2016 MARKET PULSE SURVEY

Weak Security Practices Leave Organizations Exposed

SailPoint

Executive Summary

The cyber threat landscape is infinitely more complex and dangerous today than it was even a few years ago. In fact, the world experienced data breaches as it never had before in 2015 thanks to their sheer volume, size and reach. Countless media and news outlets offered their analysis, while consumers and companies alike were left scrambling to check their inboxes and websites to see if their information had been stolen. Breaches became so frequent, in fact, that organizations around the world began realizing a startling truth: being affected by a data breach is no longer a matter of "if" but "when."

The security perimeter for organizations all over the world has evaporated: breaches are now an inevitable reality for every organization. These breaches can spread quickly, wreaking havoc on the business targeted, while often causing harm to employees, customers, partners and investors. At the same time, data breaches became more personal than ever before. Sophisticated attacks penetrated virtually every aspect of our personal lives, going well beyond stealing financial information and venturing into health records and even the information stored by children's toy companies.

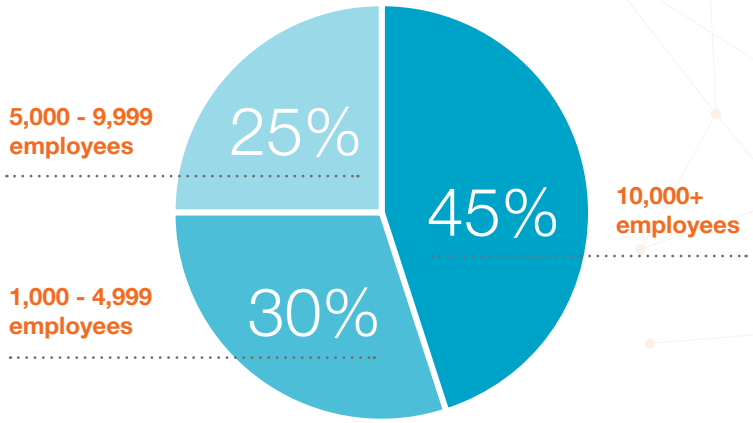
One would think that as more breaches touched more people individually, they would be more vigilant about security processes. But, in a stark contrast, it seems that while they expect their personal information's safety, when functioning as employees, these same users are practicing security incredibly ineffectively, leaving themselves and their employers exposed.

As the business world evolves into one with no physical borders, and employees expecting to use their personal devices to access work-related applications, IT and security organizations are struggling to keep up. The alacrity with which employees move or leave positions in the company, purchase SaaS applications (even outside IT's purview), and upload information to cloud applications is staggering.

This year's Market Pulse Survey was designed to measure two aspects of this situation: how employees view their individual role in IT security processes, and what (if any) improvements are being made by organizations to adapt to the new business realities.

Research Methodology

The 2016 SailPoint Market Pulse Survey was conducted by Vanson Bourne, an independent research firm. They interviewed 1,000 office workers at private organizations with at least 1,000 employees across Australia, France, Germany, the Netherlands, the United Kingdom, and the United States.

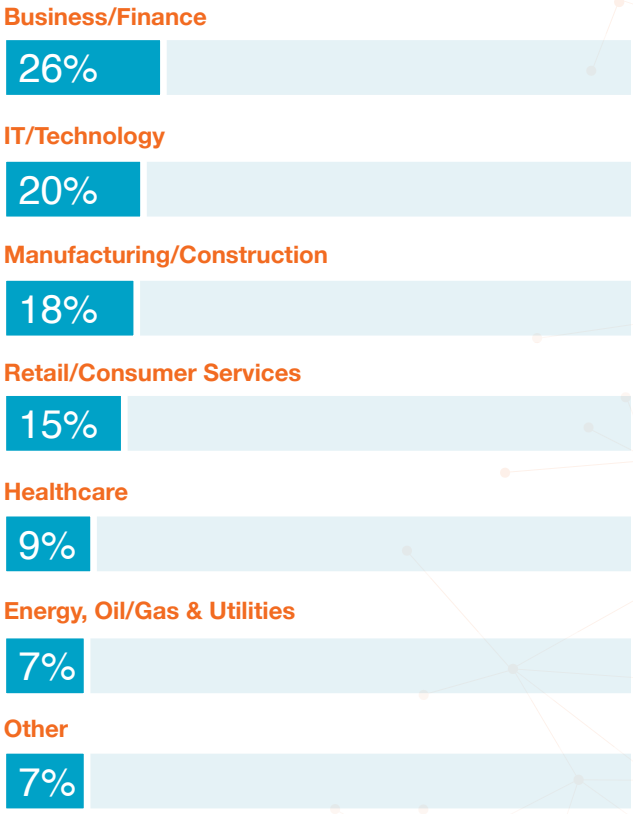


Respondent percentages by organization size

Respondent percentages by organization industry

Geographic Regions:

United States (US)	400 respondents
United Kingdom (UK)	200 respondents
Germany (DE)	100 respondents
France (FR)	100 respondents
Netherlands (NL)	100 respondents
Australia (AU)	100 respondents



Key Findings

Poor password hygiene and negligence continue to plague the enterprise.

