EBOOK

A digital identity crisis?

How mission- and life-critical industries are approaching cyber and privacy risks – and what needs to change

imprivata®

Introduction

Nearly 35 years ago, the world's first cyberattack paved the way for what would become one of the most destructive threats in the modern era. It all started when a Cornell University graduate, Robert Morris, developed a program to assess the size of the internet with a computer worm that would crawl the web, travel from computer to computer, and count the number of copies it made. Unfortunately for Morris, the program worked too well, spreading more easily than originally planned and resulting in the first denial-of-service (DoS) attack.

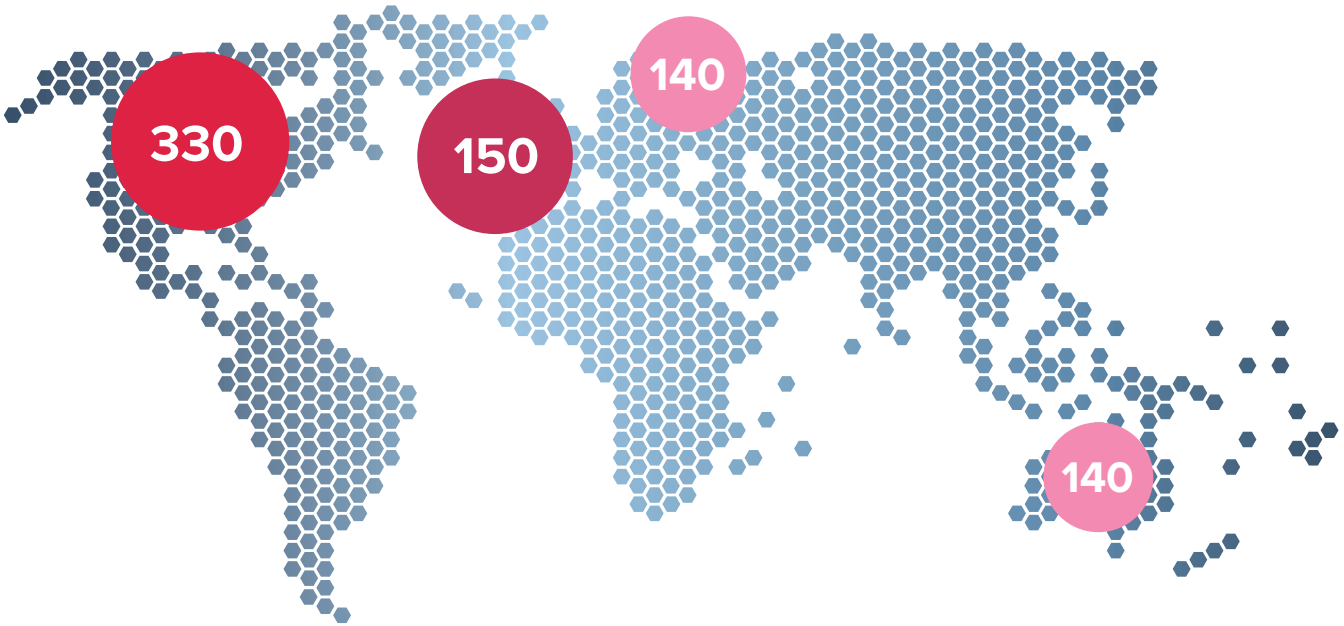
Today, the consequences of cybercrime range from loss of productivity and customer trust to loss of life. This is exacerbated by accelerating digitization, which creates new opportunities for cyber criminals to send organizations into a tailspin. Unfortunately, most organizations are likely to have their cybersecurity solutions and protocols tested at some point, but there are steps that can be taken to make sure they pass the test.

This report offers IT security and compliance leaders a lens into how mission- and life-critical industries are approaching cyber and privacy risks, with actionable steps every organization should be taking now to avoid disastrous consequences later.

About this report

This report is based on insights collected from 760 IT security leaders in healthcare, finance, manufacturing, pharmaceutical, and biotech organizations across the US, UK, Australia, and Germany. It will dive into key IT security challenges, ask what needs to change, and examine how modern principles and solutions can improve security and compliance.

Working with research partner Vanson Bourne, Imprivata surveyed decision-makers from organizations with more than 1,000 employees globally. Their seniority ranged from frontline management to the C-suite.



