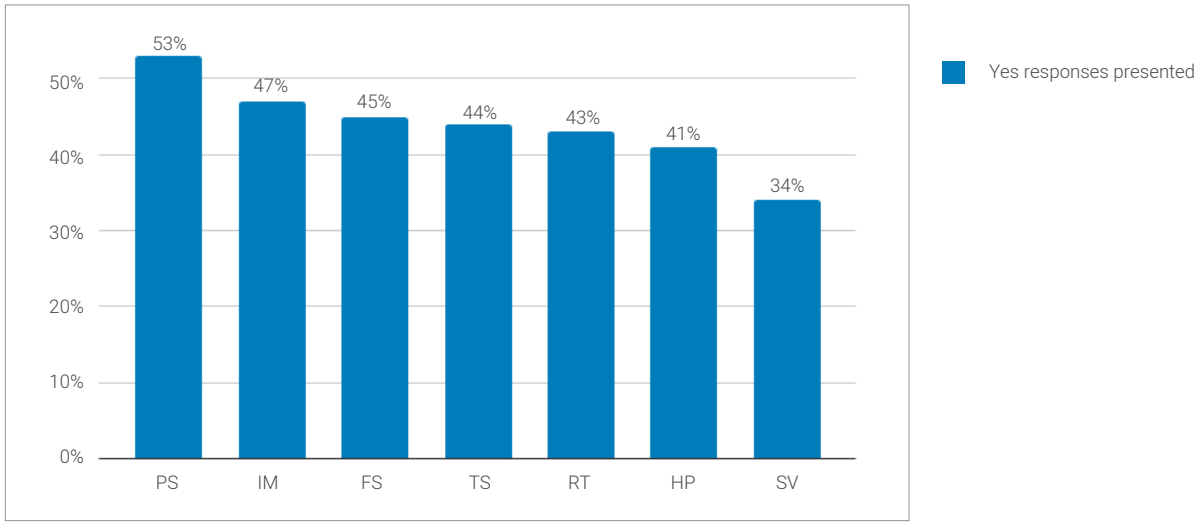


And for some organizations, the guest count is high. With the median number of third parties per organization landing between 251 and 500, it's troubling that 54% of respondents say their organizations do not have a comprehensive inventory of all third parties with access to their network.[10] When taking a look at some of the industries represented in the survey, most verticals lack complete visibility into third parties that have access to their networks: Only the public sector had more than half (53% of respondents) say they had a comprehensive inventory of third parties with access to critical systems. Just 47% of manufacturing respondents, 45% of financial services respondents, and 41% of healthcare respondents were able to claim such visibility.[11]

When it comes to third-party remote access risk, these findings support the notion that it's never too early to ensure security protocols, visibility, and management of network permissions. The more prepared an organization is in these first stages, the more it will reap the rewards of network security and protection from hackers. And although this greatly contributes to overall third-party remote access security, this still does not secure the riskiest stage of third-party management. Let's take a look at secure connection - the greatest point of risk in the third-party lifecycle.

> "It's troubling that 54% of respondents say their organizations do not have a comprehensive inventory of all third parties with access to their network."

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



SECURE CONNECTION

Protecting the network

The riskiest point in the third-party lifecycle is in the connectivity. This is the point where external third-party risk is actually introduced to the organization's network, systems, and information, and where cyberattackers often target. This is why access and connectivity are the most critical components to first and fully secure in the third-party lifecycle.

If it's not secured, then the worst can happen.

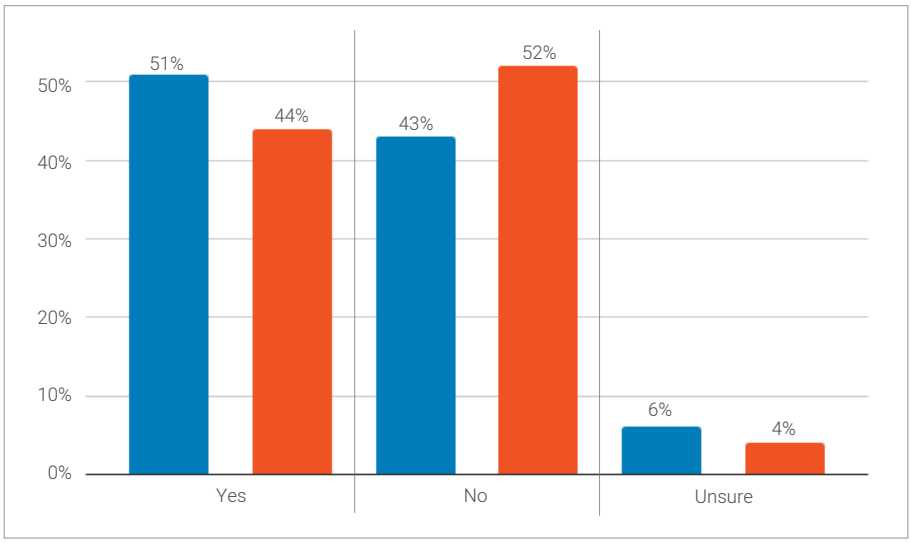
Over half of respondents have experienced a data breach caused by third parties that resulted in misuse of its sensitive or confidential information either directly or indirectly,[12] and 44% say their organization experienced one of these data breaches caused by a third party **in the last 12 months**.[12a]

What's the root cause of these data breaches that stem from "reputable" and "reliable" third parties?

74% of respondents say it was the result of giving too much privileged access to third parties.[12b] The biggest cause of a data breach is the amount of access a third party has to an organization's network.

To fully and adequately secure this integral part of the third-party lifecycle, organizations need to assess and evaluate their security and access protocols, starting with identifying and managing the third parties with access to their network. As stated earlier, 54% of respondents say their organizations do not have a comprehensive inventory of all third parties with access to their networks.[10] Moreover, an even larger number of respondents - 63% - say their organization doesn't have visibility into the level of access and permissions for both internal and external users,[13] leaving organizations in the dark as to who has access to their network, when they are in their network, and why they are in their network.

