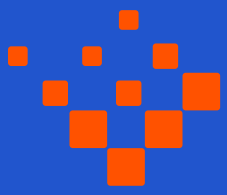
SecureLink®

Ponemon INSTITUTE



A Matter of Life and Death: The State of Critical Access Management in Healthcare

A deep dive into the critical condition of healthcare's third-party security ecosystem

Sponsored by SecureLink | Independently conducted by Ponemon Institute LLC

A Letter from SecureLink Chief Data Scientist Dan Fabbri

SolarWinds. Colonial Pipeline. Kaseya. Codecov. These companies have one thing in common: They've each faced devastating high-profile software breaches over the past year. Attacks by third parties—including both contracted vendors and unknown outside attackers—are on the rise across industries. And healthcare is no exception.

Most remote access in healthcare organizations comes from users with good intentions—but there is always a threat from valid users who are misbehaving, or worse, attackers who have gained access to compromised accounts. Now is a pivotal moment for improving critical access management, which is a vital step in monitoring and securing third-party access. In this report, you'll not only learn why the risk posed by third parties is particularly high, but you'll also learn how to protect your organization's data.

Compared to other industries, the healthcare sector suffers four times more cyber attacks. And during the pandemic, some analysts noted a 55% increase in healthcare data breaches, impacting the health information of an estimated 26 million people in the United States. Given that data breaches can ultimately shut down entire healthcare systems and compromise patient care, cyber attacks in this sector can truly be a matter of life and death.

Increasingly, industries like healthcare are adopting emerging technologies to expand and evolve their organizations so they can meet the healthcare needs of their growing communities, especially during the pandemic. But building their network of partners is also contributing to a critical access management challenge. It's clear there's an alarming disconnect between how an organization perceives a third-party threat and the actual reality of dangerous third-party access threats, as evidenced in the scarce security measures organizations employ. According to our report on the state of third-party remote access security, released earlier this year, 44% of respondents in healthcare and pharma said their organizations either directly or indirectly experienced a data breach caused by one of their third-party partners.

Managing user identities and identifying suspicious access—especially among third parties who don't have the same trusted relationships and security protocols as other parties, like internal employees—is one security measure where many healthcare organizations fall short. In our report, only 41% of healthcare respondents said they had a comprehensive inventory of third parties with access to critical systems, and fewer than half said they have visibility into the level of access and permissions that both internal and external users have. A user access review, in its most basic sense, reduces the capability for bad actors to try to access systems. And as we've seen, having unnecessarily open accounts makes organizations susceptible to attack.

People often compare securing critical access to credit card fraud monitoring, but in reality, the paradigm of how we monitor and assess threats in healthcare varies greatly from credit cards—and other industries. Credit card monitoring takes into account the time, location and value of a potentially fraudulent purchase. Meanwhile, healthcare organizations are composed of big, virtualized networks, with workers operating on rotating schedules and valuable patient information necessarily made available with a single click.

The goal of this report is to arm healthcare providers

with the information and tools to navigate the state of critical access management, mitigate future cyber attacks, and eliminate vulnerabilities that can threaten HIPAA and HITECH compliance. This isn't just about protecting a single healthcare organization's data. Rather, it's about safeguarding critical access to data belonging to patients, partners, and entire communities.

Today's resources are scaling up to match the magnitudes of the threats facing the healthcare industry. The first step is understanding the new reality of risk in critical access management in healthcare. We hope to help you begin that journey here.

Introduction: The Role of Critical Access Management in Healthcare

A closer look at the role critical assets and third parties play in the industry

Every organization has critical assets they need to protect, whether it's their networks, systems and infrastructure, applications, or data. For healthcare organizations, their most critical asset is patient data. Unfortunately, that's also the same prized possession so often targeted by hackers who sell the data—for a huge profit—on the black market. Malicious actors will therefore use whatever means they can to break into a healthcare network and claim their prize. On top of that, they've realized that healthcare providers are more likely to pay ransoms because attacks on healthcare IT systems often inhibit patient care. This also helps explain why ransomware attacks in healthcare are on the rise. In recent years, hackers have discovered that one of the most effective ways to breach a hospital network is through its third-party vendors.

