SailPoint

2017 Market Pulse Survey

Identity is the Path Forward to Secure Organizations

www.sailpoint.com

Executive Summary

The 2017 SailPoint Market Pulse Survey explores how enterprises are changing their approach to security, amid an evolving threat landscape that sees almost daily announcements of data breaches, including some of the largest ever recorded. There are now countless ways into the corporate network today – the traditional network perimeter as we know it has dissolved. New technologies and evolving policies alter the way we're working. They change with whom we're working and how we're working with them. While those surveyed believe they'll be breached, they are also ill-equipped to counter that vulnerability.

But with these challenges, there is a silver lining: enterprises are increasingly realizing that there remains one thing that links all of this together and that is identity. Because users are who hold the keys to accessing an organization's sensitive information, securing the enterprise must start with them. Once enterprises stop simply reacting to events and instead, proactively mitigate security incidents, businesses can feel empowered to move forward securely and confidently. That is the path forward to secure organizations in 2017.

Research Methodology

The 2017 SailPoint Market Pulse Survey provides a global benchmark into how IT decision-makers are navigating today's compliance and security challenges. The company commissioned independent research firm Vanson Bourne to interview 600 senior IT decision-makers at organizations with at least 1,000 employees across Australia, France, Germany, Italy, the United Kingdom and the United States.

Respondent Breakdown

(Industry, Organization Size & Location)

Industry:

Finance/Insurance	24%
IT & Telecommunications	19%
Manufacturing/Construction	18%
Retail/Consumer Services	13%
Public Sector	12%
Energy, Oil/Gas & Utilities	5%
Other*	9%

*includes healthcare, media, pharmaceuticals and higher education

Organization Size:

1,000-4,999	38%
5,000-9,999	20%
10,000+	42%

Location:

United States	200
United Kingdom	100
Germany	100
France	100
Italy	50
Australia	50

Key Findings

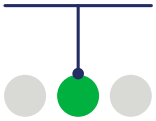
1 **Data breaches are the cost of doing business today:**
3 in 5 enterprises fully expect to be breached in 2017, and a third expect they won't even know it when it happens. They acknowledge that breaches leave a gaping security hole, but also hurt the bottom line. Enterprises surveyed admitted that they lost, on average, over $4 million as a result of a data breach in 2016.

2 **Lack of visibility is leaving enterprises exposed:**
While enterprises we surveyed understand the data breach threat, they struggle with visibility. This includes a clear view into who has access to what, with less than half of respondents having full knowledge of all users and their access to corporate applications and systems. This lack of visibility also applies to understanding and managing access to sensitive data stored in unstructured files and who within their organization is employing technologies like mobile and shadow IT to access sensitive corporate applications, files and systems.

3 **Identity is the path forward:**
At the same time, there is some good news to report: almost all (87 percent) respondents understand the importance of having strong identity governance controls in place across their organization's entire IT infrastructure.

Data Breaches are the Cost of Doing Business Today

3 IN 5
expect to be breached

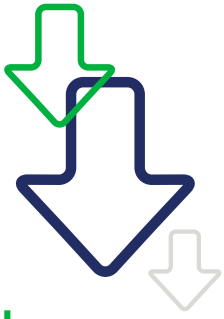


1/3
believe they won't know when it happens

With the surge in data breaches in 2016, it's become an almost daily occurrence to see yet another company derided in the headlines for a data breach impacting not just tens of thousands, but hundreds of thousands of consumers. While there is a preconceived notion that data breaches are bound to happen, visibility became a real issue for businesses in 2016. 3 in 5 respondents admitted that they fully expect to be breached this year, but a surprising one-third of them believe they won't even know it when it happens.

There is also growing risk from the general lack of visibility into what constitutes the majority of an organization's information – unstructured data – coupled with a lack of clear visibility into who has access to what across the organization, leaving a large security gap for enterprises today. And it's a costly gap – with global enterprises reporting an average of $4.1 million in financial loss due to a security breach in the last year alone.

Lack of Visibility Leaves Enterprises Exposed



$4.1m
IN LOSSES
DUE TO A SECURITY BREACH

Hand-in-hand with the potential for a data breach occurring unbeknownst to the organization, there is likewise a lack of visibility into an emerging exposure point for organizations today: unstructured data and who has access to that data. Unstructured data (i.e. emails, files, documents, PDFs, etc.) lives outside the structured corporate systems and applications, which makes it harder to manage for enterprises today. While 6 in 10 of respondents are concerned about managing and safeguarding the sensitive organizational data that lives in unstructured data files, 71% believe they are not equipped to fully protect it.

6/10
are concerned about securing unstructured, sensitive data

71%
are not equipped to fully protect sensitive data

73% would not know their risks if the CEO's email were hacked

<50% have full visibility for all users' access

7/10
organizations embrace BYOD

49%
have formal policies for BYOD & data

9/10
know that their colleagues participate in shadow IT

Further complicating matters is the lack of visibility respondents have into their exposure points overall. Given the hypothetical situation of the CEO's email being hacked, the majority of respondents – 73% – would not immediately know how and where they were at risk.

And, while the majority of respondents acknowledged having at least partial visibility, fewer than half have full visibility for all users and their access to corporate applications and systems.

More concerning still, only 33 percent of respondents could produce a company-wide report within 24 hours on who has access to what resources and what can be done with that access.