12. Data breaches caused by third parties with remote access



74%

of respondents say it was the result of giving too much privileged access to third parties

This seems to be a large commonality between respondents, which begs the question, "Why is it so hard to identify, track, and manage third parties and their permissions or levels of access?" The answer is quite simple and not so surprising - managing remote access to the network is overwhelming. In fact, 73% of respondents say managing third-party permissions and remote access is overwhelming and a drain on internal resources,[14] and the responsibility of owning third-party management is often ambiguous, with a plurality of 30% of respondents saying their organization's technical staff is responsible rather than management or executive-level staff[15]. As a consequence, 63% say remote access is becoming their organization's weakest attack surface.[16]

And it shows - 69% of respondents say that cybersecurity incidents involving third parties are increasing,[17] as evidenced in the number of data breaches caused by third parties that have already occurred over the past decade - Target, Marriott, Under Armour, GE, and social media platforms Instagram, YouTube, and TikTok to name a few. These are just a handful of dozens of attacks over the last ten years demonstrating an increasing and very real threat; however, the actions that could be taken to prevent potential hacks like these are largely ignored.

For example, one of the most effective and preventative measures an organization can take is implementing a Zero Trust model in their cybersecurity approach, which includes granting least privileged access via granular controls and permissions. However, 60% of respondents say their organizations are not able to provide third parties with just enough access to perform their designated responsibilities and nothing more.[18] And furthermore, 66% of respondents are not implementing least privileged access[19] - even though the leading cause of data breaches is granting too much privileged access to third parties.

Another Zero Trust approach organizations can easily implement is securing network credentials, but findings show that organizations (specifically 59% of respondents) are ineffective in preventing third parties from sharing usernames and passwords.[20]

And we thought the biggest cybersecurity concern was a password left on a sticky note.

At least sticky notes are visible - unlike the clear network visibility most organizations lack. If the worst were to happen, 64% of respondents lacked the confidence that third parties would notify their organization if they had a data breach involving their sensitive and confidential information,[21] and

> "Remote access is becoming their organization's weakest attack surface."

66%

of respondents are not implementing least privileged access - even though the leading cause of data breaches is granting too much privileged access to third parties

as a result, more data breaches could occur because of the lack of confidence that third parties would report an incident. Organizations cannot adequately rely on their third parties to notify them of incidents that affect an organization's network, and without proof of the third party's involvement, organizations can't keep them accountable and end up taking on the breach as their own, which, in worst case scenario, can lead to the demise of a company or its reputation.

This is where auditing comes in. With proper auditing capabilities, organizations can log each third party's activity during network sessions and track the source of any suspicious hacker activity. This also saves time on investigating or validating vendor activity.

Compliance is another area most organizations need to monitor, and third parties who offer specific services to organizations need to adhere to the compliance regulations instituted by the organization or their industry. But can organizations rely on third parties to meet those compliance requirements?

Not necessarily. On average, more than half of respondents (52%) do not believe that their third parties are aware of their industry's data breach reporting regulations,[8] and **over half of respondents (56%) gave a low rating of their third parties' effectiveness in achieving compliance with security and privacy regulations that affect their organization.**[22] This puts organizations at large risk for non-compliance with regulations.

In general, organizations are most vulnerable in the connectivity stage of the third-party lifecycle due to the lack of control, visibility, restriction, and compliance of their third-party vendors. For this reason, third-party remote access is increasingly becoming the weakest attack surface for an organization. Though there are some bright spots in the survey results - 49% are tracking and monitoring access to network resources and critical data and 45% are identifying and categorizing vendor access needs[19] - organizations do not feel confident in a third party's ability to limit the scope of what a bad actor could access through their remote access connection.

MONITOR AND ASSESS

Maintaining third-party security

Once a third party's network connectivity has been established, their activity must be monitored and assessed continuously, hence the name of the next stage of the third-party lifecycle. This seems like a best practice for organizations who engage with third parties for critical functions. However, 54% of organizations are not monitoring the security and privacy practices of third parties that they share sensitive or confidential information with on an ongoing basis.[23]

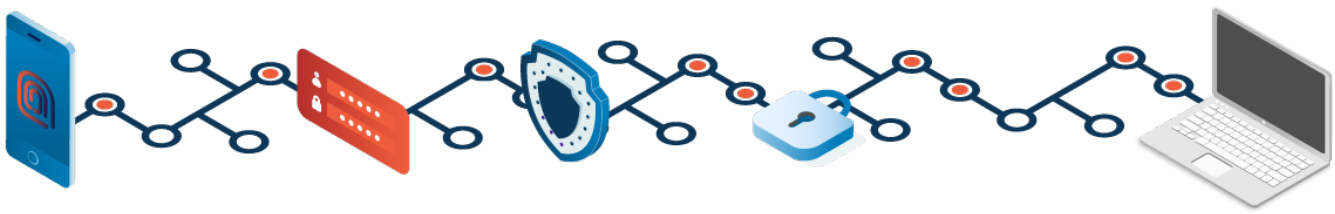
Many organizations are taking alternate routes to monitor third parties' privacy and security practices. 50% of respondents say their organizations depend on legal or procurement review for monitoring rather than automation.[24] 61% of respondents do not feel the need to monitor because of contracts put in place between the organization and the third party, with another 61% of respondents saying they rely on the business reputation of the third party as their reasoning not to monitor their privacy and security practices.[25]

59% of respondents do not use automated monitoring tools,[24] even though automation can improve the efficiency and accuracy of monitoring a third party's security practices while accessing an organization's network.

54%

of organizations are not monitoring the security and privacy practices of third parties that they share sensitive or confidential information with on an ongoing basis

This is concerning. **Contracts and reputation do not replace actual monitoring of real-time network activity, nor do they provide the insights needed to evaluate and assess current security practices.** Should something happen, organizations need to be able to swiftly address an incident without letting any security protocols fall through the cracks, and they have to be able to pivot their current privacy and security protocol based on the results of the incident. This is why establishing proper monitoring and evaluating procedures is critical to third-party management. With a reliable system in place, organizations can quickly and proactively respond to anomalies, incidents, and threats via the third-party route.