As in other industries, third parties provide critical services for healthcare organizations. Encompassing everything from health insurance companies and medical equipment suppliers to website and email providers, these third-party vendors are often given access to highly sensitive patient data—including health insurance information and social security numbers. Naturally, that makes them an easy target for hackers determined to steal electronic medical records (EMR).

Furthermore, as healthcare organizations expand, so does their need for third parties in order to continue providing quality care. The pandemic has only accelerated the need for third-party services with hospitals requiring more equipment, higher production of supplies, more advanced technology and devices, and greater IT demands from at-home healthcare workers.

Of course, with healthcare organizations becoming more reliant on third parties, securing critical assets becomes increasingly imperative.

> "The value of medical records over the years continues to grow. Some organizations have pointed out that the value of the data stored in medical records is even more valuable than credit cards."
>
> **Dan Fabbri**
> Chief Data Scientist, SecureLink

Note: Many of the findings in this report were derived from a broader report on the state of third-party security conducted by Ponemon Institute and sponsored by SecureLink.

Securing Third-Party Access in Healthcare Can Actually Save Lives

The greatest cost of cyber attacks on healthcare organizations is the human cost

Cyber attacks in healthcare are problematic for myriad reasons, not least of which is the cost and headache they cause patients and hospitals trying to keep sensitive information and medical records private. But they can also quite literally become a matter of life or death with many healthcare data breaches ending in life-threatening consequences.

In August 2021, Indianapolis-based health care system Eskenazi Health fell victim to a ransomware attack that affected all of its locations across Marion County. The breach not only allowed threat actors to gain hold of patient data and leak it online, it forced Eskenazi Health to turn away ambulances and divert patients to other hospitals, revealing just how destructive cyber attacks in healthcare can be—especially during the COVID-19 pandemic, when patients need urgent medical care.

Unfortunately, what happened to Eskenazi Health is hardly an anomaly. Memorial Health System, which includes 64 hospitals and clinics, had to cancel surgeries and radiology treatments in its West Virginia and Ohio locations due to ransomware that shut off IT access to its medical systems. Sanford Health, one of the largest healthcare systems in Sioux Falls, South Dakota, was also the victim of a recent ransomware hack. While teams raced to recover its compromised network and restore service, Sanford, like Eskeanazi, had to divert ambulances to neighboring hospitals.

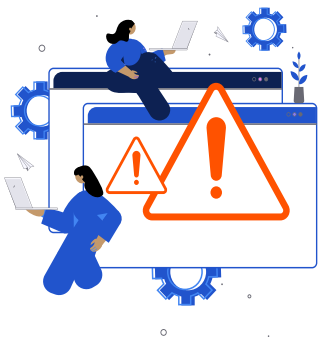
In the most extreme cases, these kinds of healthcare cyber attacks—and the downtime required to respond to them—can be fatal. A 2020 data breach of Düsseldorf University Hospital in Germany led to at least one death after the hospital turned away an ambulance carrying a patient in critical condition.

A survey by CyberMDX and Philips found that midsize hospitals shut down for an average of 10 hours at a rate of $45,700/hour when experiencing a data breach. What each of the examples above so clearly illustrates, however, is that the greatest cost of cyber attacks in healthcare is the human cost.

Third-Party Attacks in Healthcare Are on the Rise

The perfect storm of increasingly sophisticated supply chain cyber attacks and the COVID-19 pandemic have led to an uptick in third-party attacks on healthcare organizations

All industries have seen increasingly frequent and sophisticated supply chain cyber attacks—the Kayesa ransomware attack, the Colonial Pipeline breach, and the SolarWinds cyber attack being among the most high-profile examples. But this uptick in breaches has been even more prevalent among healthcare organizations.



In fact, the healthcare sector suffers four times more cyber attacks than other industries with medical breaches up 55% in 2020. In total, 2020 saw the infiltration of more than 29 million healthcare data records.