760 IT decision-makers

330 | US

150 | UK

140 | Australia

140 | Germany

Sectors

Manufacturing

Healthcare

Finance

Pharmaceuticals and biotech

PART 1

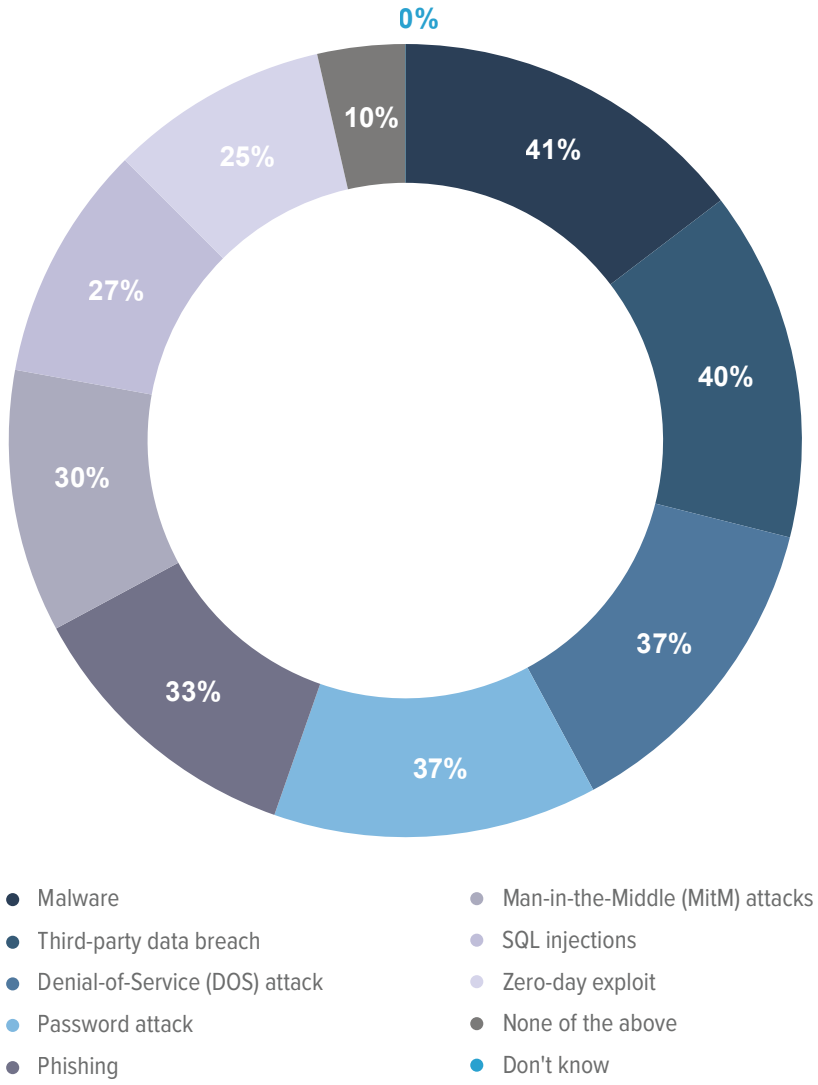
Uncharted waters: Struggling to swim in our complex IT landscape

The digital landscape is more complex and fast-moving than ever, so it's no surprise that nearly all organizations (99%) report falling victim to a cyberattack over the past 12 months, with more than half (58%) experiencing an increase in the frequency of attacks – to the tune of 21% more on average. At the same time, organizations are being exposed to a wider variety of threats than ever before.

The current IT landscape looks nothing like it did a decade ago. In the quest to stand up new services, facilities, and locations, optimize existing investments, and keep pace with countless users, roles, and applications, IT infrastructures have evolved into highly complex ecosystems that exist beyond well-defined perimeters.

This isn't lost on cyber criminals, who continuously evolve their tactics to breach organizations from every angle. Such is the case with malware and third-party data breaches, which respondents cite as the top two attack vectors. Today, malware is sold on the dark web and can be deployed with little-to-no technical expertise. And third-party data breaches have risen sharply with more organizations leveraging vendors, partners, and contractors as essential business resources.

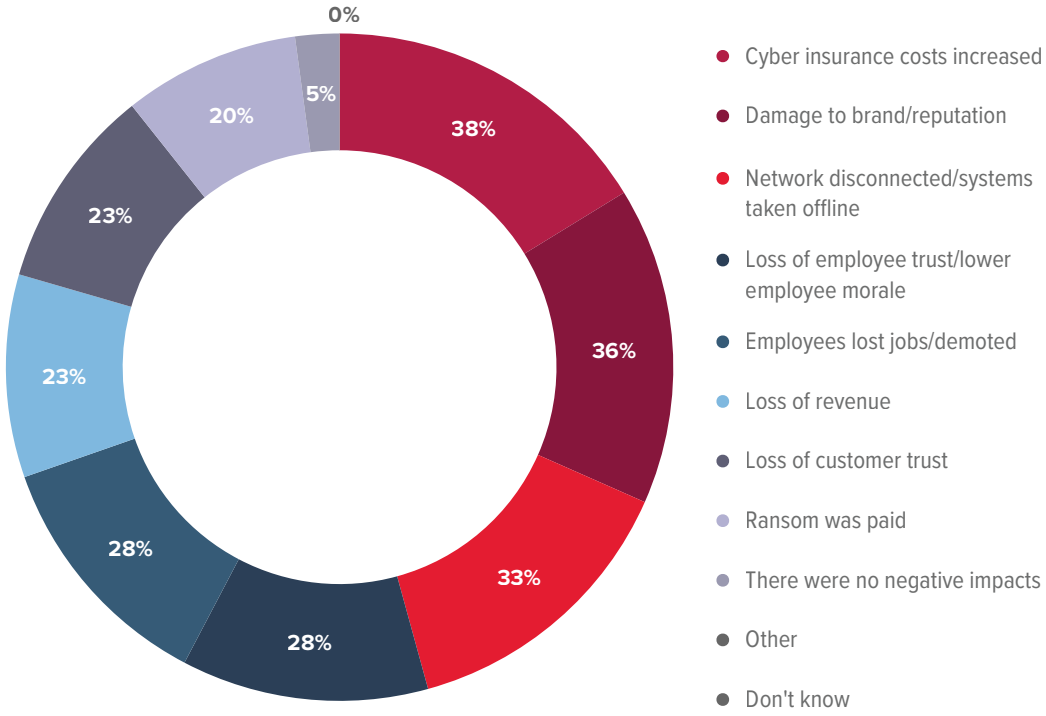
Which, if any, of the following cyberattacks has your organization experienced over the last 12 months? Chart 1.