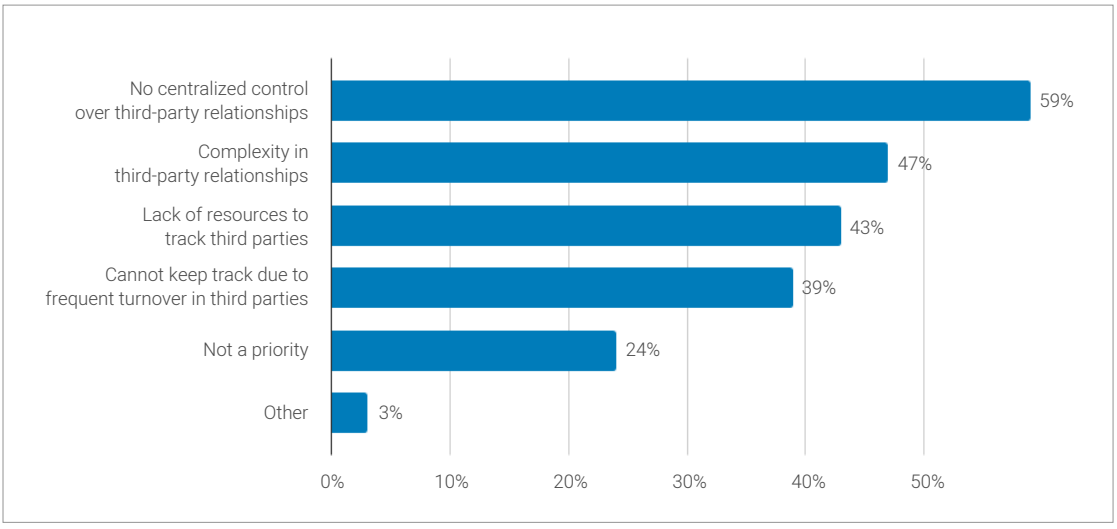
REPORT AND MANAGE

Centralizing responsibility

The last stage of the third-party lifecycle is reporting and ongoing management of a third party. While this is the final stage, there is no hard stop in the lifecycle here. Just like how third parties need to be continuously assessed and monitored for their security practices, their network activity and compliance needs to be continuously reported and managed to ensure those practices are put in place.

This area of the lifecycle remains blurry due to the majority of respondents saying their organizations see third-party management as overwhelming and a drain on internal resources (as previously referenced). Furthermore, **59% of respondents say there is no centralized control over third parties, and 47% say it's due to the complexity in third-party relationships.**[10a] Without centralized control and management, these complex relationships become difficult to report on and manage on an ongoing basis. In addition, many organizations have compliance requirements they need to adhere to, and reporting and monitoring compliance becomes difficult and burdensome without addressing these essential elements. Establishing reporting and management protocols might take time upfront, but will be well worth the effort of eliminating cyberthreats that come from third-party remote access.

10a. Why does your organization not have a comprehensive inventory of all third parties with access to its network?



Conclusion

The adoption of emerging technologies allows organizations to expand their business value and operate at high levels, especially when this entails engaging third-party vendors to increase productivity. While this trend of rapid innovation boosts the potential for growth, it also introduces serious cybersecurity challenges and threats to an organization's infrastructure.

The findings of this report showcase the crisis within third-party management, specifically within the six stages of the third-party lifecycle. It also reveals the alarming disconnect between an organization's perceived third-party access threat and the security measures it employs. Despite less than half of respondents (48%) having confidence in their third parties' ability to secure sensitive information,[3] organizations primarily rely on a third party's reputation as a substitute for due diligence and monitoring. Furthermore, 51% of respondents that experienced a recent data breach point to unchecked third-party privileged access as the cause,[12] and an even larger 66% are not implementing least privileged access[19] - a practice that could mitigate a threat at the greatest point of risk in the third-party lifecycle.

Even in sectors with high third-party risk like healthcare and finance, fewer than half of respondents in these industries say their organization has a comprehensive inventory of third parties with network access.[11]

The report provides organizations with a clear starting point as it highlights the most common gaps in third-party security. The solution lies within eliminating many of these common oversights and poor third-party security practices that can lead to data exposure and regulatory breaches. Organizations looking to improve the security of their third-party remote access programs can start by prioritizing network transparency, enforcing least privilege (or Zero Trust) access, and constantly evaluating existing third-party security practices to ensure they meet the evolving threat.

PRIORITIZING NETWORK TRANSPARENCY

Organizations with the goal of updating their cybersecurity practices and procedures need to make network transparency a top priority. Less than half of survey respondents say their organization has a comprehensive inventory of all third parties with permitted network access (46%),[10] and a whopping

63% of respondents say their organizations don't have any visibility into levels of access and permissions for all users.[13] Using a system that is purposefully built for managing third-party identities and their associated network access and permissions can significantly mitigate the risk associated with unmonitored third-party remote access.

By prioritizing third-party identity management, organizations know who is accessing their network, what they are accessing, and when they are accessing it. For the 61% of respondents who say they do not know the type of access their third parties have,[9] an identity management solution can offer full visibility of each third party's network activity and permissions.

Successful identity management should also consist of a comprehensive log of each vendor (and vendor rep) accessing an organization's network, monitored or recorded network sessions for clear insights into each third party's network activity, and a comprehensive audit trail. This visibility and transparency within the product stem from a Zero Trust approach that ensures organizational network protection.

ZERO TRUST NETWORK ACCESS

60% of respondents say their organizations are unable to provide third parties with only enough access to do their jobs and nothing more.[18] With over half of survey participants saying their organizations have experienced a data breach caused by a third party,[12] zero trust network access needs to be implemented for network safety.

Zero Trust network access operates off the principle of **"never trust - always verify."** Rather than providing access based on reputation and assumed credibility, a remote access solution needs to implement least privileged access and a verification process of each individual user every time network access is requested. This should also include secure authentication methods such as multi-factor authentication and masked credential injection. Only 40% of respondents said multi-factor authentication is "very important,"[26] showing that this essential security measure is undervalued. MFA's advanced verification ensures only authorized personnel gain access using their individual credentials.

Privileged access management (PAM) solutions, though typically used for internal employee privileged access and to vault organizational credentials, should also integrate with remote access security solutions. While integrated, the PAM solution keeps credentials masked once it permits access to third-party reps, so usernames and passwords are never exposed or shared externally, giving organizations more network control and more peace of mind.

EVALUATING THIRD-PARTY SECURITY PRACTICES

Some of the findings in this report revealed obsolete or non-existent practices for managing third-party security. This starts with the centralization of organizational responsibility for third-party security protocols, i.e., transferring the third-party monitoring obligations from the legal and procurement departments to information security and technology departments.

However, for these overburdened teams, third-party management can seem unappealing. Respondents averaged a median of 251-500 third-party vendors each, creating an entirely new workflow for already-exhausted IT departments. A solution that will help automate and streamline these processes, as well as provide network visibility, access, and compliance and risk management, offers much-needed relief to information security and technology teams.

> "An organization's attack surface is growing just as quickly as its third-party ecosystem and organizations must acknowledge this ever-changing threat landscape."