The reason for this is that the healthcare industry looks and operates differently than other industries. With vendors and third parties supplying most of the components that make up the healthcare provider ecosystem, the very structure of the healthcare industry creates a greater attack surface area for data breaches, ransomware, and remote takeover of medical devices. Over the past few years, hackers have identified third parties as a particularly good target for attacks across industries—and healthcare organizations have endless third parties to potentially exploit. Third parties also have the benefit of allowing threat actors to breach many healthcare organizations simultaneously. **In the last 12 months, 44% of healthcare and pharmaceutical organizations experienced a data breach caused by a third party.**

The COVID-19 pandemic has further increased the industry's reliance on digital health technology, ushering in welcome innovation while also further expanding the attack surface and leaving healthcare organizations even more susceptible to attacks. What's more, malicious actors took advantage of the pandemic draining hospital resources and attention to wage warfare on healthcare IT systems in pursuit of highly coveted electronic medical records.

Overwhelmed by the unprecedented surges of COVID-19 cases, many healthcare providers have understandably been focused on saving lives rather than reviewing their cybersecurity measures and securing critical access points. The result of this pandemic-induced shift in healthcare priorities has been a massive talent shortage in healthcare cybersecurity, as well as under-resourced and underfunded compliance teams. Naturally, it has also exacerbated existing healthcare vulnerabilities that hackers have worked for years to exploit. Already in 2021, 38 cyber attacks have disrupted services to 963 healthcare locations.

In the last 12 months,
44%
of healthcare and pharmaceutical organizations experienced a data breach caused by a third party.

When It Comes to Critical Access Management, Healthcare Faces Unique Challenges

Broad access rights and a lack of visibility increase the risk to healthcare organizations and sensitive patient health information

Though data breaches and other cybersecurity concerns aren't exactly new to the healthcare industry, the COVID-19 pandemic revealed just how vulnerable sensitive patient health information really is.

Unlike other industries, the healthcare industry faces a constant tradeoff: on one hand, there's the need for utility and easy access to data, and on the other, the

CASE STUDY

Transforming User Access Reviews: How SecureLink Helped LifePoint Health Raise the Bar for Accuracy and Efficiency

The problem

A healthcare network spanning 87 hospitals across the United States, LifePoint Health needed to review users' access rights across their data systems to satisfy auditing requirements. Due to LifePoint's scale and geographical dispersion, hundreds of thousands of rights needed to be reviewed. To make matters worse, due to recent M&A, LifePoint struggled with user and data mapping challenges throughout each system that also needed to be reviewed.

The solution

With SecureLink's Access Intelligence, LifePoint was able to not only efficiently include more people in the auditing process, but also bring in stakeholders who knew exactly how much access was right for them. This led to more thorough reviews and more accurate access permissions.

In one week, LifePoint and SecureLink were able to train 5,000 people on Access Intelligence. After the first quarter, support tickets dropped 70%. And, after the second quarter, 99% of reviewable access rights were completed.

need for privacy and security. Because minutes and seconds so often mean the difference between life and death in a place like a hospital, healthcare systems are often deployed with broader access rights, which allow physicians to access the data as soon as they need it. Imagine an ER doctor tending to a patient brought in with critical injuries from a car accident. She tries to access the patient's chart, but the information is blocked, and she's told to seek approval. Restricting access would, in this case, slow care and potentially cause patient harm. Unfortunately, attackers can leverage these broad access rights to gain access to a large amount of confidential data or applications, or even take control of an entire healthcare system.

In addition to the vulnerabilities created by broad access rights, healthcare organizations often lack visibility into which vendors have entry into their system. **Just 41% of healthcare and pharmaceutical organizations have a comprehensive inventory of all third parties with access to their network. And only 44% of healthcare and pharmaceutical organizations have visibility into the level of access and permissions that both internal and external users have.**

For healthcare providers, the stakes are high. The potential for a data breach poses tremendous compliance, reputational, and financial risks. HIPAA requires that these accesses be routinely audited, and healthcare organizations can face hefty fines for anything that slips through the cracks. As healthcare organizations weigh the benefits of investing in their cybersecurity defenses, they need to understand that failing to implement protocols around third parties and access management carries very real costs, not least of which are penalties and long-term damage to their reputation.