The fallout of being unprepared

For mission-critical industries, the impact of a cyberattack can be severe and wide-ranging, as demonstrated in chart two. In the immediate term, organizations often face monetary losses due to ransom payouts and operational disruption from systems going offline. But the longer-term effects – like reputational damage, lost customer trust, and low employee morale – are even more pernicious and harder to quantify.

What, if any, negative impacts resulted from cyberattacks?
Chart 2.



Interestingly, respondents name “increased cyber insurance costs” as the most common negative impact of cyberattacks, adding that their cyber insurance premiums have risen by an average of 35% in the past year. In addition, respondents report significant policy limitations. Of those without full cyber insurance, 48% say their policy doesn’t cover all real-life scenarios, while 42% find it too difficult to prove compliance.

WHEN THE COST GOES BEYOND MONETARY

For healthcare organizations, the fallout often goes beyond higher cyber insurance costs and affects patient care. In fact, three in ten (32%) healthcare delivery organizations report they’ve diverted patients to alternative healthcare facilities after a cyberattack, with 31% saying attacks have delayed procedures and tests that resulted in poor outcomes.

32%

Cite patients diverted to other healthcare facilities

31%

Said procedures and tests have been delayed that resulted in poor outcomes

26%

Have seen an increase in complications from medical procedures

Global snapshot: Integrated health systems and the Hospital of the Future Act

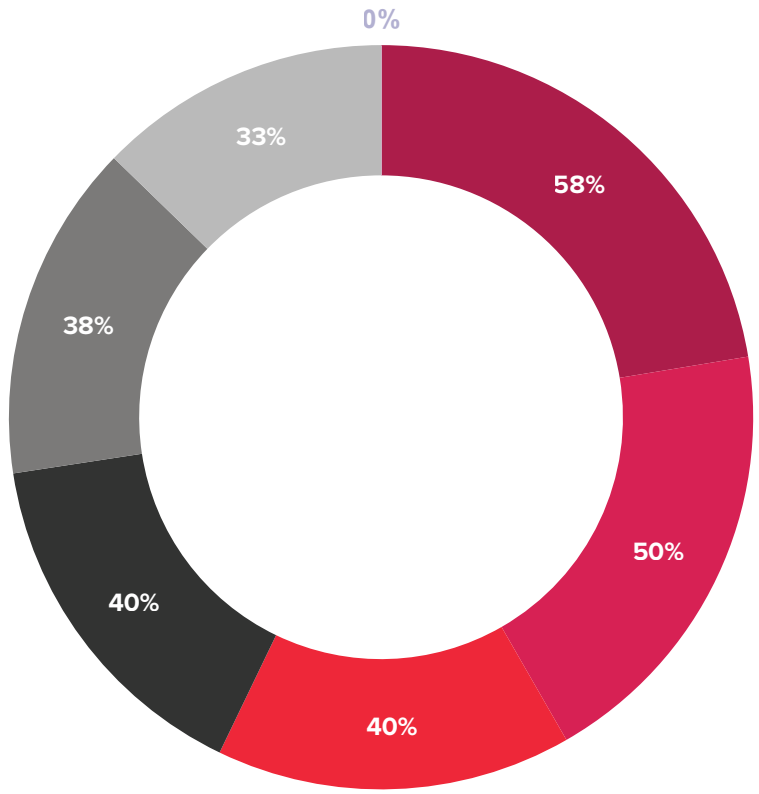
Healthcare looks very different in the UK and Germany than it does in the US, with varied delivery models and regulatory compliance mandates.

In the UK, integrated care systems (ICSs) bring together NHS organizations and local authorities to take a strategic approach to improving health and reducing inequalities. In 2022, the Health and Care Act was passed to formalize these partnerships as legal entities with the aim of delivering more cohesive care to patients who rely on multiple services.

Doing this effectively will require significant digital transformation within the NHS. The UK government's 2022 policy paper, "A plan for digital health and social care," aims to "digitize, connect and transform" the health service and is backed by £2 billion in funding from a recent government spending review. But, so far, UK hospitals have had varying success in integrating backend clinical systems, with just one third (35%) of respondents saying they have already done so.

In Germany, the Hospital of the Future Act (KHZG) is a funding program that seeks to support the digitization efforts of regional care systems. And for over half (58%) of respondents in Germany, investments will be prioritized to ensure compliance with data protection regulations, followed closely by incorporating telematics applications and improving IT security.

What, if any, are the investment priorities for your IT department based on the kenhauszukunftsgesetz (KHZG/Hospital future act)? Chart 3.



