BeyondTrust

PRIVILEGED ACCESS THREAT REPORT 2018

Urgent action required to address growing privileged access and identity threats

I: 2018 THREAT LANDSCAPE

INTRODUCTION

The WannaCry ransomware attack in May 2017 crippled the UK's National Health Service (NHS) and disrupted a range of organizations across 150 countries. Despite being a relatively unsophisticated attack, WannaCry was able to make such a global impact due to preventable vulnerabilities that had largely gone unaddressed. There were many more attacks in 2017, including high-profile breaches at Uber and Equifax, where heeding cyber-security recommendations may have reduced the impact and fallout.

The scale and sophistication of cyber-attacks is not slowing down – ranging from phishing scams to cryptocurrency-based cyber-attacks, to state-sponsored attacks on industrial control systems. These attacks present an ever growing challenge and serve as a reminder that organizations cannot afford to be complacent in the face of cyber threats. We're living in a time when cyber-attacks are a matter of when, not if, and security professionals must focus on mitigating their extent and damage.

Our 2018 research results confirm that security professionals are aware that a breach is only a matter of time, with **50%** of respondents having already suffered a serious breach or expecting to experience one within the next six months (up from 42% last year).

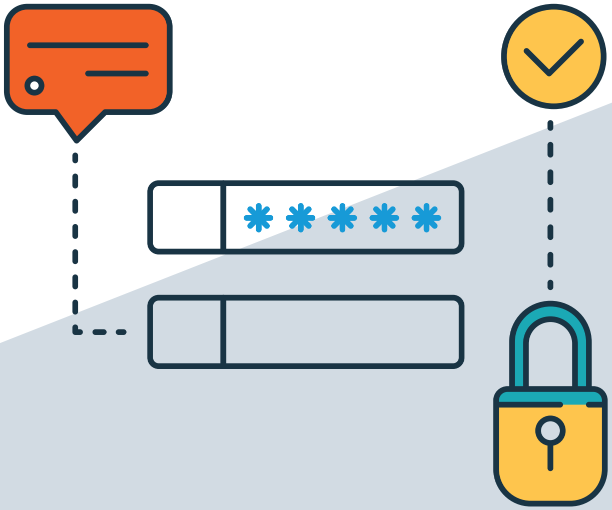
With many of these breaches linked to the misuse of insider (**62%**) or third-party (**66%**) privileged credentials, it's clear that although organizations understand the risks, they aren't successfully addressing how they manage privileged credentials to protect their critical assets and systems.

IT administrators and third-party vendors need privileged access to do their jobs effectively, but the number of privileged users and accounts is growing exponentially and access to systems and data is often being granted in an uncontrolled way. In the face of growing threats, together with the introduction of stricter compliance standards, including the EU GDPR, the need to address and implement an organization-wide strategy to manage and control privileged access has never been greater.

It's this that's defining the threat landscape in 2018 and that organizations need to address.

62% think it's possible or definite they have suffered a breach through insider action