Scaling Critical Access for Third Parties in Healthcare Also Has Its Challenges

Implementing cybersecurity solutions for healthcare organizations comes with its own challenges

Although healthcare CIOs are well aware of the risks of third-party attacks, implementing a cost-effective solution can be overwhelming for them. **60% of healthcare and pharmaceutical organizations agree that managing third-party permissions and remote access to their network can be overwhelming and a drain on their internal resources.**

For one thing, auditing millions of healthcare system and electronic medical record accesses through traditional methods, such as manual reviews, is time consuming and prone to error. No one can faultlessly review each vendor's access permissions—especially when contracts frequently expire or renew and vendor roles change. The problem remains, however, that not vetting third parties on an ongoing basis puts patient data at risk.

What healthcare organizations can do is implement user access management systems, which automate the process of reviewing, monitoring, and auditing access rights for both internal employees and external vendors. Access management solutions not only streamline the process of managing third-party permissions, they also help secure critical access points. Even so, the cost and complexity of many proposed access management solutions can place a significant burden on healthcare IT budgets and personnel.

CASE STUDY

How SecureLink helped Arizona's North Country HealthCare improve security while scaling up

The problem

North Country HealthCare (NCHC), a non-profit serving 12 communities across northern Arizona, had a problem that afflicts healthcare organizations of all sizes. Julian Bowers, NCHC's systems administrator, was worried about each new vendor he'd set up with VPN access as NCHC rapidly expanded to meet community healthcare needs, leading to a small mountain of sticky notes with login credentials unsecured and sitting out in the open. He knew he needed to ensure third-party security but didn't know how.

The solution

Ultimately, Bowers and NCHC found a solution: They were able to secure VPN access by having vendors log into SecureLink instead of directly into NCHC's systems, reducing the risk of a third-party breach while streamlining North Country HealthCare's vendor management. No more shared VPN passwords, no more sticky notes, and an extra layer of additional security with more complex passwords.

Conclusion: Remedying Critical Access Management in Healthcare Is Vital

Finding the right solutions to protect from third-party cyber attacks has never been more important

What this report reveals is that the healthcare industry faces elevated risk to its critical assets, including patient data, because of third-party access—and supply chain attacks in healthcare have truly dire consequences compared to other industries. We've also learned that healthcare cyber attacks are on the rise and will likely become even more frequent and severe. With that in mind, it's imperative that healthcare organizations secure their critical access points immediately.

To begin the process of securing critical access points, healthcare organizations must limit network and user access across applications. This includes implementing zero trust network access, monitoring application access, and regularly reviewing access rights among users and vendors using the three pillars of critical access management: access governance, access controls, and access monitoring.

ACCESS GOVERNANCE

Access governance describes the systems and processes put in place to ensure access policy is adhered to as closely as possible. For healthcare organizations, this means adopting the principle of least privilege, which grants users access only to the information and applications required to do their job and nothing more.

Identity governance solutions offer three primary benefits: adherence to the principle of least privilege, resulting in lower overall risk of access being used in a nefarious manner; employee productivity, by ensuring employees have the access required to do their job effectively and efficiently; and adherence to regulatory requirements and audits that often require organizations to demonstrate strong governance processes, especially for sensitive data and systems.

As we've already discussed, healthcare networks today are complicated and constantly face trade-offs between privacy and security. If you log into your bank, for example, you can only access your bank account. But the dynamic nature of healthcare creates an environment of broad access rights, in which authenticated individuals can log in and accessany patient information they need, often for life-saving reasons.