An organization's attack surface is growing just as quickly as its third-party ecosystem and organizations must acknowledge this ever-changing threat landscape. Given that 59 percent of respondents gave their organizations a low rating for their effectiveness to mitigate third-party remote access risks,[27] it's urgent that organizations adopt new ways of managing third-party remote access and the risk associated with external connectivity. By deploying a comprehensive third-party security solution, organizations can start prioritizing best practices such as complete network visibility, identification of third parties, zero trust network access policies, and regular assessing of compliant security practices, all of which secure the various stages of the third-party lifecycle, mitigate exposure, and increase organizational resilience.

About SecureLink

Headquartered in Austin, Texas, SecureLink is the leader in third party security, providing secure third-party remote access for both highly regulated enterprise organizations and technology vendors. SecureLink solves and secures the greatest point of risk in the third-party lifecycle for more than 30,000 organizations worldwide, providing companies across multiple industries, including healthcare, manufacturing, government, legal, and gaming, with secure remote access with identity management, access controls, audit, and compliance assurance.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in December 2020.

Survey Response	FREQ	PCT%
Total sampling frame	16,744	100%
Total returns	672	4%
Rejected surveys	45	0.3%
Final sample	627	3.7%

SCREENING QUESTIONS

S1. How familiar are you with your organization's approach to managing remote third-party data risks?	PCT%
Very familiar	40%
Familiar	34%
Somewhat familiar	26%
No knowledge (Stop)	0%
Total	100%

S2. Do you have any involvement in managing third-party data risks created by remote access?	PCT%
Yes, full involvement	38%
Yes, partial involvement	45%
Yes, minimal involvement	17%
No involvement (Stop)	0%
Total	100%

S3. Does your company have a third-party data risk management program?	PCT%
Yes	100%
No (Stop)	0%
Total	100%

REPORT CITATIONS

1. Do you evaluate the security and privacy practices of all third parties before you engage them in a business relationship that requires providing access to sensitive or confidential information?	PCT%
Yes	49%
No (please skip to Q22c)	46%
Unsure (please skip to Q23)	5%
Total	100%

2. If yes, how do you perform this evaluation? Please check all that apply.	PCT%
Review written policies and procedures	49%
Acquire signature on contracts that legally obligates the third party to adhere to security and privacy practices	59%
Obtain indemnification from the third party in the event of a data breach	33%
Conduct an assessment of the third party's security and privacy practices	39%
Obtain a self-assessment conducted by the third party	42%
Obtain references from other organizations that engage the third party	34%
Obtain evidence of security certification such as ISO 2700/27002 or SOC.	51%
Other (please specify)	4%
Total	311%

3. If no, why don't you perform an evaluation? Please check all that apply.	PCT%
We don't have the internal resources to check or verify	56%
We have confidence in the third party's ability to secure information	48%
We rely on the business reputation of the third-party	63%
We have insurance that limits our liability in the event of a data breach	52%
The third party is subject to data protection regulations that are intended to protect our information	60%
The third party is subject to contractual terms	59%
The data shared with the third party is not considered sensitive or confidential	26%
Other (please specify)	3%
Unsure	5%
Total	372%

5. What percentage of your third parties do you require to fill out security questionnaires?	PCT%
None	30%
Less than 10%	8%
11% to 20%	10%
21% to 50%	8%
51% to 75%	14%
More than 75%	25%
Unsure	5%
Total	100%
Extrapolated value	35%

6. What percentage of your third parties do you require to conduct remote or on-site assessments?	PCT%
None	39%
Less than 10%	12%
11% to 20%	9%
21% to 50%	7%
51% to 75%	13%
More than 75%	16%
Unsure	4%
Total	100%
Extrapolated value	26%

7. Does your third-party management program define and rank levels of risk?	PCT%
Yes	39%
No	58%
Unsure	3%
Total	100%

If yes, what are indicators of risk? Please check all that apply.	PCT%
Failed IT security audits, verification or testing procedures	46%
Overall decline in the quality of the third party's services	41%
Discovery that the third party is using a subcontractor that has access to our company's information	37%
Complaints from customers about privacy or security	29%
History of frequent data breach incidents	55%
Legal actions against the third party	40%
Negative media about the third party	39%
IT glitches, operational failures and stoppages	50%
Poorly written security and privacy policies and procedures	61%
Lack of security or privacy training for the third party's key personnel	42%
Lack of screening or background checks for key personnel hired by the third party	60%
High rate of identity fraud, theft or other cybercrimes within the third party's home country	42%
Lack of data protection regulation within the third party's home country	23%
Turnover of the third party's key personnel	50%
Outdated IT systems and equipment	46%
Other (please specify)	4%
Total	665%

If yes, how often are the risk levels updated?	PCT%
Never	26%
As needed	34%
Every six months	12%
Annually	17%
Every two years	6%
Unsure	5%
Total	100%

8. What percentage of your third parties are aware of your industry's data breach reporting regulations?	PCT%
0% (none are aware)	2%
Less than 5%	6%
5% to 10%	9%
11% to 25%	13%
26% to 50%	20%
51% to 75%	24%
75% to 100% (all are aware)	26%
Total	100%
Extrapolated value	48%

9. Does your organization collect and document any of the following information about its third parties? Please select all that apply.	PCT%
Relevant and up-to-date contact information for each vendor	86%
The type of network access they have	39%
Identification of third parties that have the most sensitive data	35%
Confirmation that basic security protocols are in-place	32%
Confirmation that specific security practices are in place (i.e. firewalls, employee security training, pen testing, etc.)	36%
Past and/or current known vulnerabilities in hardware or software	31%
Other (please specify)	3%
Total	262%

10. Does your organization have a comprehensive inventory of all third parties with access to its network?	PCT%
Yes (proceed to Q5)	46%
No	50%
Unsure	4%
Total	100%

10a. If no or unsure, why? Please check all that apply	PCT%
Lack of resources to track third parties	43%
No centralized control over third-party relationships	59%
Complexity in third-party relationships	47%
Cannot keep track due to frequent turnover in third parties	39%
Not a priority	24%
Other (please specify)	3%
Total	215%

11. How many third parties are in your organization's inventory?	PCT%
Less than 10	0%
11 to 50	3%
51 to 100	6%
101 to 250	11%
251 to 500	12%
501 to 1,000	13%
1,001 to 2,500	19%
2,501 to 5,000	13%
More than 5,000	23%
Total	100%
Extrapolated value	2,368

12. 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?	PCT%
Yes	51%
No	43%
Unsure	6%
Total	100%