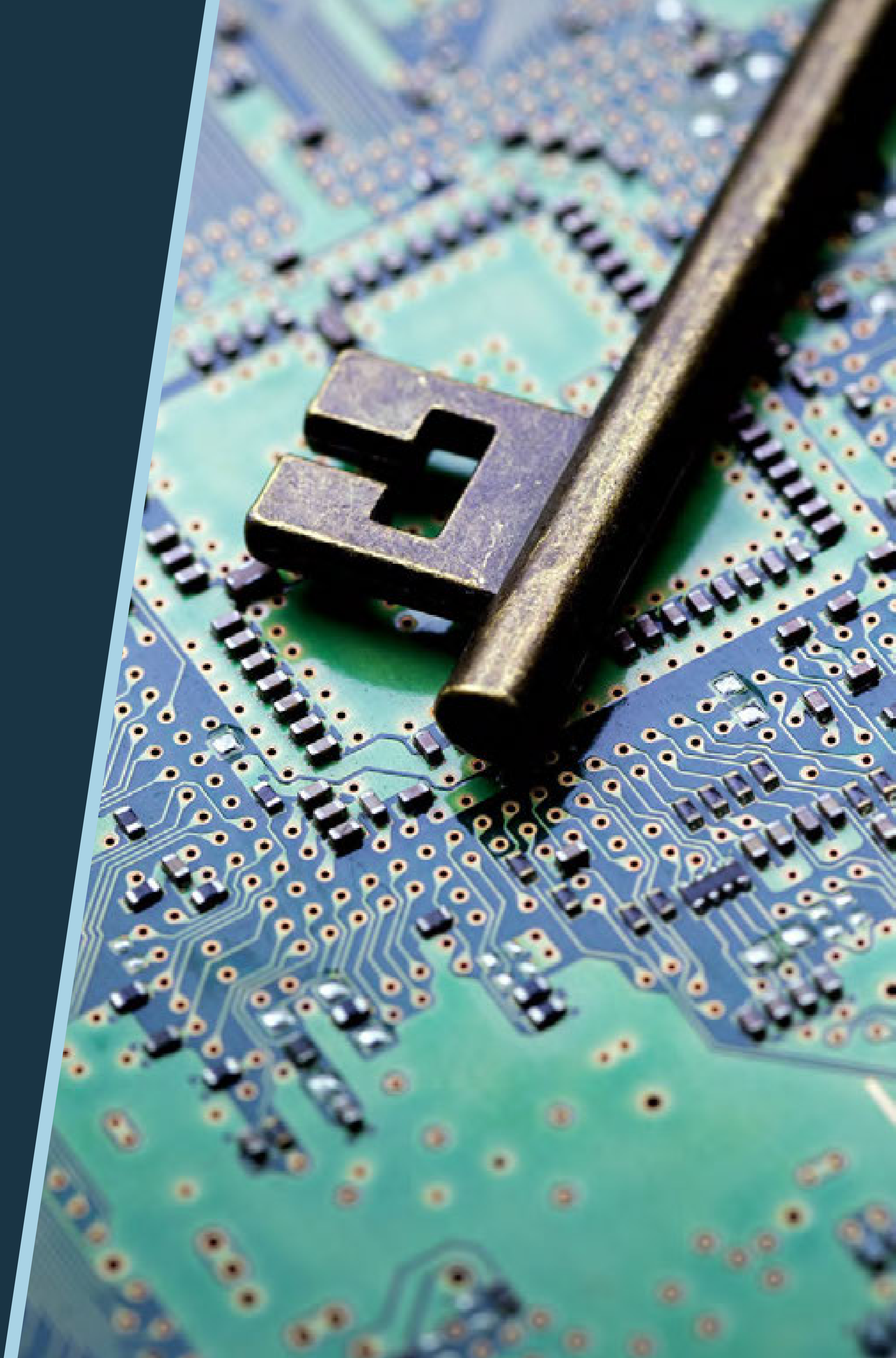
66% think it's possible or definite they have suffered a breach through third-party access



RESEARCH METHODOLOGY

1021 key decision makers with visibility over the processes associated with enabling internal users and external parties to connect to their systems completed a survey in February 2018. The surveys were completed by IT professionals across operations, IT support/ helpdesk, IT security, compliance and risk or network/general IT roles. Respondents were from a range of industries, including manufacturing, finance, professional services, retail, healthcare, telecoms and the public sector. The survey was conducted across the United Kingdom, the United States, Germany and France.

II: A MATTER OF TRUST



A MATTER OF TRUST

Despite knowing that cyber-attacks are increasingly likely – and that they have a growing number of privileged insiders and vendors – organizations are leaving large parts of their IT security to trust. Without the means or resources to monitor and manage privileged access to IT systems, a culture based on trusting people remains, however ineffective that may be in detecting and preventing security breaches.

The most trusting sector is financial services, where 46% of organizations say they completely trust insiders and 41% completely trust third-party vendors. These results are higher than in any other sector (Fig. 1), even though financial services organizations are the most likely to have experienced an insider or third-party breach in the last year (Fig. 2). Financial services is also the sector that is most concerned about the insider threat moving forward. Firms are either **very** or **fairly** concerned about insider credentials being used for malicious purposes, whether intentionally (68%) or through phishing (67%) – again, higher than in any other sector.

