SailPoint

2018 Market Pulse Survey

Balancing Efficiency and Security in Today's Enterprises

www.sailpoint.com

Executive Summary

As data breaches continue to make headlines on a daily basis, IT teams are struggling to secure their organizations and provide employees with the resources they need to do their jobs efficiently. This challenge becomes even more difficult when the rapid digital transformation organizations are undergoing today is taken into consideration. The explosion of users and applications in an organization, migration to the cloud, daily creation of enormous amounts of data and emerging technologies are impeding progress to a more secure enterprise.

SailPoint's 2018 Market Pulse Survey found amidst all the change the corporate world is experiencing – digital transformation is top of mind for many organizations – the way people approach security has not changed dramatically. People still have bad habits when it comes to both corporate and personal security, and some are even actively fighting against their organization's IT department in the search for efficiency. Complicating the situation even more is the development of new threat avenues such as software bots.

Each of these factors – the persistence of poor security choices, tension between IT and business users, and new threat avenues – are driving the need for organizations to address three new frontiers in identity governance, spanning users, applications and data. As such, organizations must adopt a comprehensive identity governance strategy that secures the entirety of today's enterprise: no matter how many or what type of users are onboard, what or where applications are deployed and what type of data or where it is stored.

Research Methodology

The 2018 SailPoint Market Pulse Survey provides a global benchmark into how employees are navigating today's compliance and security challenges. The company commissioned independent research firm Vanson Bourne to interview 1,600 employees at organizations with at least 1,000 employees across Australia, France, Germany, Italy, Spain, the United Kingdom and the United States.

Respondent Breakdown

Industry:	
Retail/Consumer Services	23%
Finance/Insurance	16%
Public Sector	16%
IT & Telecommunications	15%
Manufacturing/Construction	15%
Energy, Oil/Gas & Utilities	5%
Other	10%

Organization Size:	
1,000 – 4,999	35%
5,000 – 9,999	16%
10,000+	49%

Location:	
United States	400
United Kingdom	200
Germany	200
France	200
Italy	200
Spain	200
Australia	200

Age:	
18 – 25	7%
26 – 35	25%
36 – 45	25%
46 – 55	23%
Over 55	20%

Key Findings

Users’ Bad Habits Persist:

Despite the risks, many employees are still not adhering to cybersecurity best practices – and in some cases, bad habits not only persist but are getting worse.

- Three in four (75%) respondents reuse passwords across different accounts. This is a practice that is becoming more frequent over time – in 2014, only 56% admitted to reusing passwords.
- Almost half (47%) of respondents duplicate passwords across work and personal accounts.
- One in five respondents (23%) change their work passwords two or fewer times per year. This is considerably better than for personal accounts, however, where over two-thirds (67%) of respondents change their password as infrequently.
- Around one in seven (15%) respondents would consider selling their workplace passwords to a third party.

Friction Between IT and Business Only Increases:

The frustration employees feel when it comes to IT and their mandates leads to security concerns as employees look for ways to get around security measures.

- Over half (55%) of respondents stated their IT department can be a source of inconvenience in their organization.
- Around one in three (31%) respondents say that they (or one of their colleagues) have purchased and/or deployed software without IT’s help, an 11% increase in the past 4 years.
- If respondents had reason to believe that they had been hacked, 13% would not tell IT immediately, potentially making a bad situation much worse.
- 49% of respondents would actually blame the IT department for a cyberattack if one occurred as a result of an employee being hacked.

New Threat Dynamics are Emerging:

With the rapid changes brought on through the digital transformation, bad cybersecurity habits must be addressed before new technologies create even more exposure points for organizations to address, which is difficult as employees remain focused on themselves.

- Just under half (48%) of respondents are either already using AI chatbots/personal assistants in some form, or are planning to do so, with over one in ten (13%) already using these in the workplace to increase efficiencies.
- Regulations such as the General Data Protection Regulation (GDPR) may be relatively new, but are largely unknown for the majority of users: 66% of respondents did not know what the GDPR is or what it entails, and even fewer (63%) believe every employee plays a role in compliance.
- In the simplest terms, people are looking out for themselves. 44% of respondents would rather that the personal information of their company’s customers was hacked than their own personal information.