- The majority of respondents (65%) admitted to using a single password among applications.
- One-third share passwords with their co-workers.
- One in five employees would sell their passwords to an outsider.

Data breaches became personal.

- One-third of respondents have been impacted on a personal level by recent data breaches.
- 85% of employees would react negatively if their personal information was breached by a company.
- 84 percent of respondents are concerned that incredibly sensitive information about them is being shared.

Organizations are struggling to keep up, and are exposed in the meantime.

- One in three employees admitted to purchasing a SaaS application without IT's knowledge (a 55% increase from last year's report).
- More than 40% of respondents reported having access to a variety of corporate accounts after leaving their last job.
- 26% of employees admitted to uploading sensitive information to cloud apps with the specific intent to share that data outside the company

Poor Password Hygiene Continues

In last year's survey, we were astonished to see that not only were respondents willing to sell their passwords to a third-party (1 in 7), but they were willing to do it for as little as $150. 20% shared passwords with their co-workers, and a little more than half (56%) shared passwords among applications. This year, even among a larger concern for their personal information's security, the percentage of those willing to risk corporate data either through apathy, negligence or financial gain only increased.

Percentage increase between this and last year's respondents

62% share credentials among co-workers

42% would sell their password to a third-party

16% use only one password among applications

This year, we found that 1 in 5 respondents would sell their passwords to a third-party organization and a staggering 44% of them would do it for less than $1,000. Even more concerning? Some would sell their corporate credentials for less than $100.

Respondents who would sell their passwords to a third-party

US: 27%

UK: 16%

DE: 20%

20%

GLOBAL RESULTS

FR: 16%

NL: 12%

AU: 12%

Respondents who would sell their passwords for less than $1,000

44% GLOBAL RESULTS

40% US

56% UK

45% GE

50% FR

33% NL

42% AU

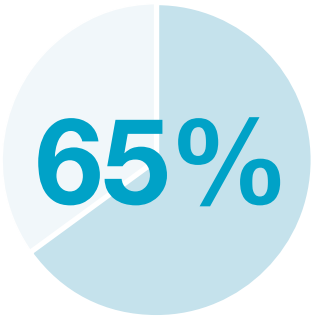
The lethal combination of shared passwords not only among applications but also among co-workers also increased: 65% use a single password among applications and 1 in 3 share credentials with other employees.

Respondents who use a single password among applications

US: 65%

UK: 63%

DE: 53%



FR: 73%

NL: 68%

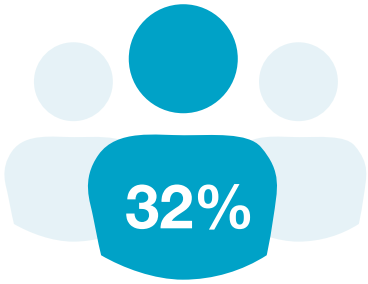
AU: 64%

Respondents who share passwords with co-workers

33% US

28% UK

32% GE



38% FR

38% NL

21% AU

Considering the average organization size for the corporations from which our respondents are employed is about 50,000, that means it's possible that 10,000 users at any of those enterprises would sell their password, and 4,400 sell theirs for less than $1,000. 32,500 **share passwords among applications** and nearly 17,000 share passwords with their co-workers.

Employees who would engage in insecure password practices in a 50,000-employee organization

32,500
would share passwords among apps

17,000
would share password with co-workers

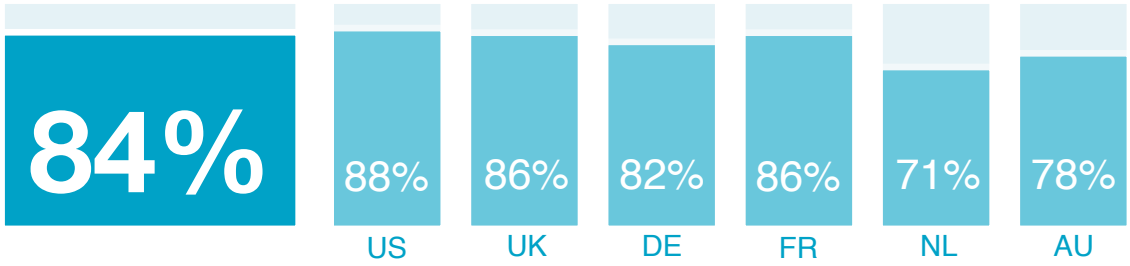
10,000
would sell their password

Data Breaches Became Personal

Even as respondents seemed to place varying levels of concern over the security of their organization's data, nearly all were concerned about their own personal information. A large majority, 84%, were concerned that their personal information was being shared by corporations with which they do business.

As breaches have become more common, it only makes sense for them to affect a larger part of the population. In fact, almost a third (32%) of respondents have been impacted by recent data breaches.

Respondents who are concerned their personal information is being shared



Respondents who have been affected personally by breaches

US: 44%

UK: 28%

DE: 19%

32%

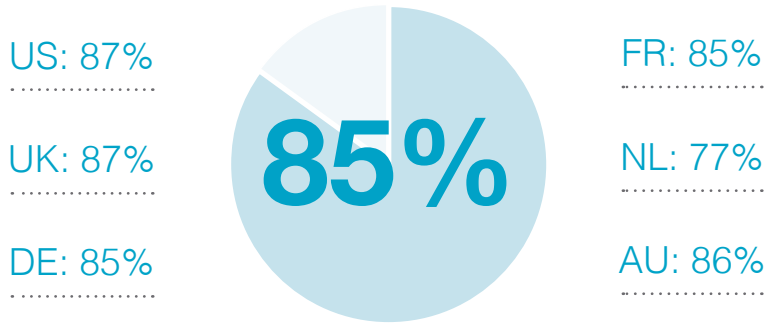
FR: 37%

NL: 22%

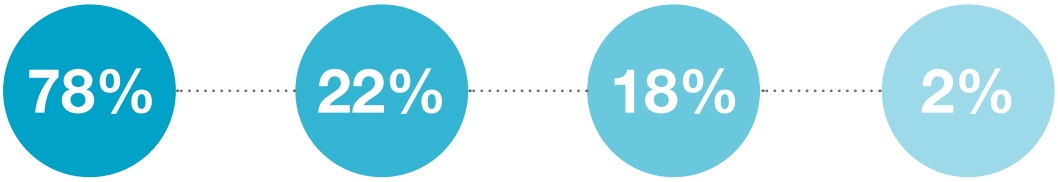
AU: 14%

Consumers are responding to data breach occurrences in the most effective way they know how: with their business. 85% of respondents in our survey stated they would react to a company with whom they do business were breached, including cutting off relations entirely.

Respondents who would react to a company's data breach



Respondents' actions after learning of a data breach



These results underscore that there is a disconnect for employees: while data breaches in and of themselves are affecting them personally, these same employees may be causing potential security breaches with poor password hygiene and circumvention of the IT department.

Organizations are Struggling to Keep Up

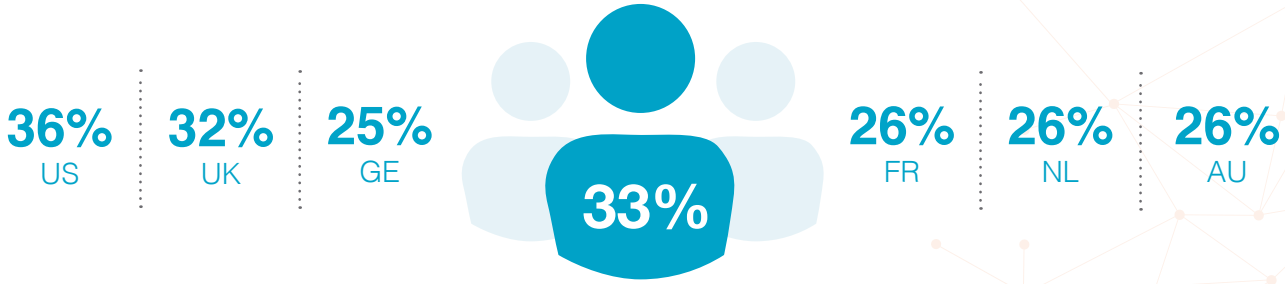
It's not just employees that are posing security risks for the organizations, however. Proper password policies and automated on- and off-boarding procedures can help to mitigate some of the security risks that come from provisioning and application usage. Unfortunately, our survey found that in a large portion of organizations, this simply isn't happening.

Of those where they had access to corporate accounts and/or information, more than 2 in 5 people could access those same accounts and data after they had left their previous employer.

Respondents who could access corporate accounts and data after termination

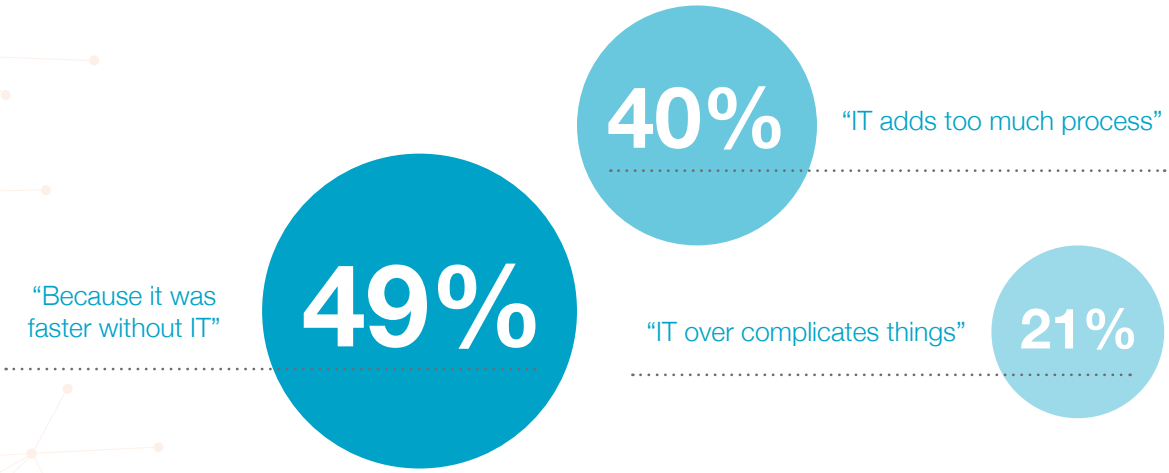
Even more troubling is that these are only the applications and accounts IT knew about. More employees, 1 out of every 3, are purchasing and using cloud applications, in particular, outside of IT's purview. And this phenomenon is only becoming more frequent. This year alone is a 55% increase over what our survey reported last year.

Respondents who purchased SaaS applications without IT



Users are circumventing the IT department for a number of reasons, largely time-based. Half of respondents who purchased a SaaS app without involving IT did it simply "because it was faster." 40% stated that IT adds too much process, and 21% believed that IT over-complicates simple purchases.

Reasons why apps were purchased without IT's involvement



On top of all this, 1 in 4 respondents also reported that they have uploaded sensitive documents to the cloud, specifically to share outside the company, 70% of which upload such documents on a regular basis. Combined with a lack of visibility and excess permissions once an employee has left, not to mention the leniency with which credentials are kept and used, the future could be scarier than we once imagined.

Respondents who upload sensitive information to the cloud and do so on a regular basis

Why this Matters: Identity is Everything

If the most recent data breaches have shown us anything, it's that no company is safe from attacks, and the method by which information is taken is slowly changing. The commonality across almost every breach is hackers are now targeting the weakest link in the security infrastructure: people.

The reason? The digital identity of an individual user is the key that unlocks corporate data and applications. Each identity and interaction between that individual user, a data source, an application (or even between applications) and a device creates another potential entry point for a breach. To complicate matters, these points of exposure are dynamic, constantly changing and extend beyond the physical walls of the enterprise to customers, partners, vendors and contractors.

The key to managing this complex and ever-shifting reality is to manage those identities. Put simply: identity is everything.

SailPoint's Market Pulse Survey brings to light several ways in which companies and users are practicing security ineffectively. For example, while not nefarious in nature, the simple act of poor password hygiene presents great risk to organizations. Now, not only are IT organizations trying to address attacks on their own company, but consumer-facing breaches could leave them exposed if employees are reusing their passwords across networks.

What's more challenging is addressing the growing trend of BYOD and shadow IT, whereby employees access company data that resides in the cloud from their personal devices – all outside the traditional "perimeter." Organizations need to strike a balance between providing the level of convenience the employees require (and expect) while also ensuring that proper IT and security controls are in place. Corporate security and business agility can no longer be competing priorities, but instead must be interwoven.

Finally, in order for companies to truly manage and secure the identity data, the end users must be involved in security processes. SailPoint believes this goes beyond educating employees on the corporate policies in a way that makes each individual act as a shepherd of the company's data, treating it in the same way they clearly expect companies to treat their own information. Just as organizations need to be committed to ensuring the proper security policies and IT controls are in place, it's imperative that employees understand the implications of how they practice those policies.

Identity is everything. And sometimes, it's the only thing standing between an organization and the next significant data breach.

About SailPoint

As the fastest-growing, independent identity and access management (IAM) provider, SailPoint helps hundreds of global organizations securely and effectively deliver and manage user access from any device to data and applications residing in the datacenter on mobile devices and in the cloud. The company's innovative product portfolio offers customers an integrated set of core services including identity governance, provisioning and access management delivered on-premises or from the cloud (IAM-as-a-service). For more information, visit www.sailpoint.com.

Corporate Headquarters

11305 Four Points Drive
Building 2, Suite 100
Austin, Texas 78726

512.346.2000
USA toll-free 888.472.4578

www.sailpoint.com