Fig. 1

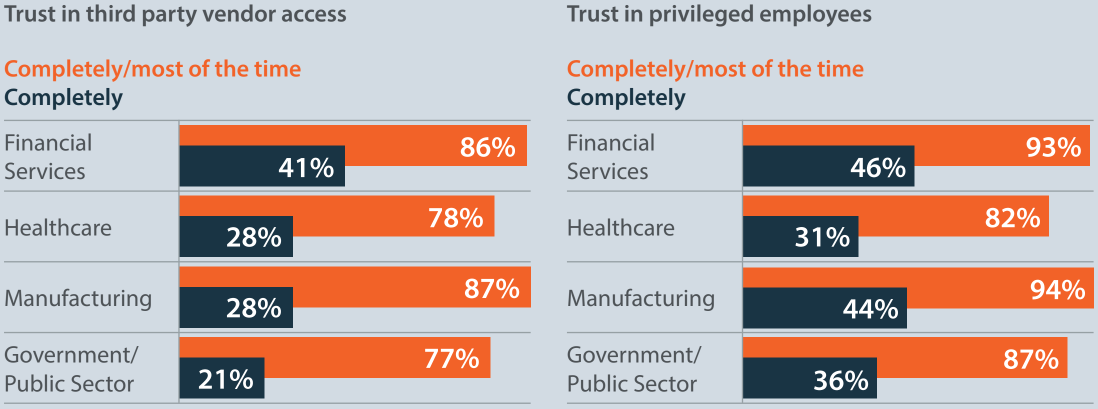
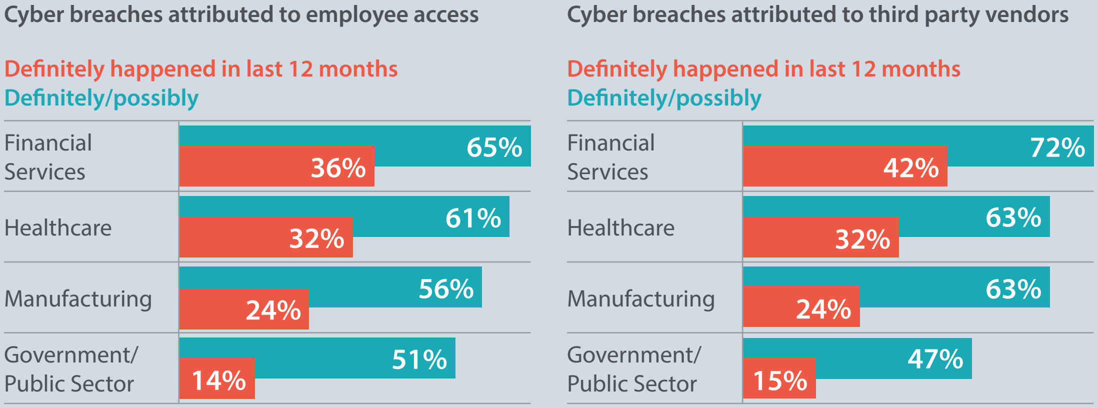


Fig. 2



A MATTER OF TRUST

Many organizations are far too trusting when it comes to insiders and third parties. Good faith is simply not a viable security strategy to address the increasing risks and threats. And while most people don't have malicious intent, many individuals create security gaps through negligence or by working around security policies, and organizations have to acknowledge and address that.

To understand why the majority of organizations have yet to achieve a desired state of visibility and control when it comes to their own IT environments, we must first understand the nature of the risks they face.

III: THE PROBLEM WITH PRIVILEGE

THE PROBLEM WITH PRIVILEGE

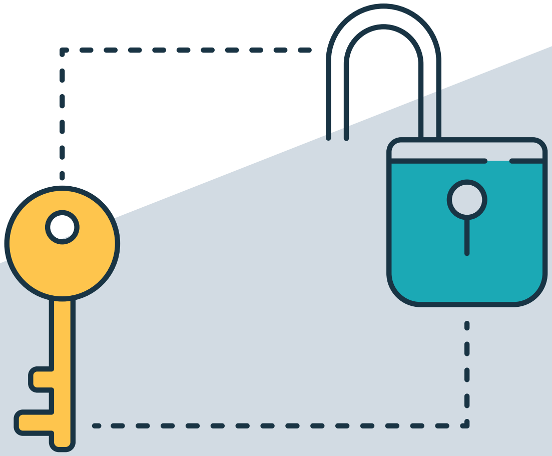
A 'privileged' identity is one which has been granted elevated access to an organization's IT environment, enabling authorized, administrative access to an organization's most critical IT systems and often sensitive, highly valuable data. Users with privileged access can include an organization's own employees (insiders), but also increasingly third-party vendors. Whether used by an internal employee or external vendor, privileged credentials are prime targets for phishers and attackers.

As revealed in Fig. 2, organizations in the financial sector are the most exposed to the threat of insider or third-party breaches, with **65%** saying they have possibly or definitely suffered an insider-related breach in the last year and **72%** possibly or definitely suffering a breach linked to a third-party identity. These numbers were lower in all other sectors: healthcare (**61%** and **63%**), manufacturing (**56%** and **63%**) and the public sector (**51%** and **47%**).