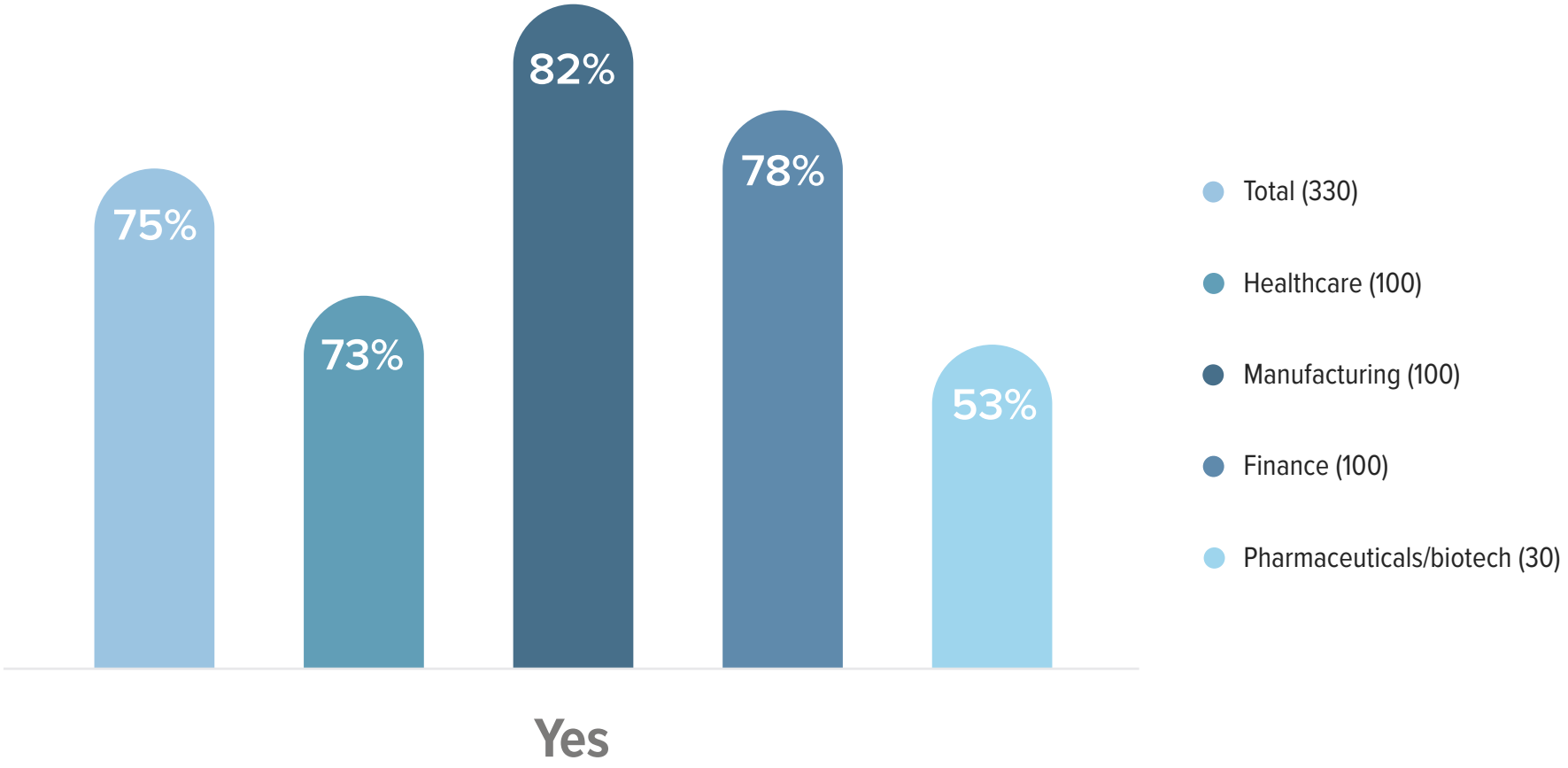
Are organizations prepared to report attacks?

US organizations classified as “critical infrastructure” are required to report cyberattacks to the Cybersecurity & Infrastructure Security Agency (CISA) within 72 hours of their discovery.

This designation encompasses many organizations in the financial services, healthcare, and pharmaceuticals sectors.

Though the majority do have reporting systems in place, the pharmaceuticals sector appears to be behind the curve. Around half (47%) of pharmaceutical respondents say their organization hasn’t yet implemented a reporting system.

Does your organization have a system in place to report cyberattacks to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours? Chart 4.



Looking beyond the perimeter

Organizations' attack surfaces have grown exponentially and, as a result, most (91%) IT and security leaders agree that their organization can no longer rely on perimeter security.

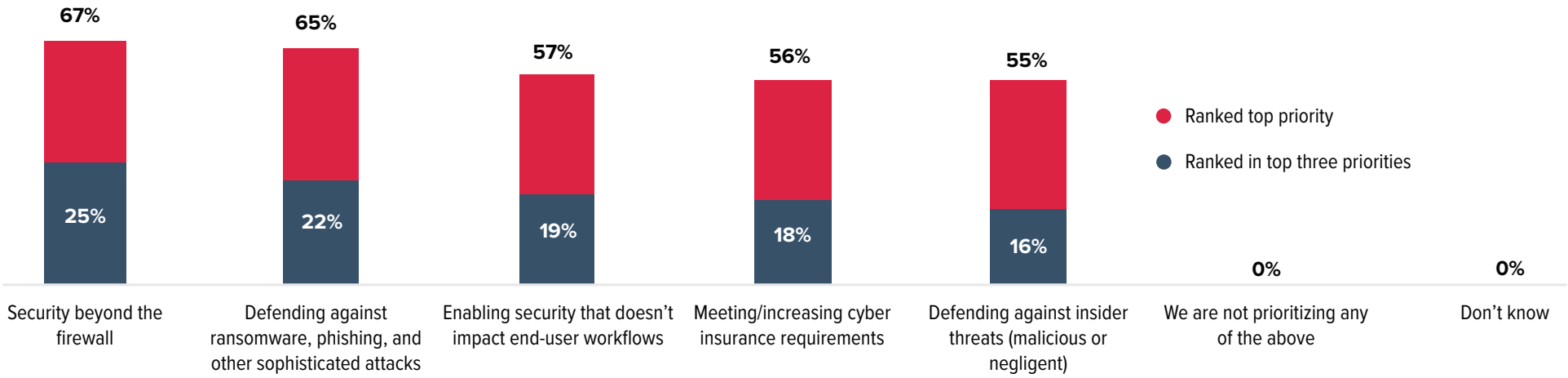
Perimeter-based, or "end point," security relies on protecting the boundaries of a network to secure data and resources. Common components include firewalls, VPNs, intrusion detection systems (IDS), and intrusion prevention systems (IPS). Once inside, users are trusted and can therefore move laterally through the network without re-authenticating.