Complicating the problem is the fact that the smartphone today is nearly ubiquitous and we use them for almost everything – including work. The enterprise today must be prepared for their users attempting to access and store corporate data on their own personal devices. In this year's survey, we found that while 7 out of 10 organizations have embraced BYOD, fewer than half have formal policies around it for corporate data.

The risk posed by this situation is further exacerbated by the fact that nearly all – 9 in 10 of respondents – are aware that at least some of their employees participate in shadow IT (procuring applications without IT oversight or approval).

While organizations may create policies to govern access that help secure the enterprise, we found that often, there is a disconnect between what is "allowed" and what is actually done. This disconnect between knowing that there is risk – 72% of respondents were concerned about shadow IT and BYOD as organizational exposure points – and the lack of setting policies to minimize that risk is worrisome. Coupled with 3 in 10 respondents citing that their users are simply not following the security guidelines put in place by the organization, it's clear that enterprises need to better outline and enforce corporate security policies, company-wide.

We Are the New Perimeter

72%
cite shadow IT and BYOD as exposure points

3/10
users are not following corporate security guidelines

77% believe that users pose the greatest risk

37%
cite poor password hygiene as increasing their risk profile

6/10 are concerned about third-party user threats

86% have only partial visibility into those users' access

An organization's own employees (including contractor workers) are both their greatest asset and, for 77% of respondents, one of their greatest risks.

But even as it's widespread knowledge that hackers are targeting users as their doorway into the enterprise, employees aren't helping matters with continued poor password hygiene. 37% of respondents cited password hygiene as a big factor into their organization's overall risk profile – with employees either sharing passwords across multiple accounts and systems, not regularly updating or changing their password or not adhering to overall password management policies as they should be doing.

While the way we work has changed with bringing our own devices into the workplace, the workforce itself has also changed. Users of enterprise systems are not just employees of the organization any longer: contractors, suppliers, vendors, partners, customers and other third parties are all part of today's diverse enterprise user base.

6 in 10 respondents are concerned with the threat that third parties, such as contractors, may pose to their organization, but 86% admit they only have partial visibility into the access contractors have to corporate systems and the sensitive data that lies within.

With all the other challenges organizations face, there needs to be a fundamental shift to treat any type of user, regardless if they are internal or external, with the same level of base security and then increase as needed. This risk-based approach to securing the enterprise's users – its identities – is critical.

Identity is the Path Forward

55% cite identity as one of their top investments in the next year

IDENTITY GOVERNANCE BENEFITS:

72%
Enhanced security

71%
More automated and efficient organization

65%
Business enablement

55%
Improved compliance

Respondents name compliance as top reason for identity

73% UK

42% Germany

49% France

The common thread among all of these data points, however, is that enterprises recognize these challenges and now view identity as the center of their security programs. Almost all (87%) respondents understand the importance of having strong identity governance controls in place across the entire organization, and 55% cite identity as one of their top IT security investment priorities in the next year.

The benefits of putting identity at the center of an organizations' security program are very clear. Those who already have an identity governance solution in place cited things like enhanced security posture, a more efficient organization, improved business enablement and improved compliance in the face of increased regulatory pressures like those posed by GDPR, for example. Being able to focus on moving business forward is obviously an important goal in today's fast-paced business environments.

Specific to European respondents, as the GDPR compliance deadline looms, compliance bubbled to the top for the some regions as a key goal and driver behind identity governance programs.

Cybersecurity and identity have become board-level topics of discussion today. Now more than ever, board members are increasingly more involved in how the companies they serve approach cybersecurity and the measures taken to ensure the company is safe from attack. 87 percent of survey respondents place high importance on being able to show their board members that there are strong identity governance controls in place across their entire IT infrastructure. This is an important shift – board members now want proof that the company they serve is secure; instead of simply relying on occasional security updates, they now want security scorecards and benchmarks that measure security posture.

The Power of Identity

In today's technology world, the risks are more complex and attacks more frequent than ever. Many organizations find themselves struggling to grant business users seamless access to an ever-increasing number of applications, while concurrently confronting more frequent and sophisticated cyberattacks. The tough balance between convenience – enabling users to work how they want, where they want – and maintaining tight control over user access has never been more difficult or more critical.

The power that an identity governance program can provide organizations is more than just security. Once enterprises know that through their efforts, the business is safer, more efficient and better protected, they are free to do what they set out to do in the first place: improve the organization.

Today's IT security teams are struggling to manage the explosion of cloud and mobile applications layered on top of the organization's traditional on-premises applications. They must also manage and enable a distributed, global workforce that blurs the lines between employees, contractors and partners.

To make matters worse, it is no longer enough to focus on defending the organization's application infrastructure and network perimeter. As recent security attacks demonstrate, it is becoming more common for identities to become the attack vector for cyber criminals. Instead of targeting networks and application infrastructures, hackers are now exploiting identities to gain access to sensitive systems and data.

The power that an identity governance program can provide organizations is more than just security. Once enterprises know that through their efforts, the business is safer, more efficient and better protected, they are free to do what they set out to do in the first place: improve the organization. Whether that means gaining a competitive advantage, chasing new opportunities for growth, or providing a better experience for its customers, the empowerment organizations gain is what allows them to be confident, fearless and unstoppable.

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 in virtually every industry, including: 9 of the top banks, 7 of the top retail brands, 6 of the top healthcare providers, 6 of the top property and casualty insurance providers, and 6 of the top pharmaceutical companies.

MP1111-1705