While insiders and third-party identities each come with their own sets of behaviors and associated risks, solutions are available to manage and control the combined threat they pose. Our research shows organizations are addressing this threat in one of three ways:

- Using a Privileged Identity and Access Management (PIM/PAM) solution (**46%**)
- Manually controlling the creation and management of privileged identities (**44%**)
- Not controlling them at all (**10%**)

The results show that one in every ten organizations has no control over privileged identities at all, while almost half are controlling them manually, with no dedicated system in place. This not only consumes valuable time and resources, but also leaves the majority of respondents wide open to cyber-attacks.

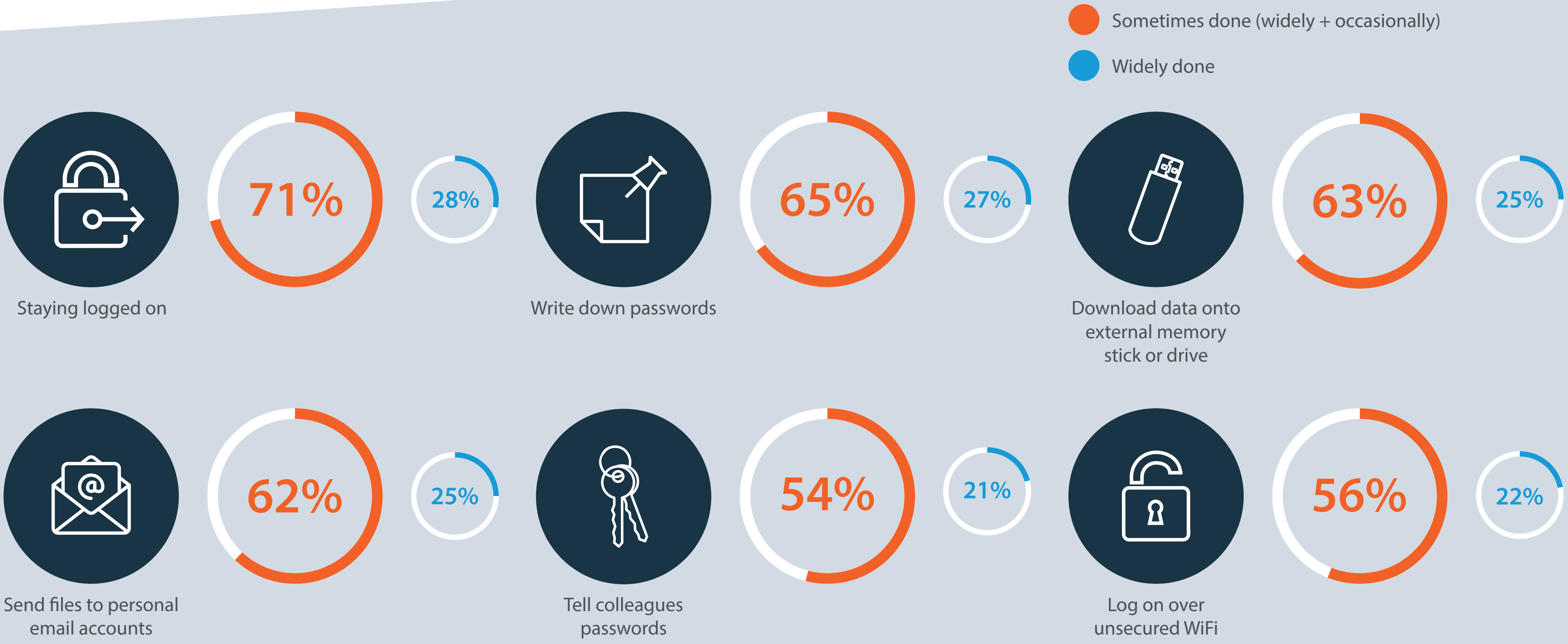


THE ‘INSIDER’ RISK

An organization’s insiders, such as IT administrators, need privileged access to sensitive systems and data to be productive and support their business, but granting that permission in an uncontrolled, untraceable way makes the organization vulnerable to attackers.

On the other hand, when insiders are faced with increased security measures that slow them down or prohibit them from doing their job, they’ll often look for shortcuts which can result in an array of risky behaviors, such as logging in over unsecured networks, downloading data to memory sticks, or writing down passwords (Fig. 3).