While this approach made sense when networks were located almost entirely on-premises, the complex and distributed networks of today require organizations to manage and govern access to data and resources through the authenticated identity of an individual or device.

Commonly referred to as "identity-based" or "identity" security, this approach is focused on ensuring users are only able to access the data and resources they need and is a cornerstone of modern security. In fact, 67% of those surveyed are prioritizing security beyond the firewall as one of their top three investment priorities this year.

Most (91%) IT and security leaders agree that their organization can no longer rely on perimeter security.

Please rank the following security related actions in order of priority for investment in your organization. Chart 5.



The role of digital identity in Zero Trust

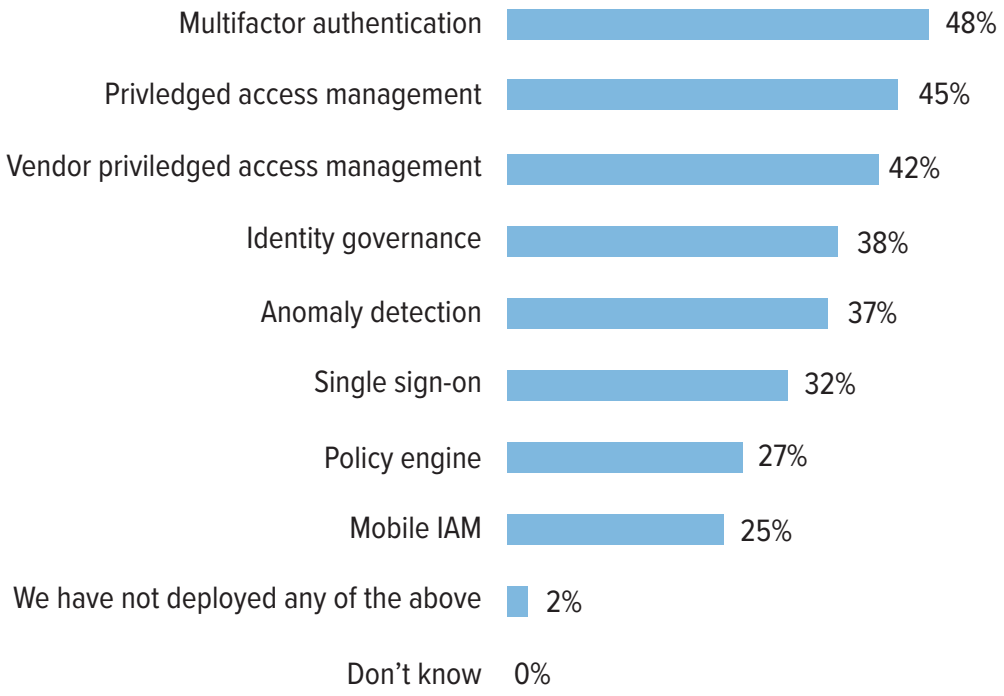
The popularity of Zero Trust principles has grown hugely in recent years, catalyzed by the rise of cloud computing and remote working – which make traditional perimeter security harder to enforce. Now considered a security best practice, Zero Trust requires continuous identity verification, driven by a sharp focus on authentication and authorization for each user, device, application, and transaction. This is only made possible through identity and access management (IAM) – the policies and technologies that ensure the right individuals are accessing the right resources for the right reasons.

Though the concept of Zero Trust isn't new, the adoption of technologies to facilitate a Zero Trust architecture (ZTA) varies – as demonstrated by survey respondents.

Many solutions, which together create a robust Zero Trust architecture, manage and govern access for digital identities within an organization. For example, identity governance technologies play a key role in automating user provisioning and de-provisioning processes. Meanwhile, privileged access management (PAM) solutions control privileged and third-party roles and entitlements, a critical need, as data is increasingly being stored off-premises in environments administered by vendors or partners. Likewise, multifactor authentication requires users to provide two or more verification factors before gaining access to organizational resources. And a single sign-on solution enables greater security and compliance by permitting users to access applications with one set of login credentials.

Despite widespread familiarity with Zero Trust principles, fewer than half of those surveyed have adopted the foundational solutions needed to achieve Zero Trust. Over a third (34%) cite high complexity as a key challenge in implementing Zero Trust, while a similar number are experiencing challenges related to impacted user workflows (33%) and lack of IT expertise (32%).

Which of the following technologies, if any, has your organization deployed to support a Zero Trust architecture? Chart 6.



PART 2

Organizational response: the use of solutions to enable, control, and monitor the digital identity

As outlined in part one, most organizations agree they can no longer rely on end point or “perimeter” security. And while many have implemented solutions to secure and control access with digital identity, there’s still significant room for improvement. For example, only six in ten (60%) respondents say their organization can both automatically modify and revoke user access.

This raises potential security concerns related to departing employees, not to mention IT security teams’ ability to quickly adjust user access entitlements following a suspected breach.