Users’ Bad Habits Persist

75%
of respondents reuse passwords across different accounts

In the face of constant, widespread change, many things end up staying the same. Unfortunately for enterprise security, one of those is the persistence of users’ bad habits. In previous years’ Market Pulse Surveys, SailPoint found poor password hygiene and other harmful security practices were rampant amongst users. This year is no different, and in fact, the problem has only gotten worse.

19%
growth of password reuse over the last four years

Since we first asked the question 4 years ago, the reuse of passwords for multiple accounts has grown nearly 20%. While the practice is understandable in terms of efficiency – the number of unique passwords one should be using can easily reach the double digits – poor user password hygiene is a major problem for organizations. With the amount of data breaches that target and then obtain sensitive information like user credentials, the reuse of passwords even just within an organization can grant hackers access to systems they may not have had otherwise.

47%
of respondents duplicate passwords across work and personal accounts

The problem extends even further when users are reusing their passwords between personal and corporate accounts – which nearly half (47%) of respondents are. This means that when a data breach occurs on a website where users are logging in with personal account credentials – like LinkedIn or Dropbox, the enterprise could also be at risk due to these exposed user credentials. Once stolen, a user’s credentials are often made available to hackers on the dark web and can be used again and again to carry out future cyberattacks on personal or corporate accounts.

Completing the trifecta of users’ bad password practices is the infrequency with which those passwords are changed. More than one-fifth of respondents do not change their password more than twice per year for their corporate accounts, with nearly a quarter of those never changing their passwords at all. Nevertheless,

23%

of respondents change their work passwords **2 or fewer times per year**

The same is true for

67%

of personal account passwords

personal account passwords are changed exponentially less, with more than two-thirds of respondents not changing their password more than bi-annually. As discussed previously, while the corporate accounts are slightly more secure than the personal ones, the other bad habits users have – especially with account password duplication – make this practice a particularly dangerous one.

While the goal of efficiency versus security with regards to passwords seems to always be at odds, the blatant disregard for security is most frightening. Throughout the years, the answer to our question of the potential sale of passwords has been fairly consistent with about one in seven stating they would sell their password. Yet again, 15% of this year's respondents answered they would provide their password in exchange for monetary compensation, with a few accepting less than $100.

15%

of respondents would sell their workplace password to a third-party

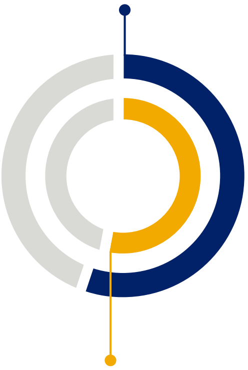
A New Generation of Password Challenges

Despite their technological prowess, the 18 – 25 age group were found to have the worst password practices. Each of the bad habits we questioned had higher percentages among the younger generations, especially the amount of whom would sell their password to a third party. While there could be many reasons for this, including just a lack of compassion for company security, the simple truth is as younger generations join corporations and become a larger part of the user population, the future is very uncertain for corporate security.

- **87%** of 18 – 25 year-olds reuse passwords across different accounts compared to **75%** of all employees
- **60%** of 18 – 25 year-olds use the same password across work and personal accounts compared to **47%** of all employees
- **28%** of 18 – 25 year-olds would provide their passwords to a third party compared to **15%** of all employees and just **4%** for those aged over 55

55%

of respondents state the **IT department is a source of inconvenience**



53%

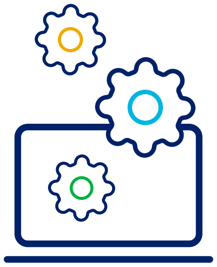
of respondents state that **enterprise security measures make their job more difficult**

The unsecure and frankly, lazy password practices of today's employees make properly securing any enterprise that much more difficult. When users are only concerned with increasing their efficiency and unconcerned with the security holes their bad habits create, enterprises must respond to attempt to correct the issues. But unfortunately for many organizations, the efforts their IT team is making to protect the enterprise are only exacerbating the problem.