Fig. 3



THE 'INSIDER' RISK

These risky behaviors are becoming more widespread, with the number of respondents saying they 'happen sometimes' increasing in every instance from last year. Writing down passwords, for example, was cited as a problem by **55%** of organizations in 2017, but has risen to **65%** in 2018. And telling colleagues passwords was a problem for **46%** of organizations in 2017, rising to **54%** in 2018. This rise may be genuine and the sign of a growing issue, or it may be that organizations are more keenly aware of these risky behaviors due to the increased focus on data protection and preventing breaches. Either way, the numbers indicate an issue that needs to be addressed.

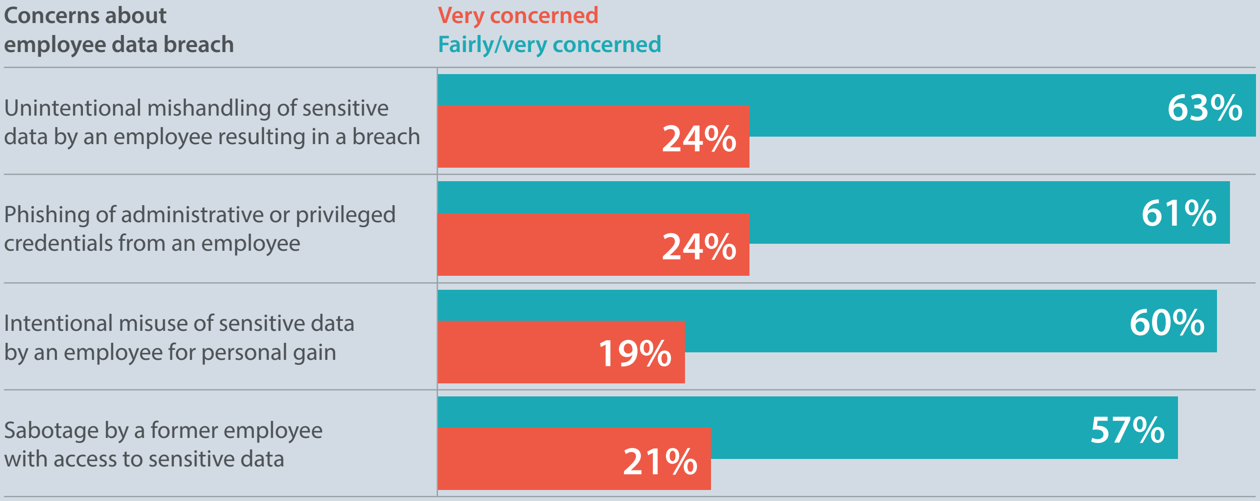
Whether intentional or not, this kind of behavior poses an insider threat that is a genuine concern for businesses (Fig. 4), with only two in five (**41%**) respondents having complete trust in insiders with access to privileged accounts. The research highlights the fact that the majority of organizations continue to lack the oversight required to effectively address these concerns and manage their privileged users and accounts in a way that significantly reduces their vulnerability.

Only **35%** have complete visibility of which insiders have privileged access

Only **37%** have reporting on individual user activity tied to privileged insider accounts

Only **34%** can identify specific threats from insiders with privileged access

Fig. 4
Concerns about employee data breach



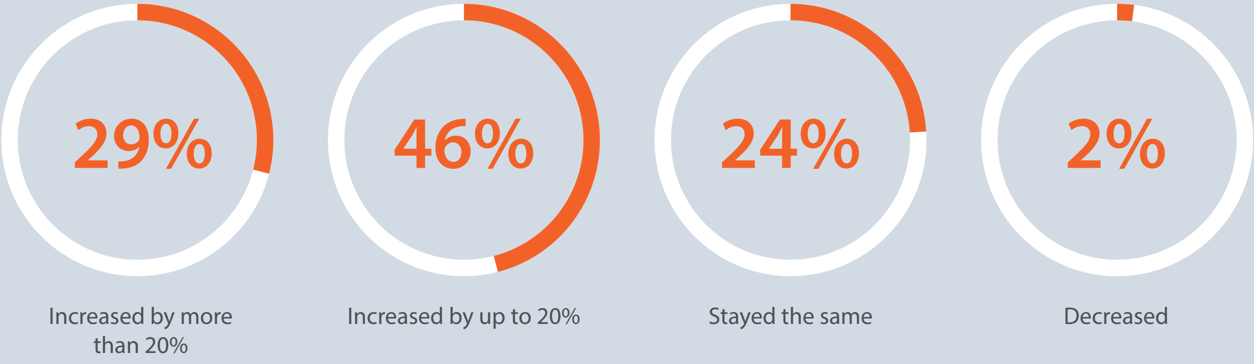
THE 'THIRD-PARTY' RISK

Also posing a risk to organizations are third-party vendors with privileged access. The proliferation of those third-party users is becoming increasingly difficult for organizations to manage, further increasing risk.