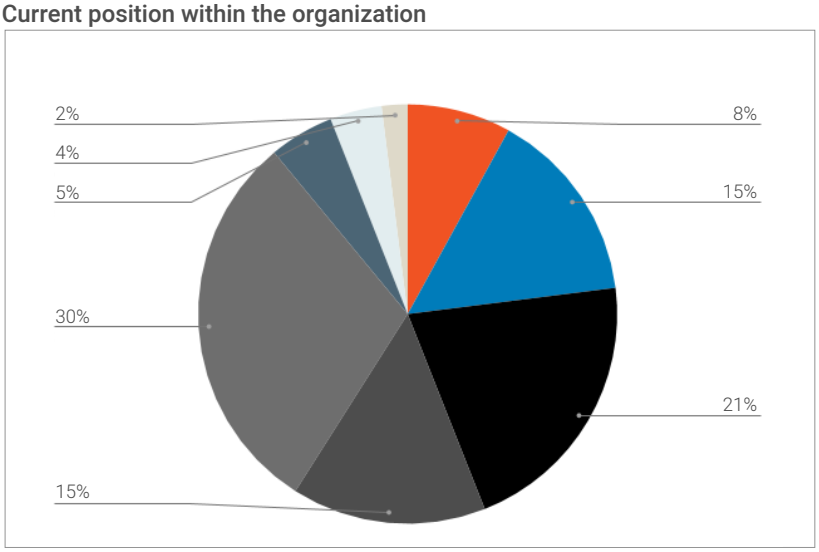
12a. In the past 12 months, has your organization experienced a data breach caused by one of your third parties, either directly or indirectly?	PCT%
Yes	44%
No	52%
Unsure	4%
Total	100%

12b. If yes, did any of these breaches result from giving too much privileged access to your third parties?	PCT%
Yes	74%
No	23%
Unsure	6%
Total	103%

	PCT%
13. Strongly agree and agree combined: Our organization has visibility into the level of access and permissions both internal and external users have.	37%
14. Strongly agree and agree combined: Managing third-party permissions and remote access to our network can be overwhelming and a drain on our internal resources.	73%

15. A final sampling frame of 627 individuals who have some level of involvement in their organization's approach to managing third-party remote access risks were selected as participants to this survey. This pie chart reports the respondent's seniority within the participating organizations. By design, more than half (59%) of respondents are at or above the supervisory levels. The largest category, at 30% of respondents, is technical staff.

Current position within the organization



	PCT%
16. Strongly agree and agree combined: Third parties' remote access to our network is becoming our organization's weakest attack surface.	63%
17. Strongly agree and agree combined: The number of cybersecurity incidents and data breaches involving third parties is increasing.	69%
18. Strongly agree and agree combined: Our organization is able to provide third parties with just enough access to perform their designated responsibilities and nothing more.	40%

19. To ensure third parties' compliance with privacy and security regulations, does your organization take any of the following steps? Please check all that apply.	PCT%
Identify and categorize third-party vendor and partner access needs	45%
Perform access assessments for each vendor and partner	41%
No vendor-supplied security parameters or default passwords	38%
Implement least privileged access	34%
Insist on unique user access credentials	52%
Encrypt transmissions for all open or public networks	56%
Track and monitor all access to network resources and critical data	49%
Capture detailed audit logs of each support session	55%
Install and maintain a firewall configuration to protect data	46%
Develop secure application and system implementation	45%
Protect all systems against malware and regularly monitor anti-virus protections	50%
Restrict physical access	48%
Other (please specify)	5%
Total	564%

20. Using the following 10-point scale, please rate your organization's effectiveness in preventing third parties from sharing credentials in the form of usernames and/or passwords. 1 = not effective to 10 = highly effective)	PCT%
1 or 2	20%
3 or 4	23%
5 or 6	16%
7 or 8	21%
9 or 10	20%
Total	100%
Extrapolated value	5.46

21. How confident are you that third parties would notify your organization if they had a data breach involving your sensitive and confidential information? (1 = not confident to 10 = highly confident)	PCT%
1 or 2	26%
3 or 4	21%
5 or 6	17%
7 or 8	21%
9 or 10	15%
Total	100%
Extrapolated value	5.06

22. Using the following 10-point scale, please rate the effectiveness of your third parties in achieving compliance with security and privacy regulations that affect your organization. 1 = not effective to 10 = highly effective)	PCT%
1 or 2	18%
3 or 4	22%
5 or 6	16%
7 or 8	20%
9 or 10	24%
Total	100%
Extrapolated value	5.70

23. Do you monitor the security and privacy practices of third parties that you share sensitive or confidential information with on an ongoing basis?	PCT%
Yes	46%
No	51%
Unsure	3%
Total	100%

24. If yes, what monitoring procedures does your organization employ to ensure the adequacy of security and privacy practices? Please check all that apply.	PCT%
Legal or procurement review	50%
Independent audit or verification by a third party	38%
Automated monitoring tools	41%
Random tests or spot checks	38%
Annual self-certification	40%
Use of security ratings firms	38%
Other (please specify)	3%
Total	248%

25. If no, why doesn't your organization monitor the third parties' security and privacy practices? Please check all that apply.	PCT%
We don't have the internal resources to check or verify	54%
We have confidence in the third party's ability to secure information	47%
We rely on the business reputation of the third party	61%
We have insurance that limits our liability in the event of a data breach	50%
The third party is subject to data protection regulations that are intended to protect our information	59%
The third party is subject to contractual terms	61%
The data shared with the third party is not considered sensitive or confidential	30%
The third party will not allow us to independently monitor or verify their security and privacy activities	23%
Other (please specify)	3%
Total	388%

26. How important is the use of multi-factor authentication that includes industry standards such as time-based one-time passwords (TOTP) 1 = not important to 10 = very important)	PCT%
1 or 2	8%
3 or 4	11%
5 or 6	16%
7 or 8	25%
9 or 10	40%
Total	100%
Extrapolated value	7.06

27. Using the following 10-point scale, please rate how effective your organization is in mitigating remote access third-party risks. (1 = not effective to 10 = highly effective)	PCT%
1 or 2	20%
3 or 4	24%
5 or 6	15%
7 or 8	21%
9 or 10	20%
Total	100%
Extrapolated value	5.44

Additional Findings

	PCT%
Strongly agree and agree combined: My organization requires the assessment of third-party risks associated with having access to its network, including SaaS systems and/or cloud infrastructure.	67%
Strongly agree and agree combined: My organization's IT/IT security function makes ensuring the security of third parties' remote access to its network a priority.	51%

Using the following 10-point scale, please rate how effective your organization is in detecting remote access third-party risks. (1 = not effective to 10 = highly effective)	**PCT%**
1 or 2	19%
3 or 4	14%
5 or 6	15%
7 or 8	20%
9 or 10	32%
Total	100%
Extrapolated value	6.14

Using the following 10-point scale, please rate your organization's effectiveness in responding to a third-party incident. (1 = not effective to 10 = highly effective)	**PCT%**
1 or 2	11%
3 or 4	21%
5 or 6	15%
7 or 8	23%
9 or 10	30%
Total	100%
Extrapolated value	6.30

Using the following 10-point scale, please rate the effectiveness of your organization's third-party risk management program. (1 = not effective to 10 = highly effective)	PCT%
1 or 2	12%
3 or 4	18%
5 or 6	20%
7 or 8	20%
9 or 10	30%
Total	100%
Extrapolated value	6.26

Using the following 10-point scale, please rate the effectiveness of knowing all third-party concurrent users. (1 = not effective to 10 = highly effective)	PCT%
1 or 2	11%
3 or 4	21%
5 or 6	18%
7 or 8	27%
9 or 10	23%
Total	100%
Extrapolated value	6.10

Using the following 10-point scale, please rate the effectiveness of your organization in controlling third-party access to your network. 1 = not effective to 10 = highly effective)	PCT%
1 or 2	15%
3 or 4	19%
5 or 6	25%
7 or 8	21%
9 or 10	20%
Total	100%
Extrapolated value	5.74

Who is most accountable for the correct handling of your organization's third-party risk management program?	PCT%
General counsel/compliance officer	8%
Chief technology officer (CTO)	9%
Chief information officer (CIO)	21%
Chief information security officer (CISO)	19%
Chief security officer (CSO)	3%
Head of business continuity management	2%
Chief privacy officer (CPO)	0%
Data protection officer (DPO)	0%
Head of human resources	1%
Head of procurement	3%
Chief risk officer (CRO)	15%
No one person/department is accountable	19%
Unsure	0%
Total	100%

What information security control standard(s) is your organization required to comply with? Please check all that apply.	PCT%
NIST	41%
ISO 27001/27002	37%
PCI-DSS	44%
HIPAA/HiTrust CSF	30%
COBIT	39%
Other (please specify)	5%
Total	196%

Does your organization regularly report to the board of directors on the effectiveness of the third-party management program and potential risks to the organization?	PCT%
Yes	32%
No	63%
Unsure	5%
Total	100%

If no, why?	PCT%
Not a priority for the board	44%
Decisions about the third-party risk management program are not relevant to board members	41%
We only provide this information if a security incident or data breach has occurred involving a third party	50%
Other (please specify)	5%
Total	140%

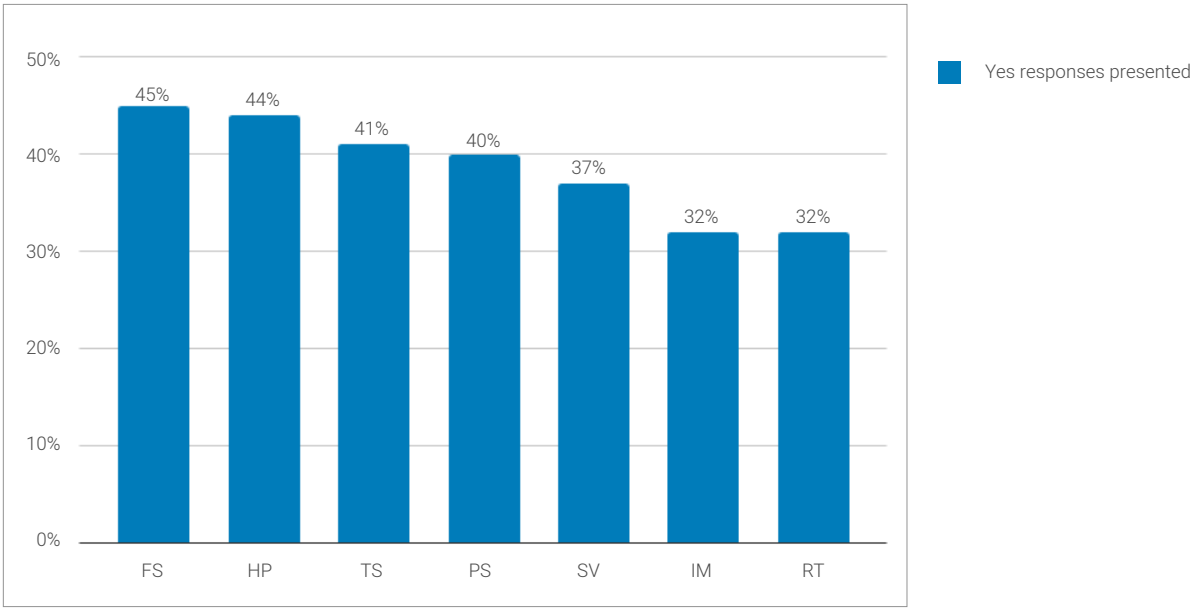
Does your organization report to the board of directors about potential risks created by third-party remote access?	PCT%
Yes	40%
No	60%
Total	100%

INDUSTRY DIFFERENCES

This section presents the differences among the following industries: Financial services (FS 113 respondents), health and pharma (HP 69 respondents), public sector (PS 63 respondents), services (SV 64 respondents), industrial and manufacturing (IM 56 respondents), retail (RT 56 respondents) and tech and software (TS 56 respondents).

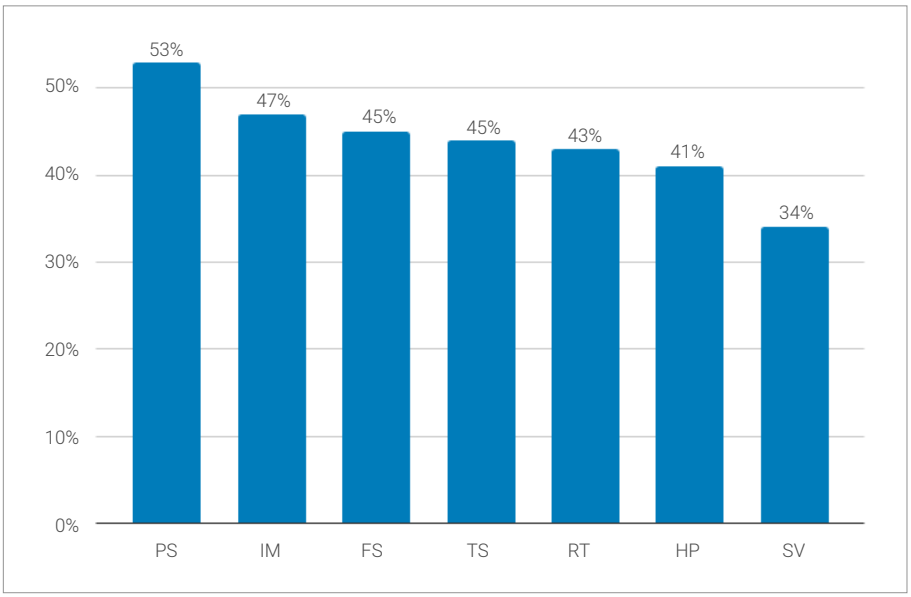
Healthcare and financial organizations are more likely to have a data breach caused by a third party. As shown in the chart, 45% of respondents in financial services and 44% of respondents in healthcare and pharma say their organizations either directly or indirectly experienced a data breach caused by one of their third parties. Fewer organizations in industrial manufacturing and retail had such a data breach.