Friction Between IT and Business Only Increases

Usually there are two sides to any story, and in the case of enterprise security, it often ends up being IT versus the business. While the former creates the necessary policies and procedures to keep the organization secure, the business users feel frustration as their efforts to procure software and work more efficiently are constricted. This constant battle between security and efficiency has led to distinct friction between the IT and business sides of enterprises today.

In fact, over half (55%) of this year's survey respondents stated their IT department can be a source of inconvenience in their organization, and nearly the same amount of people (53%) stated the security measures their organization enforces result in their job being more difficult to perform.



31%

of respondents state they or a colleague **have procured software outside of IT's purview**

The negative impact of the frustrations with security policies and procedures has led to employees searching for a way around the IT department. Around one-third of respondents stated they or one of their colleagues had purchased software without the help or knowledge of IT (a practice commonly referred to as shadow IT). Since first asking this question of survey respondents in 2014, we have seen a marked increase of 11%, signifying the problem is only getting worse, and IT is losing the battle.

13%

of respondents **would not immediately inform the IT department in the event of a data breach**

48% of respondents are either already using or planning to use AI bots

13% of respondents are using bots in a workplace setting

66%

of respondents do not know what the GDPR is or what it covers

While efforts to skirt IT are often not done for malicious reasons, and instead to take advantage of new technologies to increase work efficiency, the simple fact is these efforts increase risk for the organization. With that increased risk comes a better chance for a data breach to be successful and the organization to be compromised. In an effort to better understand how employees felt about such an event, we asked what their response would be if they found they had been hacked. The disheartening result is that more than one-tenth of respondents (13%) wouldn't immediately tell their IT department.

Perhaps the most unsettling result is that even though users don't want to heed IT's warnings or follow their policies, only 40% of respondents would feel personally responsible if their company suffered a cyberattack as a direct result of an employee being hacked. 49% of respondents would actually blame the IT department for the attack. The dissonance between these two sides of an organization is only creating opportunities for hackers and other malicious threats. This battle between efficiency versus security, as well as between IT and the business, cannot continue if enterprises are to effectively secure themselves.

New Threat Dynamics are Emerging

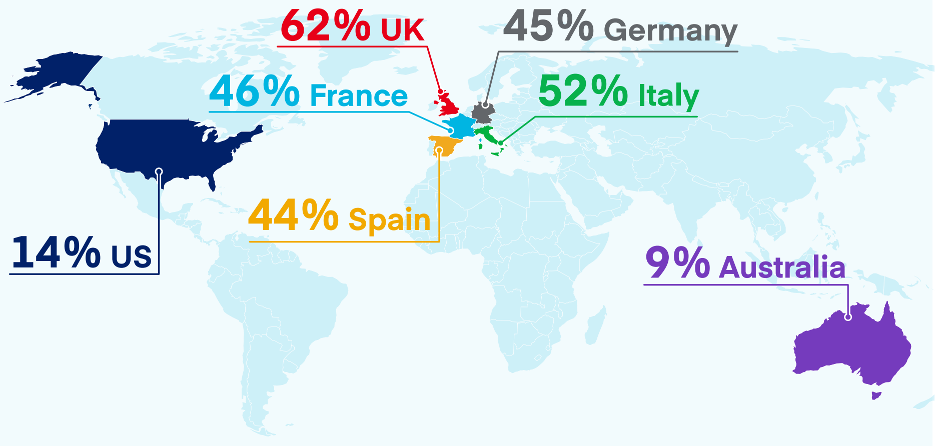
In addition to the same struggles organizations have been facing for years, the constant evolutions in technology are bringing about new avenues of risk. Users are a top target for hackers today, and even the definition of "user" is rapidly changing. Enterprises are increasingly adopting software bots powered by robotic process automation (RPA) and granting them the same types of access as their human counterparts. Just under half of respondents (48%) are either using or planning to use AI chatbots and personal assistants such as

Apple's Siri and Microsoft's Cortana. More than one-tenth of Respondents are already using these in their organization to increase their work efficiency.