As we see in Fig. 5, the rise in third-party vendor numbers is significant, with **75%** of organizations increasing the number of vendors accessing their IT systems by up to or more than 20% in the last year. In addition, only **38%** are very confident they can keep track of the number of vendors with privileged identities and access, and only **35%** are very confident they can keep track of vendor log-ins. The statistics demonstrate that monitoring the number of third-parties with some level of access to IT networks is becoming more challenging, increasing the risk of a breach.

The growing risk from third-party vendors is a problem for organizations of all sizes. Our respondents included organizations with employees ranging from 200 all the way up to 5,000 employees, but the proliferation of third-party vendors was common to all of them. In small to medium enterprises (200-499 employees), over a quarter (**26%**) have the same number of third-party vendors logging in to their network in a typical week as they have employees. In large enterprises (5,000+ employees), around one in every eight don't know how many vendors are logging in to their network in a typical week.

Fig. 5
Change in number of vendors accessing IT systems

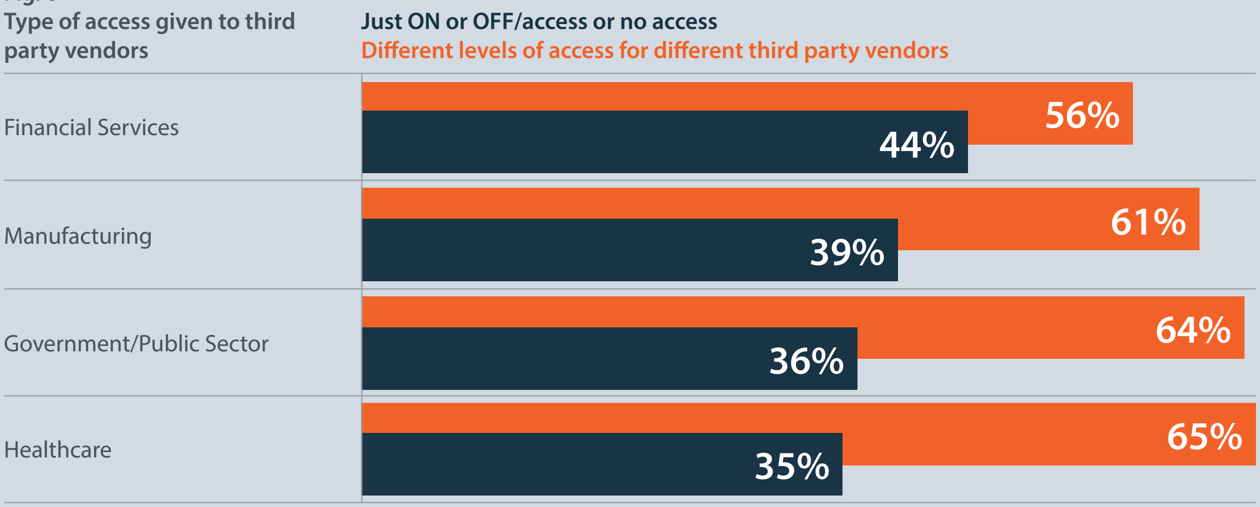


THE 'THIRD-PARTY' RISK

As with last year's report, risks posed by third-party vendors remain high. Sharing an organization's network passwords amongst their own team still tops the list, with 76% of businesses saying it's a significant or moderate risk. Also high on the list was a lack of secure data management due to third parties not recognizing the importance of data security (76%), along with vendors outsourcing work to sub-contractors and therefore widening exposure (73%). It could be said that a large part of the risk also sits with the organizations themselves, as they report that they rely on third-party vendors too heavily (73%) and have cultures that are essentially too trusting of partners (72%).

One way of managing this risk is tailoring the type of access granted to third-party vendors, but we found that only slightly more than half of organizations (56%) follow this practice. And while the level of exposure from insiders is highest in financial services organizations, the tailoring of third-party privileged access was found to be lowest in that sector (Fig. 6).