At the same time, broad access rights make way for bad actors to misuse access for nefarious or inappropriate reasons. The access governance practice of user access review, then, becomes imperative, particularly in large healthcare organizations. Furthermore, HIPAA and HITRUST certifications require that healthcare organizations implement procedures to determine that access to electronic protected health information (ePHI) is appropriate and establish a process to terminate access to ePHI when it is no longer needed. User access reviews inventory the access rights of users and delegate reviews to a staff member's respective manager so they can approve or reject the access right, triggering an automatic ticket to the IT team to modify access accordingly. From both a security and compliance perspective, performing user access

reviews is critical to any healthcare organization's data management practices, and as our report findings indicate, many companies are not keeping tabs on user access rights.

ACCESS CONTROLS

Access controls are mechanisms to reduce risk, heighten visibility, and increase friction when it comes to granting access rights and privileges, or extending such access rights and privileges to third parties. They offer an extra layer of protection on top of access governance for situations that present higher risk to a healthcare organization. Fine-grained access controls, which include access schedules, approvals, and notifications, allow IT or security professionals to maintain more control over the exercise of user access rights. These differ from access rights—they don't change a user's rights—but instead provide a greater degree of control over their ability to use them. Credential vaulting and management further help manage the use and potential misuse of privileged credentials. To use a privileged credential, a user must request to "check out" a credential, and is often required to perform additional authentication before being granted access to the credential.

Additionally, employing zero trust network access solutions that microsegment the network prevents lateral movement in the case of a bad actor gaining a foothold with one account or application. Think of zero trust network access like navigating two mazes in a cornfield that never connect. You may be in the cornfield, but you can't jump from one maze to the other because there's a towering haystack in your way. By keeping you off of the network, zero trust ensures you can only access or even be aware of the explicit application you have access to.

ACCESS MONITORING

Access monitoring is the observation and analysis of what happened while a user was in a session—the period of time a user was "logged in," presumably performing work. Session audits can provide video replay or text audits of all access events and provide contextual data, including information such as who accessed what data, when, how, why, and for how long. It's also critical to implement robust machine learning-based access monitoring to electronic health records. Given the volume of daily accesses, it would be impossible to determine misuse without the aid of machine learning, so it's crucial to have a tool that can identify access events that have no apparent clinical relevance, and flag those instances for review or investigation by a privacy or compliance professional.

Healthcare organizations should think about implementing each of these three pillars of critical access management lest they fall victim to the next healthcare hack. By taking these necessary steps to secure user access, they ensure they're mitigating risk from privacy breaches and third-party attacks while protecting their most important asset: patient data. Scaling critical access management in turn allows healthcare organizations to avoid wasting precious time, personnel, and resources responding to data breaches and compliance missteps, and instead focus on what matters most—providing quality care.

SecureLink®

About SecureLink

SecureLink is the industry leader in critical access management, empowering organizations to secure access to their most valuable assets, including networks, systems, and data. By leveraging Zero Trust principles, machine learning, and artificial intelligence, SecureLink provides comprehensive security solutions to govern, control, monitor, and audit the most critical and highest risk access points. Organizations across multiple industries, including healthcare, manufacturing, government, legal, and gaming, trust SecureLink to secure all forms of critical access, from remote access for third parties to access to critical infrastructure, regulated information, IT, and OT.

Appendix: Additional Survey Results

The data points included in this report were from a broader study conducted by Ponemon Institute in December 2020 on behalf of SecureLink. The original study featured responses from 627 individuals across six industries, including financial services, health and pharma, public sector, services, and industrial and manufacturing. This report focuses on the responses of 69 individuals from health and pharma industries who are involved in their organization's approach to managing critical access data risks. Respondents are based in North America.