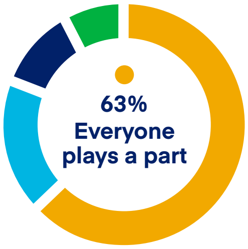
At the same time, corporate data stored in files is increasing exponentially, and employees have unprecedented – and often unlimited – access to it. Enterprises are struggling to understand where their sensitive data resides, much less attempt to manage and secure it. With new regulations such as the GDPR and California Consumer Privacy Act, it is imperative that organizations get a handle on this sensitive data. Unfortunately, we found that many employees do not yet understand the legal implications of data mismanagement, which could be damaging for their organizations. For instance, nearly two-thirds of respondents (66%) did not know what the GDPR is or what it covers.

Understanding of the GDPR Differs Drastically Based on Country

Respondents from the **UK were the most likely (62%)** to have a good knowledge of what it is and what it covers, followed by **Italy (52%)**, **France (46%)**, **Germany (45%)** and **Spain (44%)**. However, only a minority of respondents from **Australia (9%)** and the **US (14%)** share this understanding. While this is not surprising given the GDPR is a mandate from the EU, it applies to all countries with customers in the EU, meaning virtually every global organization is subject to its rules and repercussions.



Who's responsible for GDPR compliance?



- ● 18% IT
- ● 11% HR
- ● 8% Not Sure

44%

of respondents stated they would rather see customer information hacked versus their own

24%

of respondents **would share their SSN**

VS

27%

of respondents **would share their customers' SSNs**

The level of disillusionment with personal responsibility extends to the situation where, even after learning what the GDPR requires of organizations, only three in five respondents (63%) believe it is something in which every employee plays a role. 18% of respondents felt it was solely the IT department's job to ensure compliance and 11% pointed the finger at HR. So, while organizations are struggling with securing the new frontiers of both users and data, the actual enterprise employees are complacent in their own responsibility towards achieving that security.

Unfortunately for organizations, employees are focused more on protecting their own personal data instead of that of their customers. More than two-fifths of respondents (44%) stated they would rather customer personal information was hacked instead of their own. In fact, when asked if they would share Social Security Numbers (SSNs) with co-workers, 24% of respondents stated they would share their SSN, but 27% said they would share their customers' SSNs.

These statistics paint a rather grim picture of the current state of enterprise cybersecurity today, especially when it comes to employees and their behavior. IT teams are struggling to address these bad habits while also keeping pace with the digital transformation – no simple task. With findings like these, it can seem like an unwinnable battle for organizations. However, there is a solution that can address the needs of employees and IT teams without disrupting business, ultimately securing the enterprise.

The New Frontiers of Identity

USERS

APPLICATIONS

DATA

The struggle between security and efficiency, persistence of poor security practices, advancements in technology that are creating shifts in security paradigms, and the lack of concern felt by enterprise users with regards to corporate data are all creating a perfect storm that can only be addressed with identity governance. Deploying an identity governance program can help organizations enable and secure their digital identities in order to reduce risk, grant full visibility over **all users, applications and data**, and better protect the organization against threats such as data breaches.

It's only through a comprehensive identity governance strategy that organizations can address each of the issues we discovered in this year's report: cleaning up user password hygiene, alleviating the stress between the IT and business departments, and addressing the concerns that come from new technologies entering the enterprise. With a user-centric cybersecurity strategy powered by identity, organizations can achieve not only efficiency, but also security.

This comprehensive program can also fully extend to cover the new frontiers of identity:

- Traditional users as well as software bots
- Thousands of applications both on-premises and in the cloud
- Zettabytes of data, no matter whether it's stored in structured systems like applications and databases such as CRM, HR, and financial systems or in unstructured systems such as file shares like SharePoint, and cloud storage systems, such as Box and Google Drive

The power of identity enables organizations to secure the digital identities of all users across all applications and all data, which is SailPoint's vision and the only secure path forward for global enterprises today. To learn more, visit us at **www.sailpoint.com.**

SAILPOINT: THE POWER OF IDENTITY™

sailpoint.com

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies.