TREND STUDY: CYBERSECURITY

Identity and Access Management in the Digital Age

Paul Fisher, Research Director

May 2016

Premium Sponsor — Gold Sponsors — In partnership with

KPMG

CYBERARK

SailPoint

kuppingercole ANALYSTS

PAC
A CXP GROUP COMPANY

TABLE OF CONTENTS

PREFACE

Many enterprises are scrambling to transform their businesses to take advantage of the new digital economy. This transformation journey may often introduce risks, which if not carefully managed, can expose the weaker links in their cybersecurity protection.

The issue can be further complicated by the fact that existing platforms and technologies, including Identity and Access Management (IAM) solutions, which deliver key business processes today were not built to address digital economy imperatives like the Internet of Things (IoT), hybrid cloud, social identities and the obfuscation of the identity perimeter.

For cybersecurity and IAM specialists these are stimulating times because, as they grapple to understand the many vectors of insider risk, the digital transformation opportunity comes knocking hard on the door.

Caught up in this vortex of change, clients are faced with more questions than answers:

- What is the span of the identity perimeter?
- How far apart are the principles of managing enterprise and customer identities (really)?
- Is a single view across internal and external identities possible?
- IAM as a digital transformation critical service – how does it impact delivery, training and adoption?

In association with PAC and KuppingerCole, we have attempted to chart the role of IAM in digital transformation through this study. We hope that this report will engender a greater appreciation of the role of IAM in digital transformation and ultimately help with comprehending IAM's journey into the heart of business transformation.

Manoj Kumar
Principal Advisor,
Cyber Security,
KPMG in the UK

John Hermans
Cyber Security Lead,
Europe, Middle East and Asia
KPMG in the Netherlands

The infographic and the Executive Summary of this study are available at https://www.pac-online.com/trend-study-identity-and-access-management-digital-age.

Please visit our sponsors' websites for further information.

Identity and Access Management in the Digital Age

Paul Fisher
Research Director, PAC UK
May 2016

INTRODUCTION

Keeping enterprises secure and ensuring that only the right people can access data and systems has long been the role of the tens of thousands of Identity and Access Management (IAM) systems installed across Europe.

Traditionally, such solutions have been configured to manage personal identities of employees and have scaled to manage the shift to mobile working, and multiple endpoints.

But today a new challenge is emerging as European businesses, across all verticals, are looking to embrace digital transformation to improve competitiveness, gain efficiencies or get closer to customers and supply chain.

More than just a buzzword, digital transformation is really happening across Europe - as the results of our study show.

But digital transformation will have an impact on existing technologies and processes too. At the heart of keeping the organization secure as it transforms will be secure identities.

However identities in the digital age are likely to multiply exponentially and present themselves in different and more challenging forms. For the first time, businesses are contemplating the role of consumer identities in the enterprise, how they can be managed and how they can be secured. The public sector is contemplating how digital identities can be used to transform public services.

This challenge will, in a very short space of time, be one that senior security and information chiefs across Europe will need to address – if they are not doing so already. They will need to look at how IAM solutions will assist them in managing the identity needs of the digital business.

We believe this study provides valuable insights into how IT decision makers across Europe are preparing to face the new cyber security challenges of identity and access management systems in a changing business environment.

Businesses are contemplating the role of consumer identities in the enterprise.

KEY FINDINGS

The findings shows a significant awareness among senior IT decision makers of the need for IAM solutions that can function securely, while fulfilling the challenges and opportunities of the digital age.

Senior security and information chiefs from banking, insurance, manufacturing, retail, services, telecoms, transport and the public sector across major European territories revealed a concern that the onset of digital transformation could only achieve its benefits if security is baked in.

When questioned on what were the primary goals of their digital transformation strategies, 48% of respondents said threat or breach mitigation was very important.

Shadow IT is emerging as a serious threat to secure IAM deployment in the digital age.

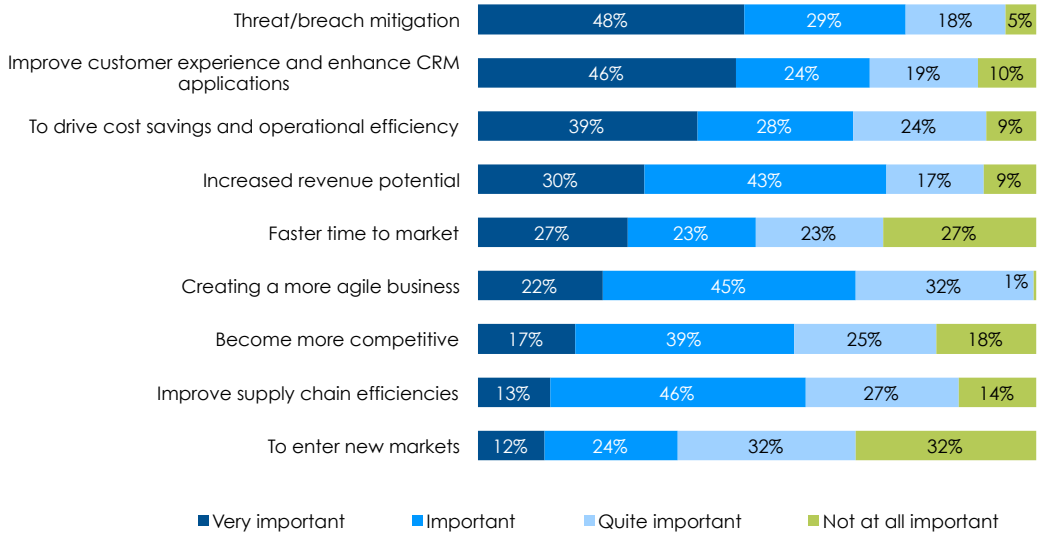

Fig. 1: Importance of individual goals of digital transformation strategies

This was placed higher than improving customer experience or driving costs savings and efficiencies – both expected enterprise priorities for the businesses surveyed.