Fig. 6
Type of access given to third party vendors



IV: CONTROL, CONFIDENCE, SECURITY

CONTROL, CONFIDENCE, SECURITY

As this research shows, some organizations are managing the insider and third-party risk with an automated privileged identity and access management (PIM/PAM) solution. It can be concluded that those organizations experience less severe security breaches and have better visibility and control than those who use manual solutions or no solution at all. As we see in Fig. 7, less than half (**44%**) of organizations using PIM/PAM have experienced a serious breach or expect to in the next six months, compared to **69%** of those without control of their privileged users.

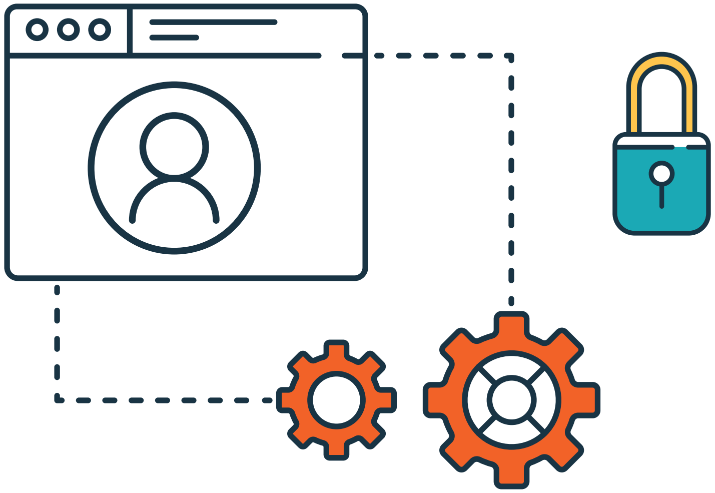
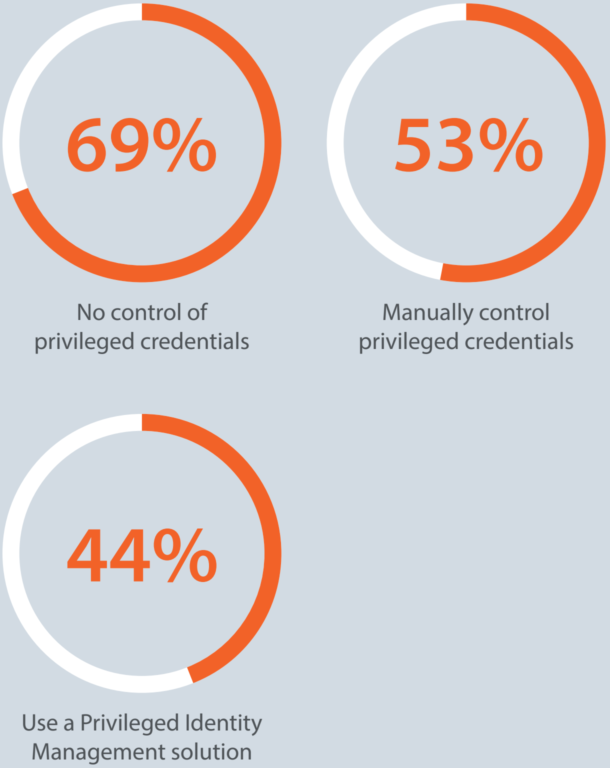


Fig. 7
% who have had a serious breach or expect to in the next 6 months



CONTROL, CONFIDENCE, SECURITY

Fig. 8 and Fig. 9 show how many security breaches organizations have experienced split by insider and third-parties. In both cases, organizations using a PIM/PAM solution to manage their privileged users and accounts reported experiencing significantly fewer security breaches.

Earlier we noted that organizations lack confidence in their ability to know which employees have privileged access, as well in their ability to report on individual user activity and identify specific privileged user threats.