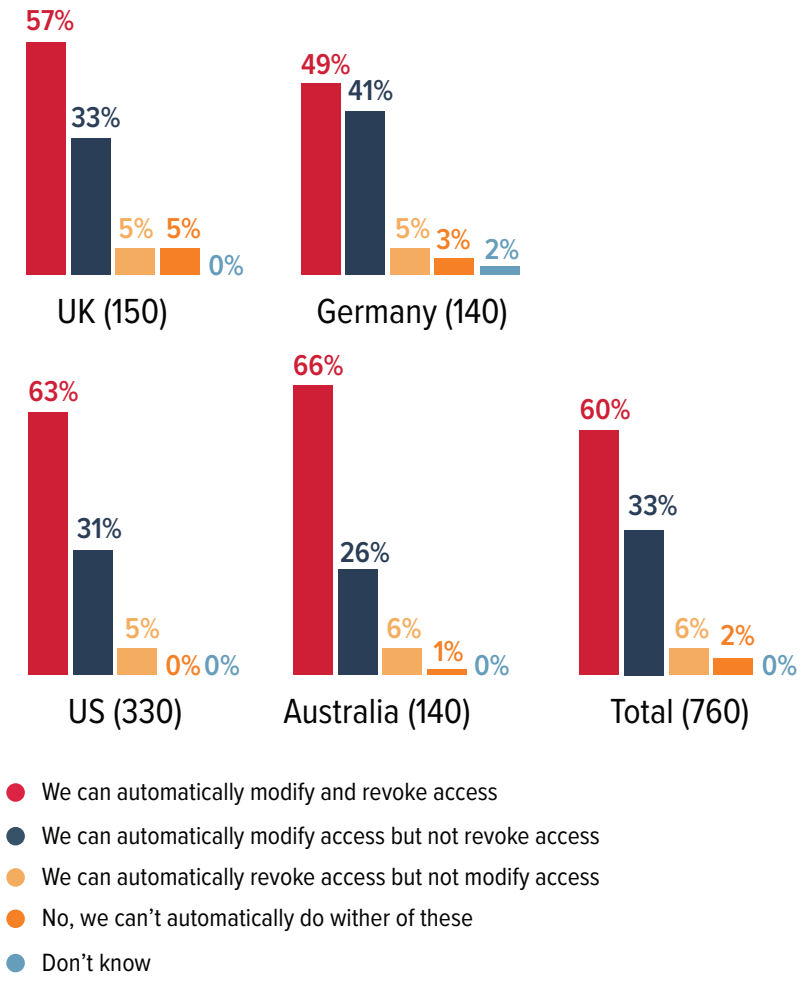
When business partners are breached

Managing digital identities doesn’t stop with end users or employees. Securing all user identities is important as third-party vendors, partners, and contractors often have remote access to critical resources and can pose a huge risk to organizations. Despite this, third parties often use traditional remote access methods like VPNs or desktop sharing tools that bad actors can easily exploit. Indeed, respondents report that just 42% of third-party remote access is governed, controlled, and monitored by respondents. A scant 2% say they govern access for all third-party remote access.

These figures make for alarming reading, especially considering that 40% of those surveyed say their organization has fallen victim to a third-party data breach over the last 12 months, second only to malware at 41% (chart 1).

Just 42% of third-party remote access is governed, controlled, and monitored by respondents.

Is your organization able to automatically modify or revoke access as users change roles or leave the organization? Chart 7.



Are threats coming from within?

Increasingly, cyber threats are originating from within organizations – whether from disgruntled or departing employees, the abuse of privileged user credentials, or unauthorized or accidental data access.

These insider threats pose a unique challenge because threat actors often have intimate knowledge of systems and applications. Understanding typical activity patterns in your CRM and office productivity applications is fundamental to being able to quickly identify anomalies and reduce risk, with around half of respondents opting to incorporate data science to monitor, alert, and interpret data in real time.

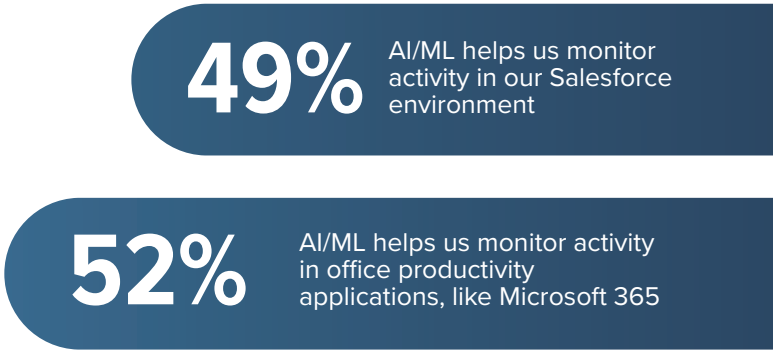
A full 52% of respondents cite leveraging artificial intelligence (AI) and/or machine learning (ML) to monitor activity in office productivity applications like Microsoft 365, with 49% using these technologies to monitor activity in Salesforce. It appears that the other half use manual processes to identify and investigate impermissible access, making it much more likely that warning signals are overlooked.