CAVEATS TO THIS STUDY

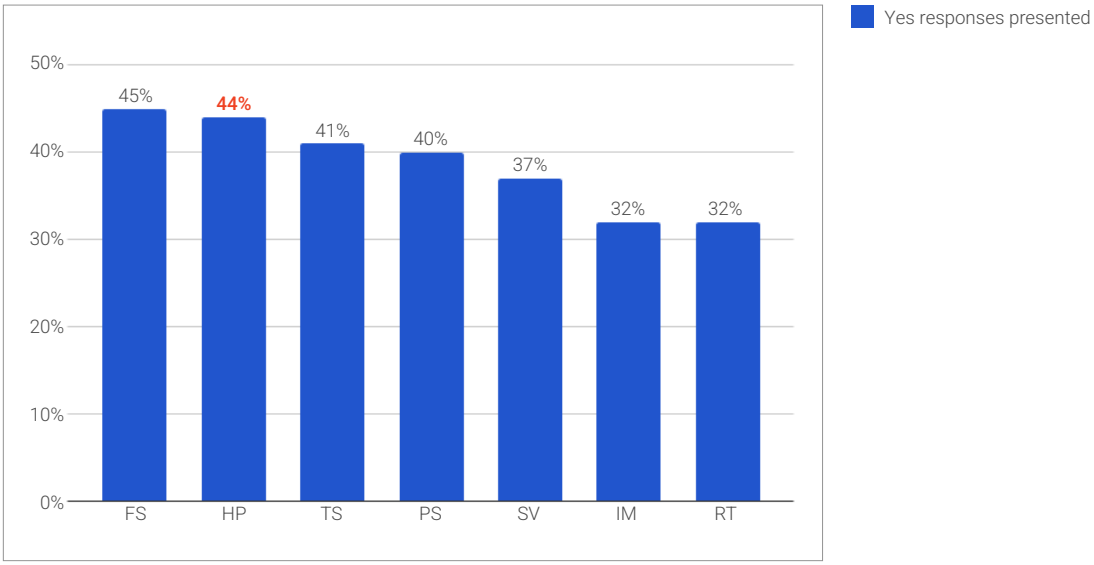
There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

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.

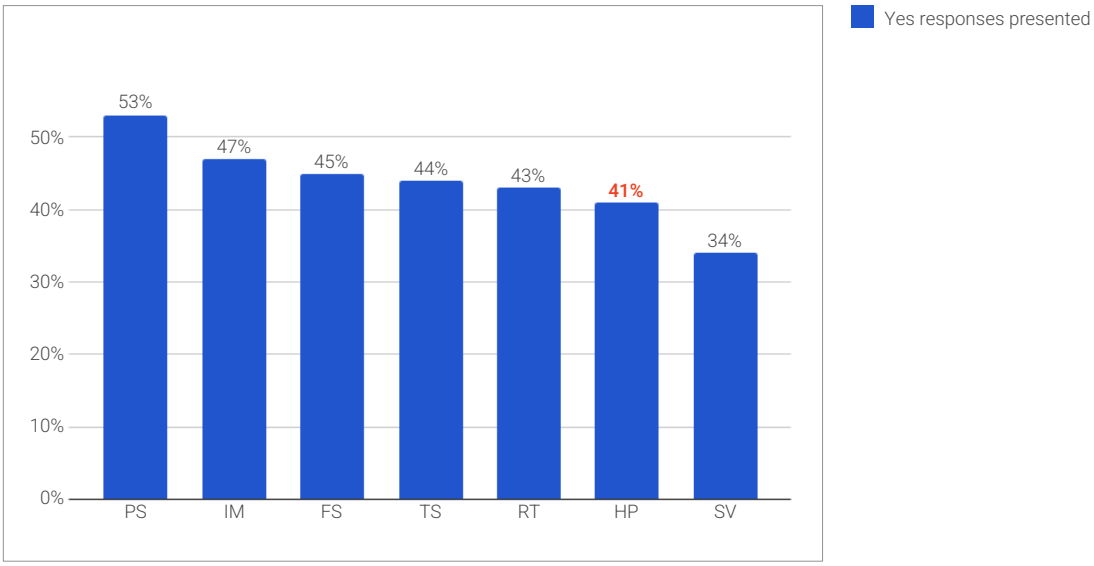
Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