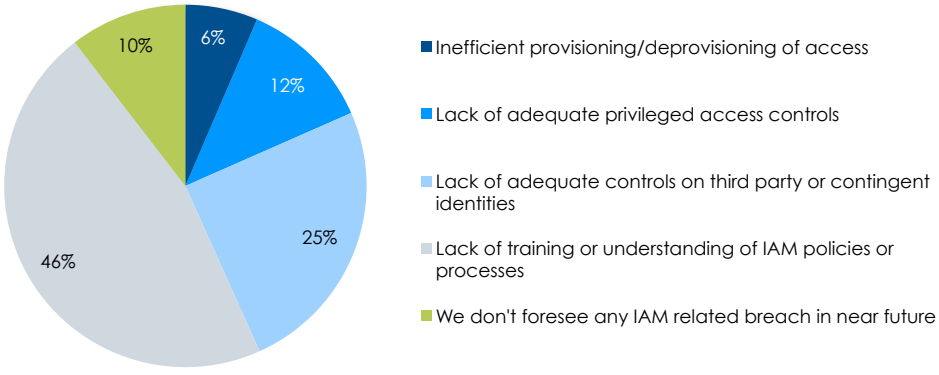

Fig. 2: Main cause of next IAM-related breach

Of the respondents, 46% said that they believed the lack of training or understanding of IAM policies or processes would be the main cause of the next IAM related breach.

Meanwhile, shadow IT is emerging as a serious threat to creating a secure IAM solution as companies digitally transform, with 43% saying it was challenging, and 22% very challenging.

Other highlights of the study:

- 92% of respondents will maintain or increase their IAM investment in the next three years
- 65% of respondents see consumer identities and applications as a factor in their next IAM investment
- 57% of respondents are considering adopting a solution at least partly managed by a Managed Security Services Provider (MSSP) for their next IAM investment

92%

of organizations in Europe will maintain or increase their IAM investment in the next three years.

77%

of businesses in Europe are undergoing digital transformation

IAM AND THE DIGITAL AGE

Digital transformation is changing business models, technology strategies, and partnerships in order to make businesses ready for the opportunities and challenges of the digital economy.

According to our study, it's a process well underway across Europe with some 77% of respondents saying that their organization has already implemented an enterprise wide transformation strategy, or already changing some enterprise operations.

This is a significant number and is likely to increase in the next three years as more companies realize that to compete effectively in a digital market, they need to go digital themselves.

Even those sectors once thought resistant to digital change, like insurance or manufacturing, are accelerating their programs, according to our results.

This could mean embracing digital outside of the traditional boundaries of the business, getting closer to customers through social media or making use of omni-channel trading models, particularly in the retail sector.

It could also include integration of IoT technologies in certain sectors such as utilities, services or manufacturing and in general the use of connected things, from activity trackers to connected vehicles. In technology terms, digital may well see uptake in developments such as hybrid data centers, DevOps and agile computing.

In all cases however, digital transformation will put identity center stage of secure business operations, and IAM should assume greater importance to not just security and information chiefs, but other CxO decision makers.

One of the challenges of scaling IAM is convincing other business leaders of the increased risk that digital transformation creates.

There are two good reasons: the increased attack surface that connected devices provide and the increased levels of vulnerable customer and IP related data.

To reduce the risk, information leaders need to convince the board of the need to connect objects with security processes from the outset, and scale data protection to avoid breaches and subsequent brand damage and loss of investor confidence.

41%

in the banking sector have implemented an enterprise wide digital transformation strategy.

DIGITAL TRANSFORMATION BY SECTOR

To establish how IAM planning may be affected by digital transformation it's important to establish how far industry sectors are down the digital road. Some we might have expected to be pushing ahead with digital transformation are relative laggards; while others are pursuing a process of catch up.

At the same time, respondents observing changes in some enterprise operations doesn't necessarily mean that this change is underpinned by a comprehensive, enterprise-wide digital transformation strategy.

However, while our analysis factors this in, the underlying trend remains one of transformation gaining real traction.

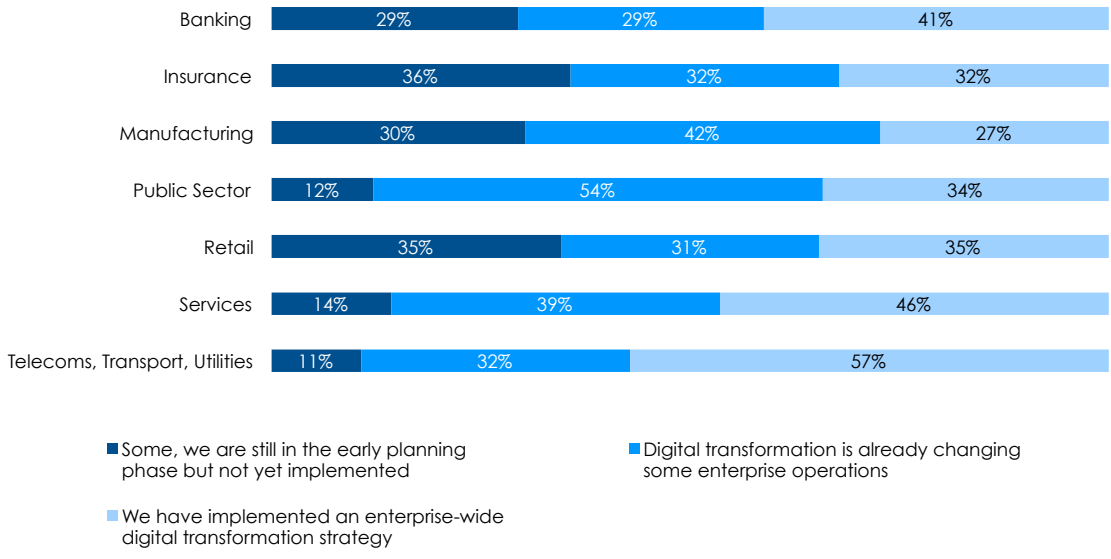

Fig. 3: Impact of digital transformation on the overall running of business (results by industry)

Across banking, 41% of respondents said their business had implemented an enterprise wide digital transformation strategy.

However in retail, quite often thought to be a sector ahead of the curve in digital, 35% had fully implemented digital across the enterprise and 31% said that digital was changing some operations.

Manufacturing was a relative laggard with 27% having implemented an enterprise wide digital transformation strategy.

A key vertical is the Public Sector, which formed the largest percentage of our overall sample, and is pushing ahead with transformation across Europe.

Of those sampled, 34% said they had implemented an enterprise-wide digital strategy, but perhaps more significant is the 54% who said that digital was already changing enterprise operations - higher than any other sector in the study.

This is significant in two ways. Across Europe, the public sector is under pressure to reduce costs and make governments and local governments more customer-focused. Which translates as making services digital.

In the UK, the government speaks of creating a Digital Platform for government, while in Germany the Federal Government is pursuing a national transformation policy outlined in a 2014 white paper, *The Digital Agenda*. Within this is its commitment to transforming public services under the banner "Digital Administration 2020".

Both these countries, and others across Europe, see digital skills and high-speed broadband access as crucial to future economic growth and an integral part of this is to make government digital ready. The

Across Europe, the public sector is under pressure to reduce costs and make governments and local governments more customer-focused.

EU has a commissioner for digital transformation and runs a variety of programs to drive the digital transformation of both governmental organizations and businesses.

Part of this process will be to create digital identities for citizens that will allow seamless access across different departments and government websites.

And obviously crucial to this is making access and identity highly secure. This goes beyond the IAM requirements of a single enterprise into a system secure enough to serve whole populations.

Perhaps it's no surprise that both the public sector and the services sector (where 46% have implemented an enterprise wide digital strategy) are ahead of the game as both offer soft products that lend themselves easily to the digital agenda.

The telecoms sector had the highest percentage of respondents, 64%, who have implemented an enterprise wide transformation strategy.

Manufacturing and retail both have some way to go. A significant portion of insurance companies and banks claim not having a strategy yet, even while FinTech upstarts threaten to fundamentally disrupt these businesses, particularly in the UK, France and Germany.

Again, this is a highly competitive market that depends on close customer relationships and added value services to stay competitive.

Digital is evolving at variable rates country by country, but as yet no nation shooting ahead of the pack.

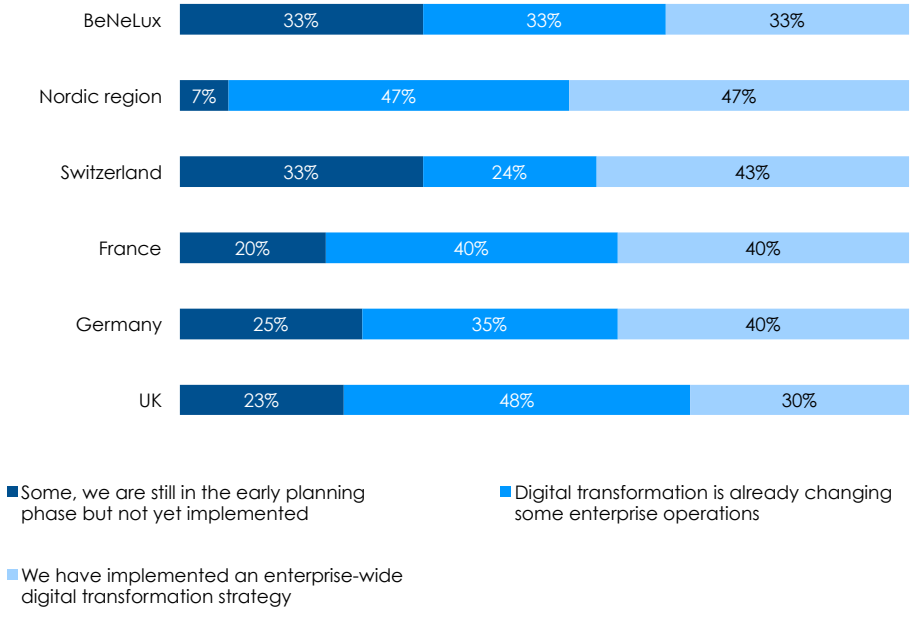

Fig. 4: Impact of digital transformation1 on the overall running of business (results by region)

SECURING THE DIGITAL BUSINESS WITH IAM

When we asked respondents what were the important goals of their organization's digital transformation we got some surprising, and some not so surprising results.

However it's significant that 48% of respondents thought threat or breach mitigation was a very important prerequisite for digital transformation.

Significant because if they are influential enough in their organizations there is a greater chance that transformation will be secured from the outset.

While it was expected that security would be well understood as a major challenge by our sample, they are not working in security bunkers either, blinkered to the needs of the business. Beyond security, the strategic goals of business transformation also figure highly in the responses.

These include improving customer experience, driving operational efficiency and increased revenue potential.

48%

of senior IT leaders in Europe think threat or breach mitigation is a very important component of digital transformation.

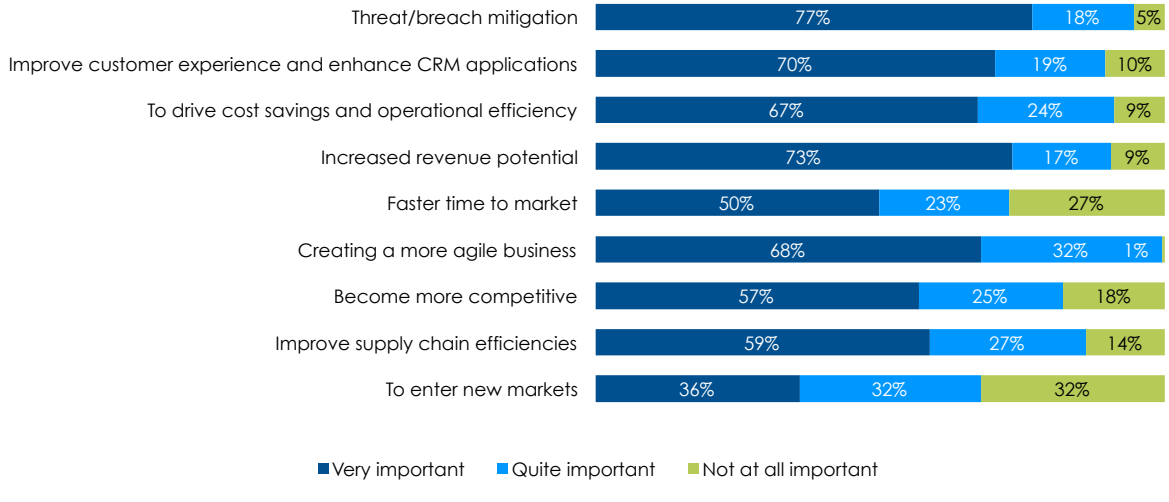

Fig. 5: Importance of individual goals of digital transformation strategies

Virtually all organizations have understood that they must become more agile – their digital transformation strategies always involve increasing business agility.

Interestingly, the lowest values of "very important" are for "to enter new markets", even while digital transformation will open doors to new routes to market for established organizations – Apple Pay is one example.

THE IMPACT OF THE EU GENERAL DATA PROTECTION REGULATION

Identity and access management is fundamentally designed to help prevent security breaches at organizations. Preventing breaches is also now a fundamental business goal.

Apart from operational and reputational damage and loss of trust, the regulatory cost of a breach within the EU will also soon increase significantly.

The new EU General Data Protection Regulation (GDPR) will make life harder for those companies that lose data, form cyber attack or otherwise. From April 2018 businesses that compromise any data they hold on EU citizens could be subject to fines of up to 4% of turnover or 20m Euro whichever is higher, and any breach must be reported within 72 hours.

The GDPR has been in the planning stages for so long that many business people, not to mention information and security professionals may have let it slip from their radar. But it is now a reality and it should be factored into risk management strategies from now on. And that will include decisions on future identity and access management solutions to cope with increased risk of a breach from digital transformation.

€20m or 4%

of annual turnover. That's how much businesses may have to pay in fines if they fail to comply with GDPR.

THREAT VECTORS FOR IAM

Digital will increase threats across a number of vectors including mobile, cloud and shadow IT.

MOBILE COMPUTING

Mobile computing will impact on the security of identities as businesses transform, and its growth is across all sectors.

Banking, a conservative sector and one that understandably is shy of shifting infrastructure beyond traditional perimeters, is still playing catch up in mobile usage. Aside of services (which is a mixed industry) it will remain the industry with the highest rate of its workforce not using mobile devices (based on the values for 10-24% and 25-49%).

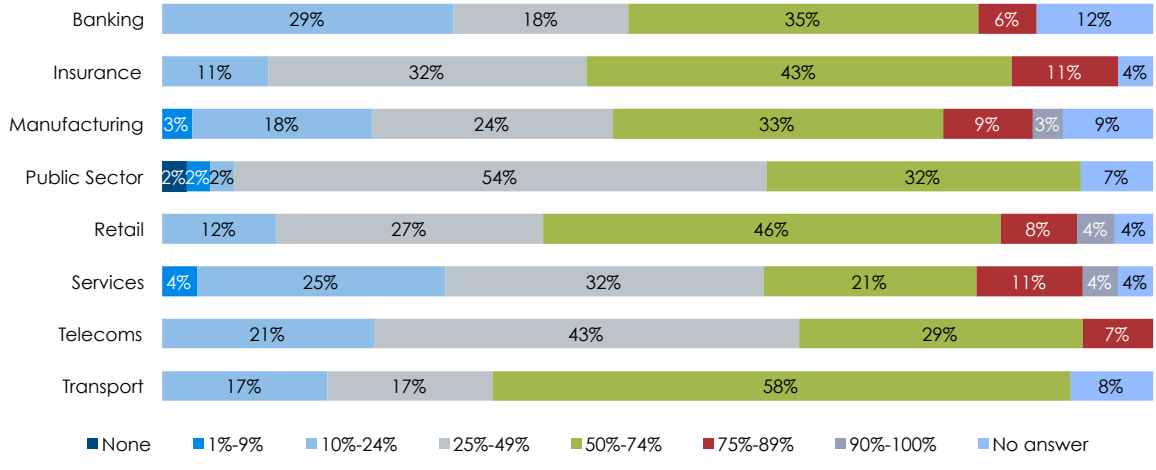

Fig. 6: Percentage of workforce currently using mobile devices for corporate services access

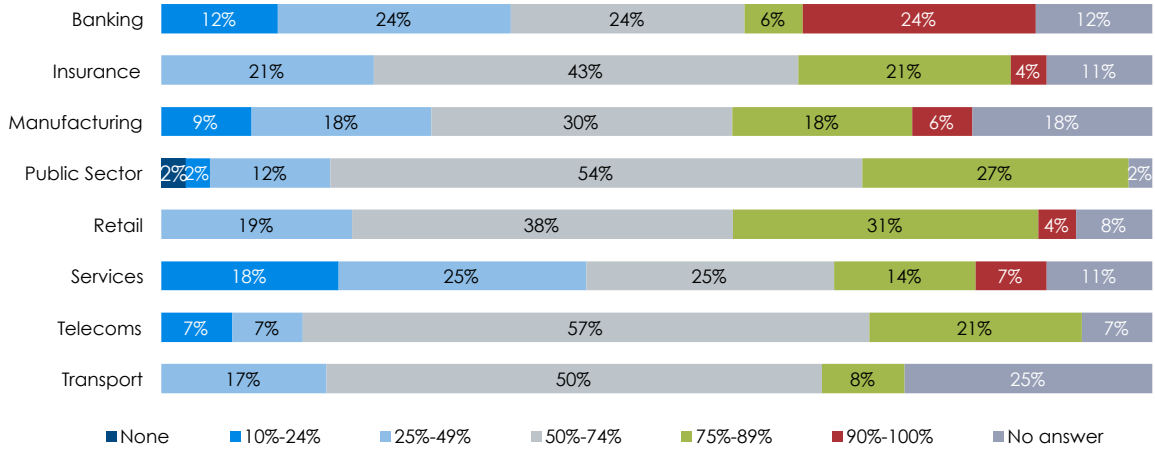

Fig. 7: Percentage of workforce expected to be using mobile devices for corporate services access in 3 years time

This is particularly based on the traditional workplaces e.g. in branch offices, but also partially in back offices, where people only work from their desk in the office.

On the other hand, the increase in the 90-100% range is significant, which indicates that some banks are fundamentally transforming their business towards a mobile business (perhaps to fend off challengers), away from traditional banking workplace practices.

Telecoms are predictably going mobile. This increases the complexity of security analytics, due to the fact that systems must also understand the relationship between users, devices, and things in use, plus the context of access. Advanced security analytics will be essential for handling the ever-growing complexity.

Overall the growth in mobile numbers is in-line with our expectations across all sectors, and, if anything, we believe they could be higher.

Security operations will need to be capable of dealing with cloud and on-premise systems.

THE CLOUD

The shift to the cloud is in line with general expectations with all sectors expecting an increase in corporate systems sitting in the cloud in three years time.

Interesting highlights here include formerly cloud-averse sectors such as banking, insurance and public sector all moving to the cloud according to expectations.

This will be driven by costs considerations, particularly in the public sector. There will remain security concerns however, especially if access to corporate systems is allowed to non-traditional parties (consumers, supply chain) through transformation programs.

All organizations are moving more of their workloads to the Cloud. Security operations will need to be capable of dealing with both cloud (public, private and hybrid) and on-premise systems.

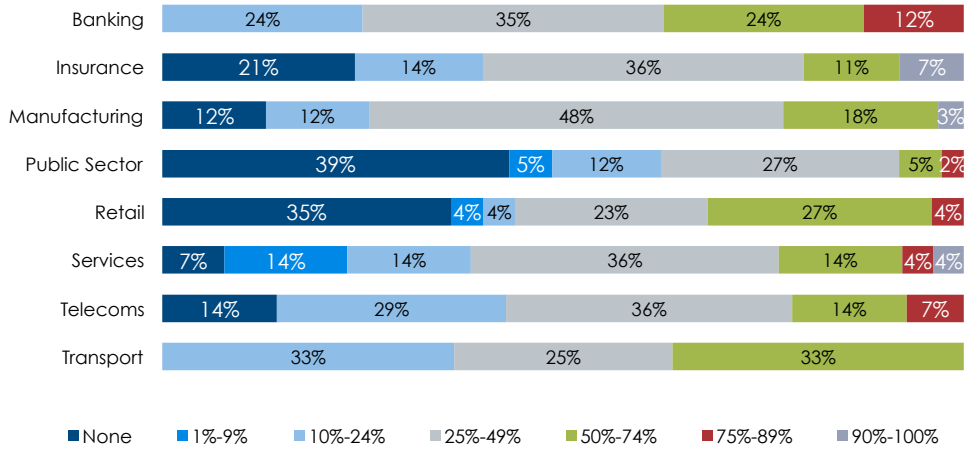

Fig. 8: Percentage of corporate systems expected to be sitting in the cloud in 3 years time

SHADOW IT

And in the digital age, one area where people are already "failing" is in the deployment of Shadow IT, which remains a controversial topic in IT circles.

It is in a way an expression by employees within enterprises to digitally transform almost organically, and without an enterprise led strategy in place.

The ease of access and low cost of web-based apps, cloud resources, mobile devices and virtual tools has seen a growth in procurement outside the IT department.

Applications such as AWS, Dropbox, Box and Salesforce are being used on the fly, yet at the same time used quite productively with good intent by employees to get projects done. This will continue and accelerate.

Employees are also used to installing messaging and social apps on personal devices, getting to like their ease of use and adapt them for business use, often across devices that have also not been authorized or sandboxed.