Fig. 8
Experience of cyber breach from employees in the last year

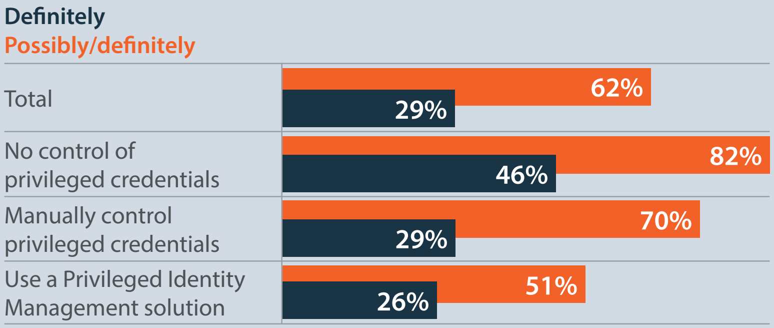
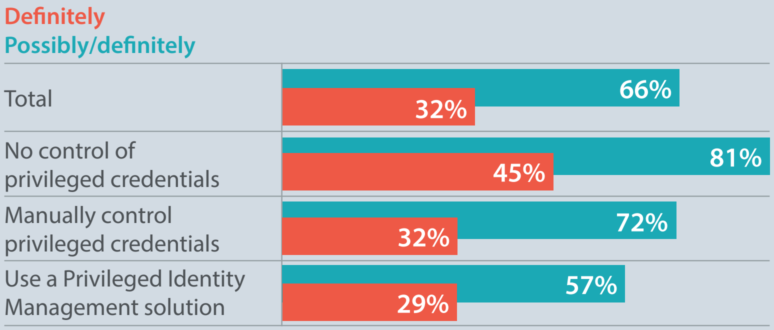


Fig. 9
Experience of cyber breach from third parties in the last year

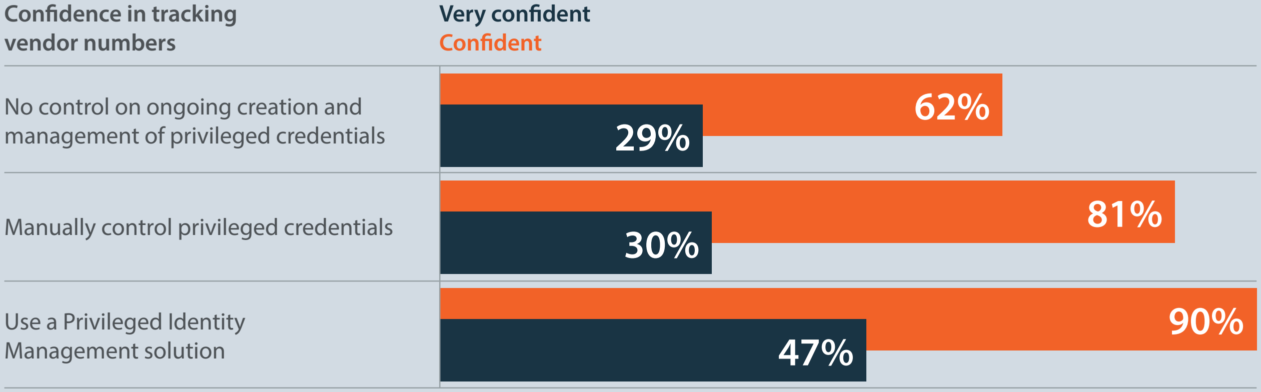


CONTROL, CONFIDENCE, SECURITY

The good news is that compared to organizations with manual or no controls, those using a PIM/PAM solution have much greater confidence in their visibility and their ability to detect threats. For example, **43%** of businesses using PIM/PAM are confident they could identify specific threats from employees with privileged access compared to **24%** with no control of privileged users and **26%** with manual controls. It's particularly interesting to note that using manual controls offers little more control and visibility than using no controls at all.

It's a similar story when it comes to the visibility of third-parties accessing an organization's systems. As we see in Fig. 10, organizations using a PIM/PAM solution are confident they're better able to track the number of vendors with privileged identities and access, as well as the frequency with which they log in to the organization's IT environment.

Fig. 10
Confidence in tracking vendor numbers



V: PROTECTING PRIVILEGED IDENTITIES AND ACCESS FROM THREATS

PROTECTING PRIVILEGED IDENTITIES AND ACCESS FROM THREATS

This research shows that crucial issues remain when it comes to the ways organizations manage privileged insider and third-party access to their systems. Risks posed by compromised or misused privileged identities and access continue to increase as cyber-attacks evolve and compliance mandates intensify. Although data breaches are inevitable, security and IT professionals need to implement controls and least privilege policies to contain attacks and mitigate damages.

Today, organizations of all sizes and across all sectors can reduce their attack surface and better protect their critical data and IT systems with solutions that continuously discover and automate the management of insiders and third parties with privileged access and credentials.

PIM/PAM solutions give organizations greater visibility and control of both privileged insiders and third-party vendors. Selecting a solution that is designed with the user experience in mind can increase the productivity and efficiency of those users, enable the automation of privileged access, and remove the vulnerabilities associated with risky behaviors. Together with ongoing employee training, successful adoption of a PIM/PAM solution allows for the ongoing discovery, protection and management of privileged credentials, improving security and reducing the risk of a primary attack vector.

BeyondTrust