THE HUMAN FACTOR OF INSIDER THREATS

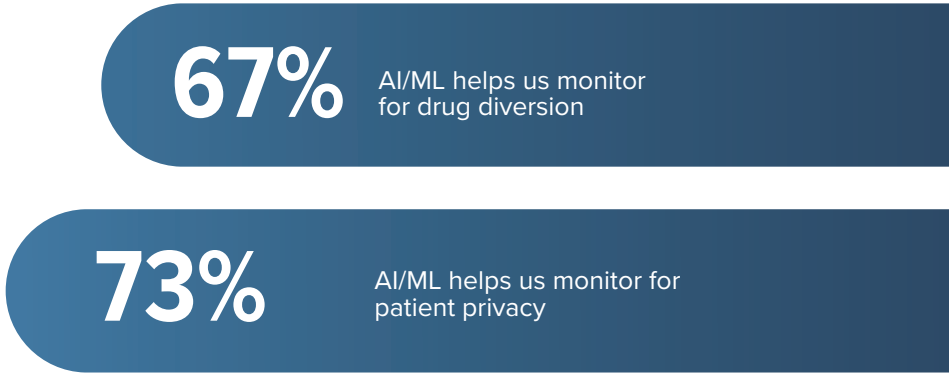
Anomalous behavior in the healthcare sector often goes uninvestigated, with inaction carrying significant human cost. For example, the over-prescription of opiate painkillers has reached epidemic levels at hospitals, pharmacies, and other healthcare organizations. Addicted employees put themselves, their colleagues, and patients at risk. Patients may be denied pain relief or exposed to blood-borne pathogens, while health systems may be subject to fines and regulatory liability.

Behavioral monitoring can help reduce the risk of unauthorized access to health records and drug diversion. Although most attempt to monitor for this in some capacity, many cases remain uninvestigated due to widely used manual methods that rely on a small, random subset of transactions. The good news is that more respondents are turning to advanced data science to make an impact, with 73% using AI/ML to monitor patient privacy and 67% to monitor drug diversion.

To what extent does your organization use solutions with artificial intelligence (AI) and/or machine learning (ML) to proactively monitor user activity? Chart 8.



To what extent does your organization use solutions with artificial intelligence (AI) and/or machine learning (ML) to proactively monitor user activity? Chart 9.

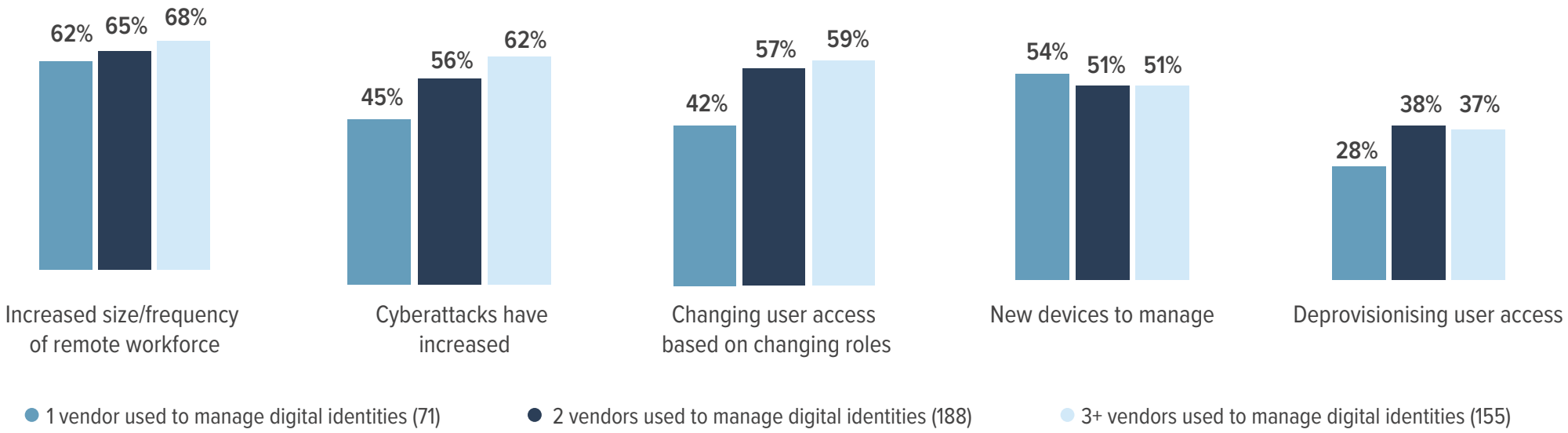


More vendors, more problems?

Already facing pressure before the pandemic, IT leaders scrambled to bolster security defenses when the world changed overnight back in 2020 – with remote working suddenly the norm and healthcare organizations immediately inundated. Before they knew it, some were deploying over a dozen unintegrated solutions that may have been a quick fix but haven't proven effective or sustainable long-term.

With respect to digital identity, most (82%) respondents currently work with two or more solution vendors, with nearly four in ten (37%) using three or more. A common reason for this is the need to support legacy applications in an era of cloud-first vendors. While using multiple vendors may be necessary in some cases, respondents that use a single vendor to manage digital identities are less likely to experience challenges to the degree of those that use more – as demonstrated by the below chart below.

In what ways, if at all, has identity management become more challenging? Chart 10.



PART 3

Sector-specific takeaways

Unfortunately, the risk of cyberattacks continues to rise, and mission-and life-critical industries have a lot at stake. In addition to defending against ransomware, phishing, and other attacks, they must support an increasingly remote workforce, keep up with ever-changing user roles and new devices, and meet cyber insurance requirements – all while streamlining end user workflows. That's a tall order.

When looking at key metrics across industries, it's evident that some have a more mature approach to managing digital identities, but, as ever, there's significant room for improvement.