65%

of senior information security decision makers in Europe see Shadow IT as a challenge to creating a secure IAM solution.

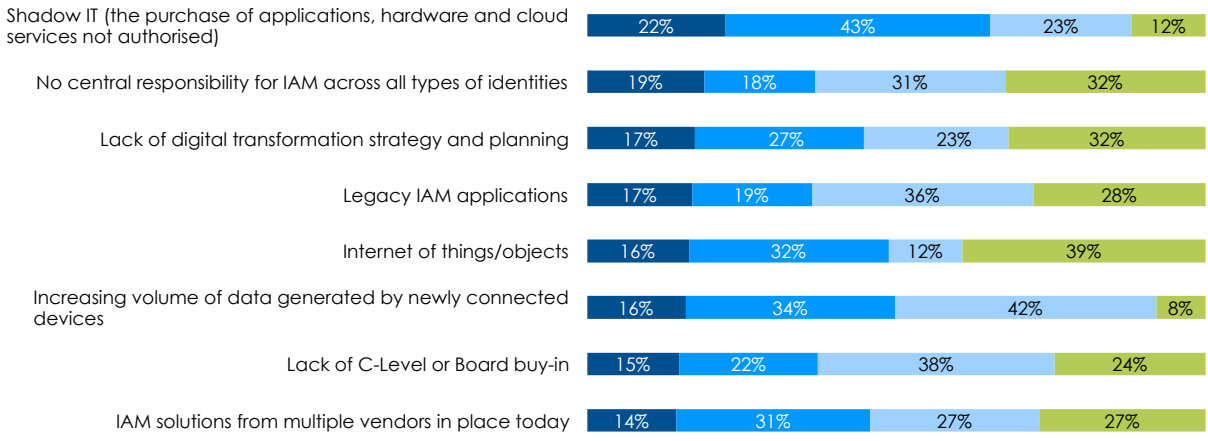

Fig. 9: How challenging are the following barriers to creating a secure IAM solution ready to support your organization in its digital transformation within the next 2-3 years?

The problem for the CIO, CISO and IT Security departments is that these open up new vulnerabilities and access points that are potentially insecure, even if the business benefits are clear.

It's obviously on the minds of our respondents with 22% seeing this as very challenging, and 43% as challenging to creating a secure IAM solution.

The challenge is clearly for IAM suppliers and IAM focused MSSPs to fully factor Shadow IT into their solutions. This is a growing and important issue for users and sellers alike.

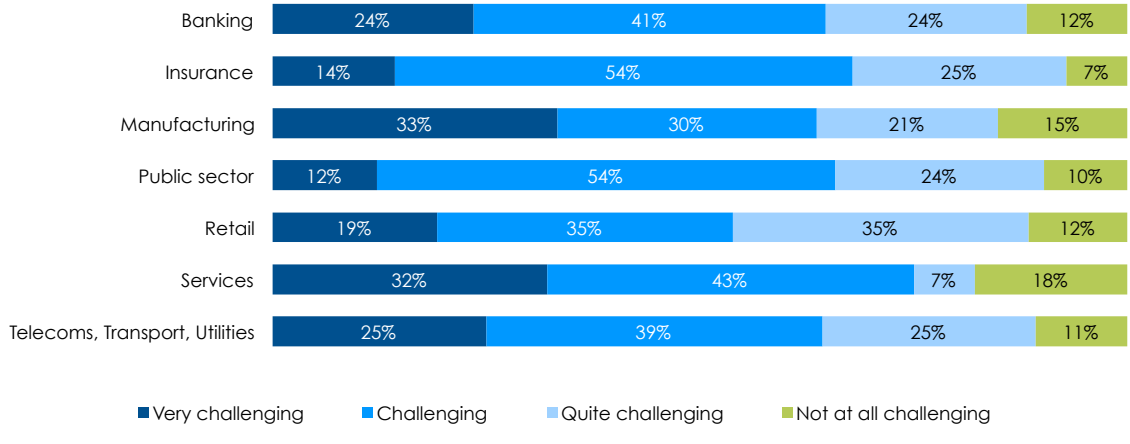

Fig. 10: How challenging is Shadow IT in creating a secure IAM solution for digital transformation within the next 2-3 years?

The cloud is impacting too. Organizations need adequate resources to manage the shift to the cloud, including well thought-out cloud risk assessments that are enforced by procurement and not only IT.

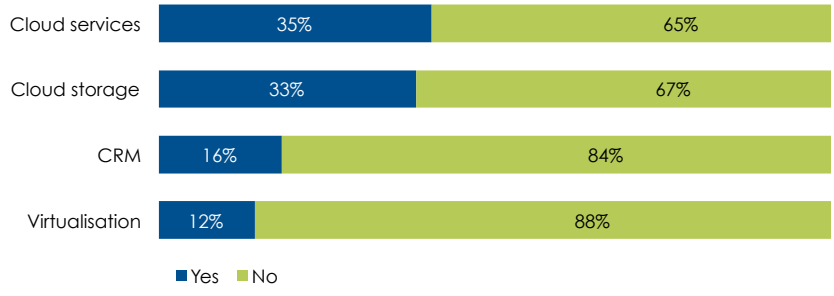

Fig. 11: Are your employees using any of the following applications without consulting the IT department?

Thirty five per cent of respondents said employees were accessing cloud service without authorization, while 33% were using cloud storage, 16% CRM tools and 12% virtualization.

Here, this is a case of a low number not always being a good number. Even a fraction of employees accessing or using resources that are unauthorized is a security risk. The significant unauthorized use of cloud storage means that a considerable level of sensitive information is stored out of the IT Department's control.