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



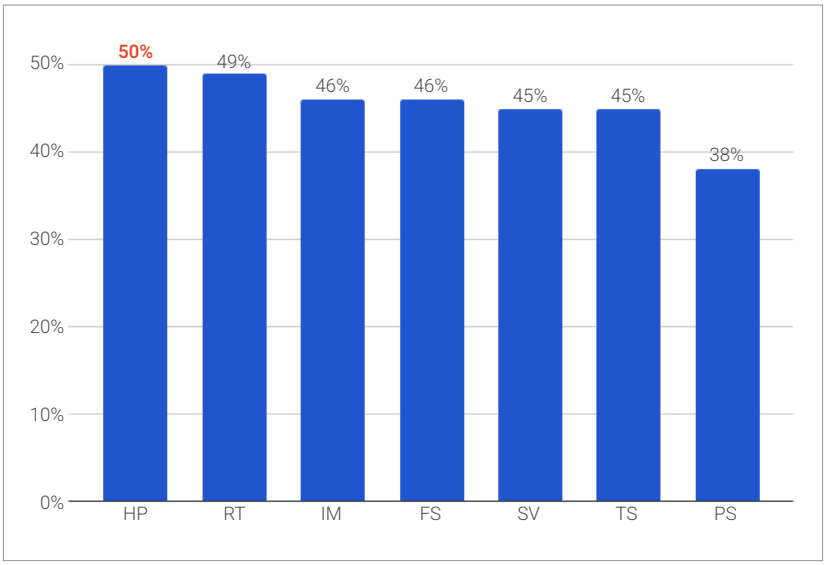
44% of healthcare and pharma

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



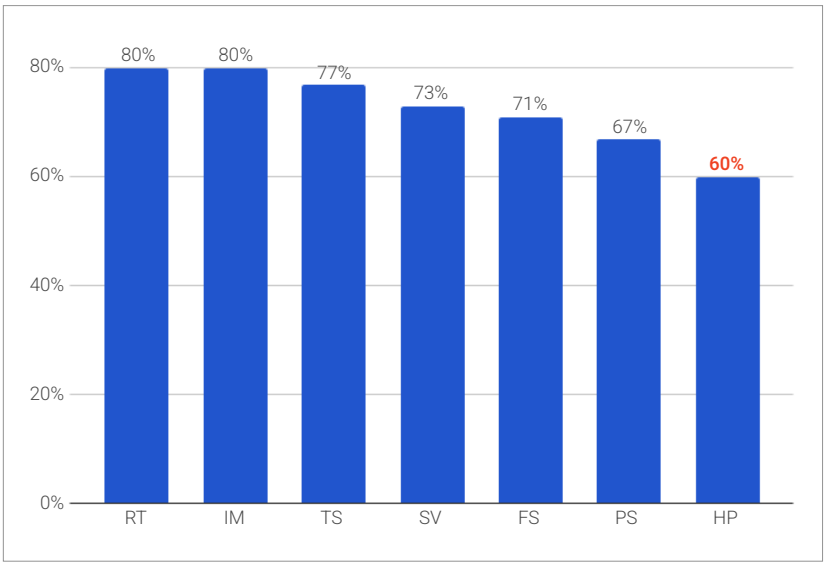
41% of healthcare and pharma

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



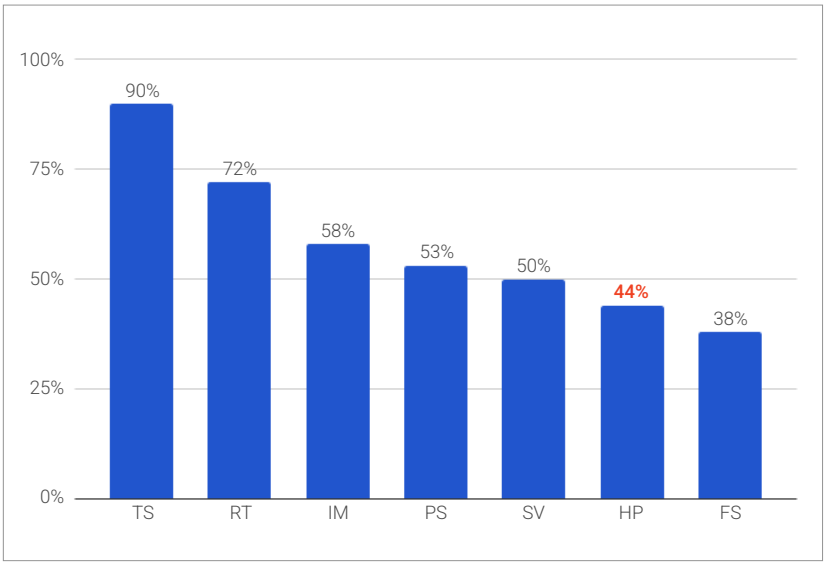
50% of healthcare and pharma

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