In the past 12 months has your organization experienced a data breach caused by one of your third parties, either directly or indirectly?

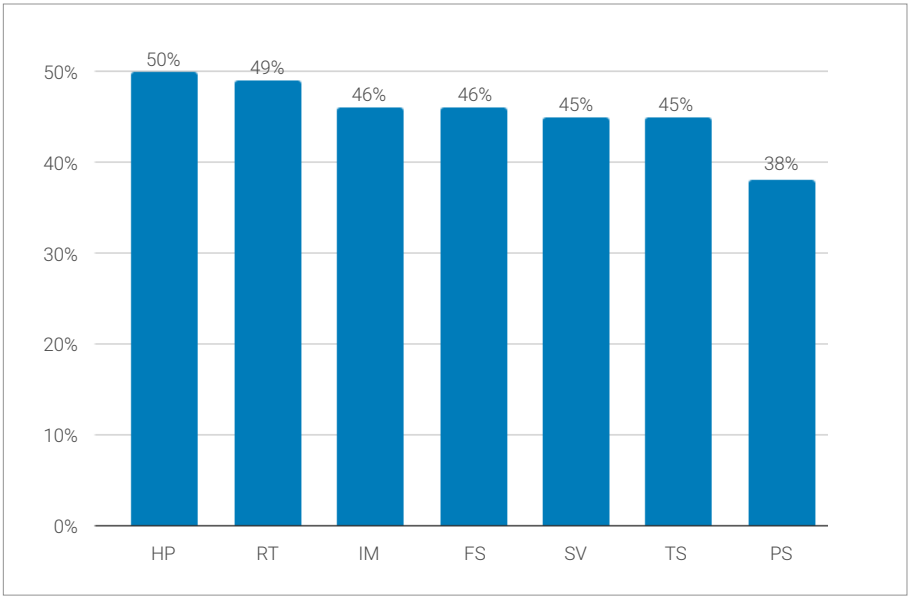


Only the public sector had more than half (53% of respondents) say they had a comprehensive inventory of third parties with access to critical systems.

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

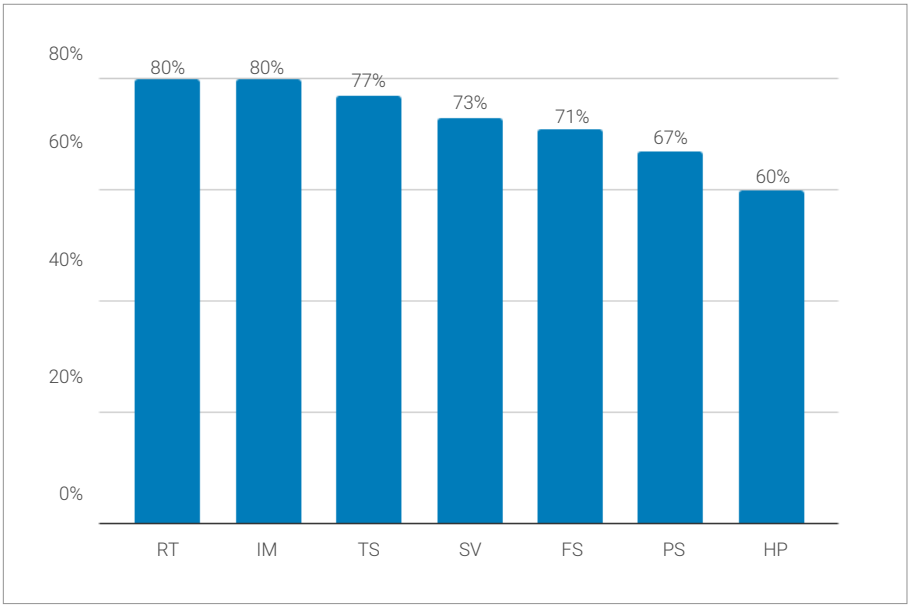


My organization's IT/IT security function makes ensuring the security of third-parties remote access to its network a priority



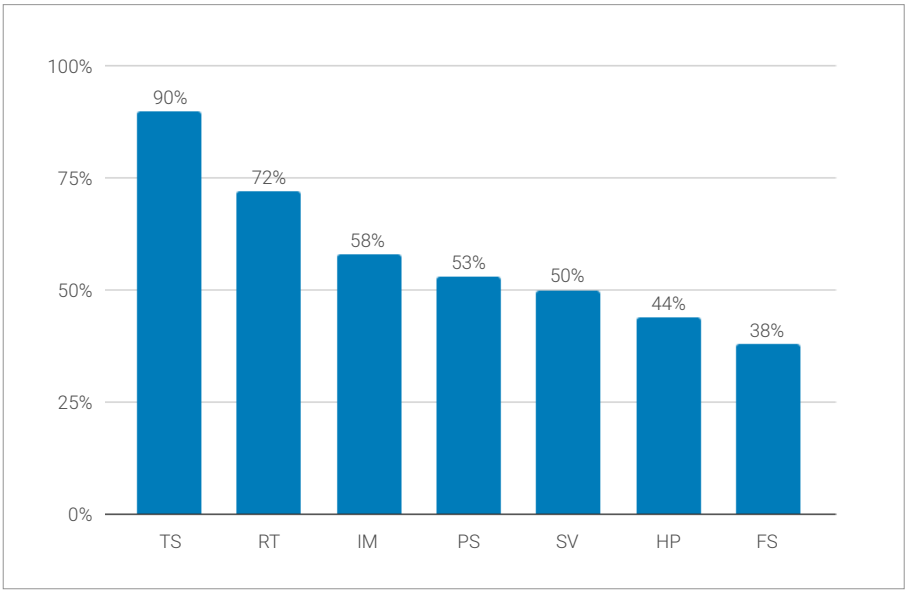
Retail and industrial manufacturing industries are more likely to have problems managing third-party permissions.