As companies go through what will inevitably be a complex and unpredictable process of transformation, such usage of shadow IT is likely to be even more of a risk.

Shadow IT is also listed as the second biggest threat to successfully implementing Privileged Account Management (PAM), with 26% of all respondents expressing concern about this. As the number of unauthorized apps or clouds increase, it's becoming harder to determine what are genuine privileged accounts and which are unsupported or regulated, and which of those belong to genuine employees.

Elsewhere, there is clearly a desire and an opportunity for cleaning up legacy IAM solutions from multiple vendors.

Some 31% saw this as a barrier to a secure IAM solution going forward. Given the security concerns and pressures that Shadow IT and cloud is already bringing the added vulnerability that stitched together legacy IAM systems must be a concern.

There is a desire and an opportunity for cleaning up legacy IAM solutions from multiple vendors.

RISKS AND REWARDS OF IAM

We live in an age where cyber attacks are constant and no company or organization is immune from breach. And even the best IAM solutions can be breached if rules are broken, or if operational changes take place that are not sanctioned by IT. Increasingly security at European businesses is threatened by the growth in shadow IT.

We wanted to know what our sample thought the main causes of the next IAM related breach could be. For those in the enterprise who do not believe in the power of security awareness training the results may serve as a wake up call.

For 46% of all respondents across all sectors believed that lack of training or understanding of IAM policies or processes could lead to an IAM related breach. This is a situation that could potentially get worse as the complexities of digital transformation take hold.

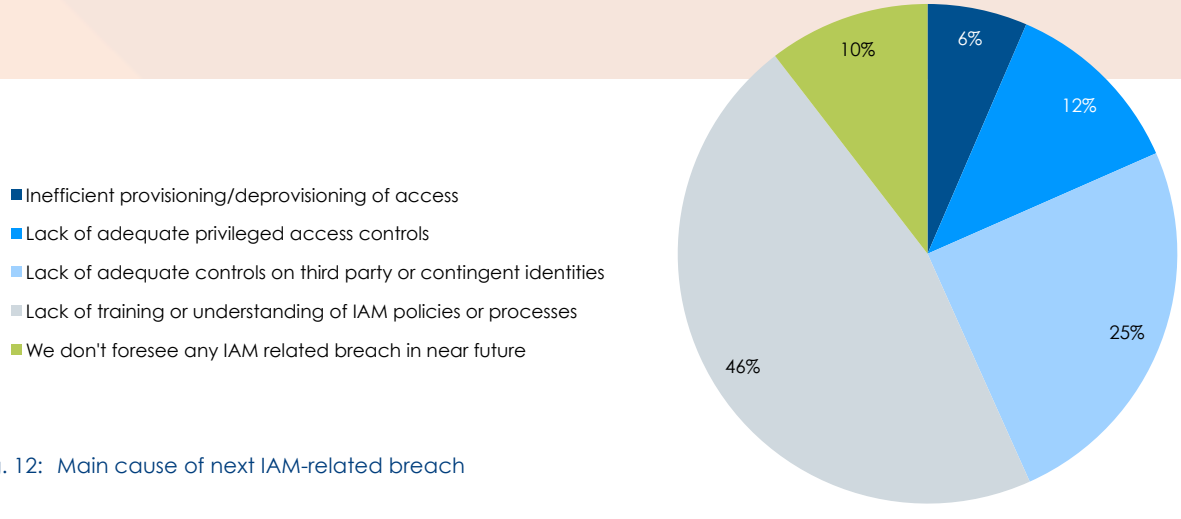

Fig. 12: Main cause of next IAM-related breach

Are our respondents pointing the finger at their enterprise colleagues or flagging the risk of insider threats before it is too late, especially in relation to the increase in the number of identities?

On a sector basis, services, telecoms and transport are most worried about the lack of training and understanding of IAM.

Paradoxically, across all sectors there is a surprising level of confidence that there won't be any IAM related breaches in the near future, with 10% expressing this view. In our opinion this represents an unusually high degree of optimism.

Aside of all technical controls, workforce education & training for information security is a mandatory element.

46%

of senior IT decision maker across all sectors believe that a lack of training or understanding of IAM policies or processes could lead to an IAM related breach

Technology might be perfect, but if people fail, things go wrong – starting with granting excessive access to resources.

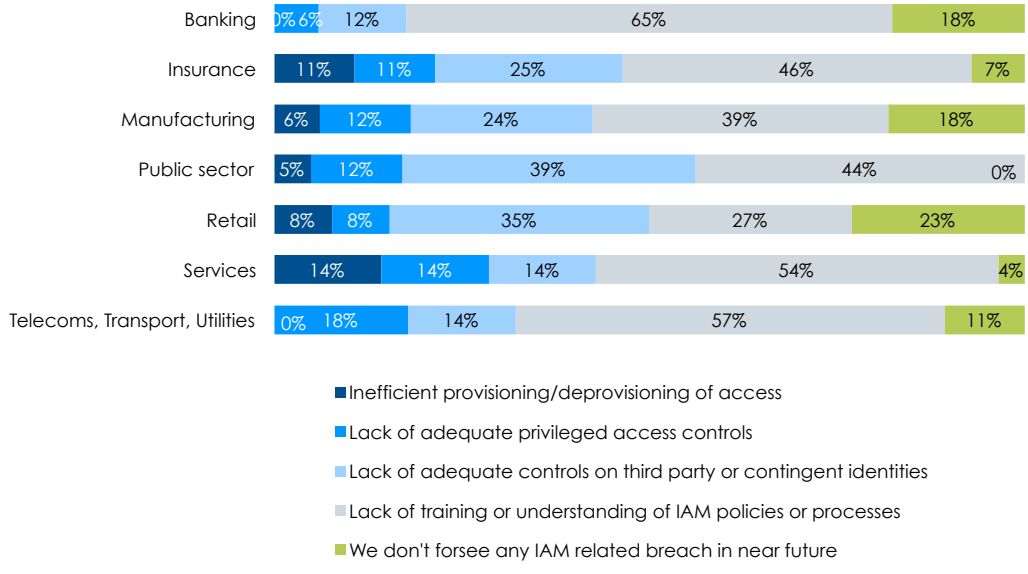

Fig. 13: What do you think will be the MAIN cause of the next IAM related breach in your organization?