For example, over half of organizations surveyed report having had login details stolen because of a cyberattack within the past year, yet there's a noticeable gap in their ability to quickly modify or revoke user access as roles change or users leave an organization. About half of respondents also enforce complex passwords to control access to applications and data, but a sizable portion aren't leveraging single sign-on technology to streamline the user experience. Finally, of those surveyed, third-party data breaches are the second-most cited type of cyberattack, however respondents govern less than half of third-party remote access. Clearly, there's a mismatch between security challenges and organizations' ability to combat them.

Obviously, implementing a comprehensive strategy with robust solutions takes time and money, but investing in technologies that keep mission- and life-critical organizations secure is a good investment for the future.

PHARMACEUTICAL/BIOTECH SECTOR HIGHLIGHTS

74% Say employee and customer login credentials were stolen as a result of a cyberattack within the past year

52% Can automatically modify or revoke user access as roles change or they leave the organization

45% Enforce the use of complex passwords (minimum of 16 characters)

42% Have implemented single sign-on across the organization to eliminate the need for manual password re-entry

48% Have deployed a privileged access management solution to support zero trust

37% Of third-party remote access is governed, controlled and monitored, on average

MANUFACTURING SECTOR HIGHLIGHTS

66% Say employee and customer login credentials were stolen as a result of a cyberattack within the past year

67% Can automatically modify or revoke user access as roles change or they leave the organization

50% Enforce the use of complex passwords (minimum of 16 characters)

54% Have implemented single sign-on across the organization to eliminate the need for manual password re-entry

50% Have deployed a privileged access management solution to support zero trust

45% Of third-party remote access is governed, controlled and monitored, on average

FINANCE SECTOR HIGHLIGHTS

68% Say employee and customer login credentials were stolen as a result of a cyberattack within the past year

62% Can automatically modify or revoke user access as roles change or they leave the organization

52% Enforce the use of complex passwords (minimum of 16 characters)

43% Have implemented single sign-on across the organization to eliminate the need for manual password re-entry

41% Have deployed a privileged access management solution to support zero trust

40% Of third-party remote access is governed, controlled and monitored, on average

HEALTHCARE SECTOR HIGHLIGHTS

68% Say employee and customer login credentials were stolen as a result of a cyberattack within the past year

54% Can automatically modify or revoke user access as roles change or they leave the organization

47% Enforce the use of complex passwords (minimum of 16 characters)

40% Have implemented single sign-on across the organization to eliminate the need for manual password re-entry

45% Have deployed a privileged access management solution to support zero trust

44% Of third-party remote access is governed, controlled and monitored, on average

PART 4

Conclusion

It comes as little surprise that cyber threats are numerous and varied across all sectors surveyed. The outcomes of cyberattacks range from lost customer trust and skyrocketing cyber insurance premiums to poor patient outcomes in the healthcare sector.

But organizations are fighting back. IT security leaders are no longer relying on traditional perimeter-based security, with nearly seven in ten (67%) prioritizing security beyond the firewall and over half (57%) enabling security that doesn't impact end user workflows.

Where to start: Building a Zero Trust architecture for people

Employees and third parties need access to data and applications, while organizations need to secure them against access from bad actors. Thus, one of the key challenges of Zero Trust is controlling access without bringing employee workflows to a halt.

The reality is that people prefer convenience to security and will generally find workarounds when technology gets in the way. However, risky user behavior such as credential sharing leaves gaping holes in an otherwise sound security strategy that cyber criminals are waiting to exploit.

The good news? Since the workflow experience is often one of the least mature areas of a Zero Trust strategy, it's often the quickest to improve with four foundational processes and technologies in place:

1. **Implement lifecycle provisioning and de-provisioning.** Identity governance is a crucial component to ensure you can automatically modify or revoke access as users change roles or leave the organization.

2. **Create user checkpoints with multifactor authentication.** One of the most common initial attack vectors is compromised user credentials, so ensuring users are who they say they are is of utmost importance. Multifactor authentication can provide a secure, auditable chain of trust across the enterprise without getting in the way of user productivity with non-disruptive modalities such as biometrics and proximity-based authentication.

3. **Enable a passwordless experience.** Enforcing complex passwords is a security best practice, but not entirely realistic when users must enter them into multiple applications all day, every day. Single sign-on technology supports streamlined workflows and improves compliance by reducing the need to enter usernames and passwords to access on-premises and cloud applications.

4. **Practice the principle of least privilege.** Make sure you're not giving employees and third-party vendors more access than they need by providing just enough to complete a task, and nothing more. Privileged access management prevents overprivileged users through granular policy control at the system level.

Broader solutions may be added to build on this foundation, but with this groundwork in place, you can build a Zero Trust strategy that balances strong security and compliance with end user convenience.

Take the next step

Building a strategy for identity-centric Zero Trust can be daunting, which is why we've developed a framework that addresses key governance and administration, identity management, authorization, and access and authentication functions to support the planning process.

Whether you need help getting started or understanding what step to take next, we can help.

ACCESS THE FRAMEWORK >

BOOK A PERSONALIZED CONSULTATION >

About Imprivata

Imprivata is the digital identity company for mission- and life-critical industries, redefining how organizations solve complex workflow, security, and compliance challenges with solutions that protect critical data and applications without workflow disruption. Its platform of interoperable identity, authentication, and access management solutions enables organizations in over 45 countries to fully manage and secure all enterprise and third-party digital identities by establishing trust between people, technology, and information.

www.imprivata.com