Managing third-party permissions and remote access to our network can be overwhelming and a drain on our internal resources



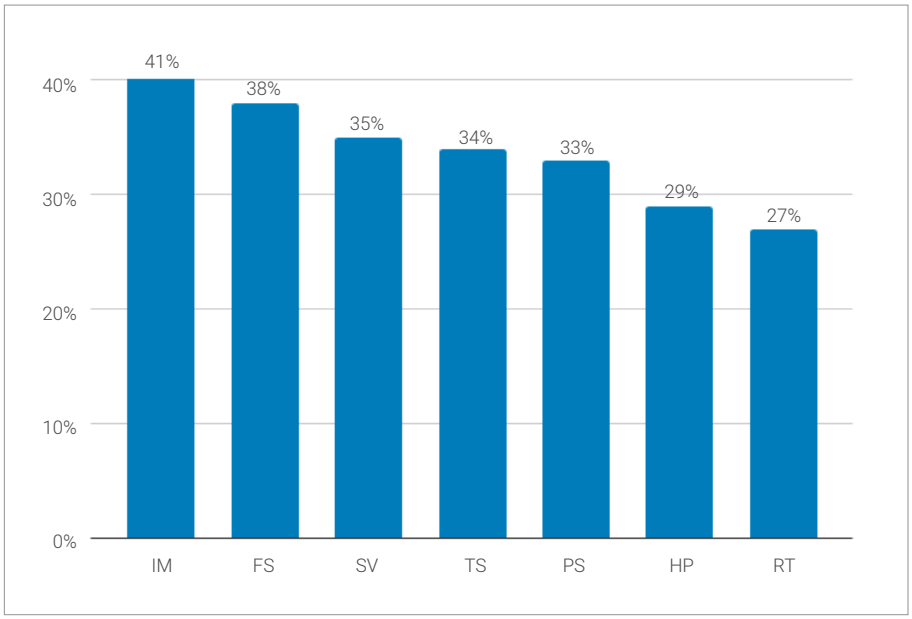
Technology and software industries have high visibility (90% of respondents) into both internal and external users' level of access and permissions. According to the chart, in contrast, healthcare and pharma (44% of respondents) and financial services (38% of respondents) have the least visibility.

Our organization has visibility into the level of access and permissions both internal and external users have



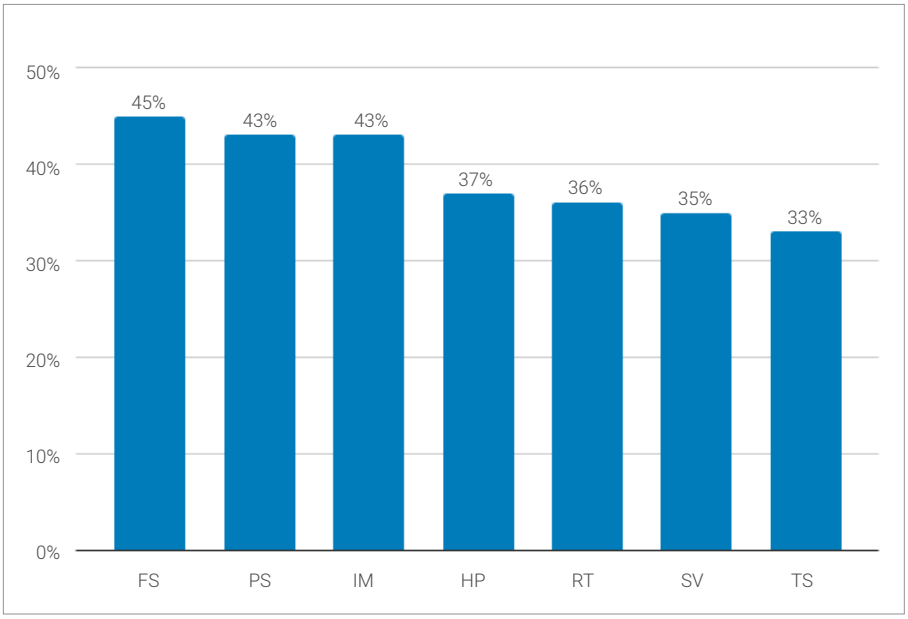
Few respondents say they regularly report to the board of directors on the effectiveness of their third-party management program and potential risks. Industrial manufacturing (41% of respondents) are most likely to regularly report.

Does your organization regularly report to the board of directors on the effectiveness of the third-party management program and potential risks to the organization?



If they do report to the board of directors, 45% of respondents in financial services say they do present the potential risks created by third-party remote access.

Does your organization report to the board of directors about potential risks created by third-party remote access?



DEMOGRAPHICS AND ORGANIZATIONAL CHARACTERISTICS

What organizational level best describes your current position?	PCT%
Senior executive/VP	8%
Director	15%
Manager	21%
Supervisor	15%
Technician	30%
Staff	5%
Contractor	4%
Other	2%
Total	100%

Check the Primary Person you report to within the organization.	PCT%
CEO/executive committee	7%
Chief financial Officer	2%
General counsel	4%
Chief information security officer	19%
Chief privacy officer	1%
Chief information officer	37%
Compliance officer	8%
Chief technology officer	7%
Human resources VP	1%
Chief security officer	3%
Chief risk officer	8%
Other	3%
Total	100%

What industry best describes your organization's industry focus?	PCT%
Financial services	18%
Health and pharmaceutical	11%
Public service	10%
Services	10%
Industrial and manufacturing	9%
Retailing	9%
Technology and software	9%
Energy and utilities	5%
Communications	3%
Education and research	3%
Entertainment and media	3%
Hospitality	3%
Transportation	2%
Agriculture and food services	1%
Defense and aerospace	1%
Other (please specify)	3%
Total	100%

What is the worldwide headcount of your organization?	PCT%
Less than 500 people	12%
501 to 1,000 people	23%
1,001 to 5,000 people	23%
5,001 to 25,000 people	21%
25,001 to 75,000 people	13%
More than 75,000 people	8%
Total	100%

CAVEATS TO THIS STUDY

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who have some level of involvement in their organization's approach to managing remote third-party data risks. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Please contact research@ponemon.org or
call us at 800.887.3118 if you have any questions.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high-quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.