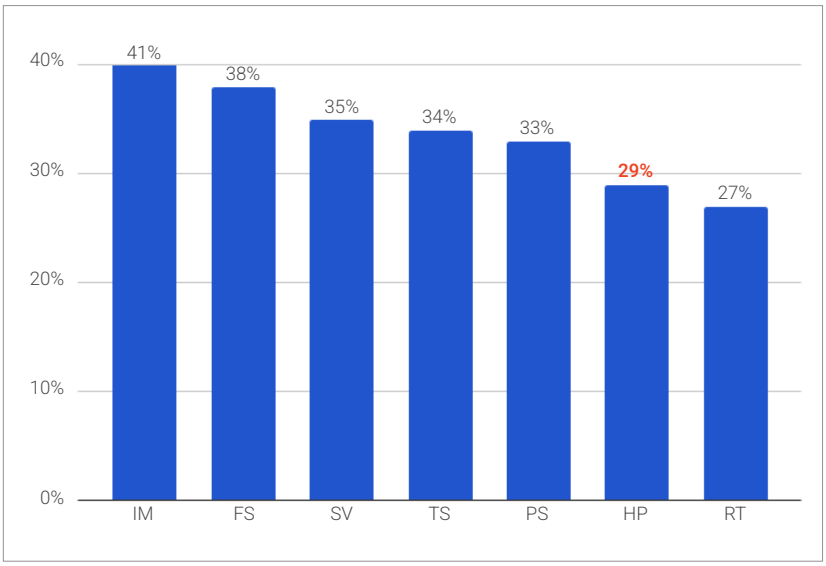
60% of healthcare and pharma

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



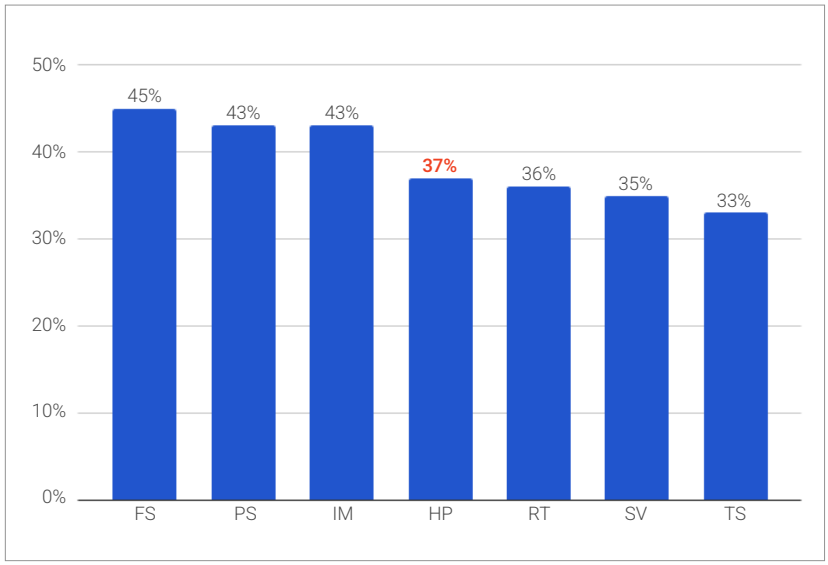
44% of healthcare and pharma

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?



29% of healthcare and pharma

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



37% of healthcare and pharma

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.