DIGITAL GOALS FOR IAM BECOMING APPARENT

Going beyond security, our respondents demonstrated clarity of purpose to what they saw as the goals for their existing IAM solutions.

Awareness of digital was there with 21% seeing "scalability for managing consumers in our digital transformation" as very important and 45% important.

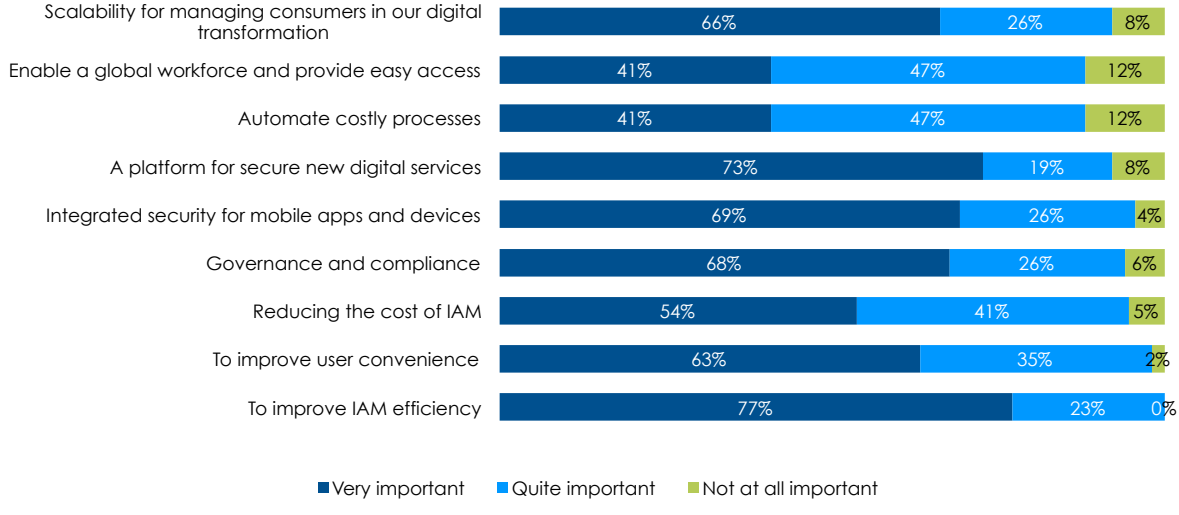

Fig. 14: Thinking beyond enterprise security, how important are the following roles of your current Identity and Access Management applications?

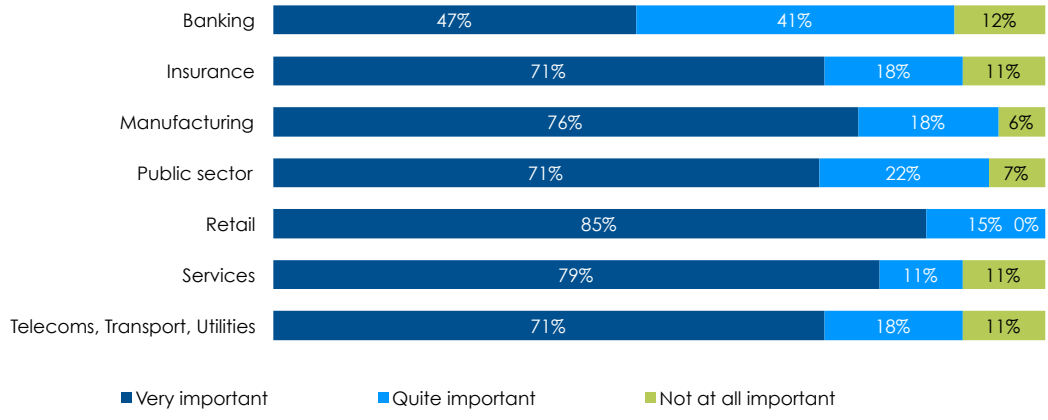

Fig. 15: How important is it for IAM to be a platform for secure new digital services?

Even better, 24% saw making it a platform for secure new digital services as very important, and 47% as important.

This was across all sectors and countries and shows that digital is on the minds of our decision makers.

Boosting efficiency is still however the prime goal with 40% ranking this as very important.

At the same time, risk mitigation remains an important factor in any IAM solution. A significant number across all sectors saw integration and interoperability with Enterprise Risk Management (ERM) as an integral part of any IAM investment.

When prompted as to whether digital transformation would impact ERM, 35% fully agreed and 46% agreed that IAM should address this.

41%

of European organisations will increase investment in IAM in 2016

IAM INVESTMENT PATTERNS

Market analysis by PAC predicts continued growth in the IAM market by volume, between 2016 and 2019. For a representative outlook, Fig. 16 shows the projected figures for the UK market.

Such growth highlights the importance of IAM to an already challenging security landscape.

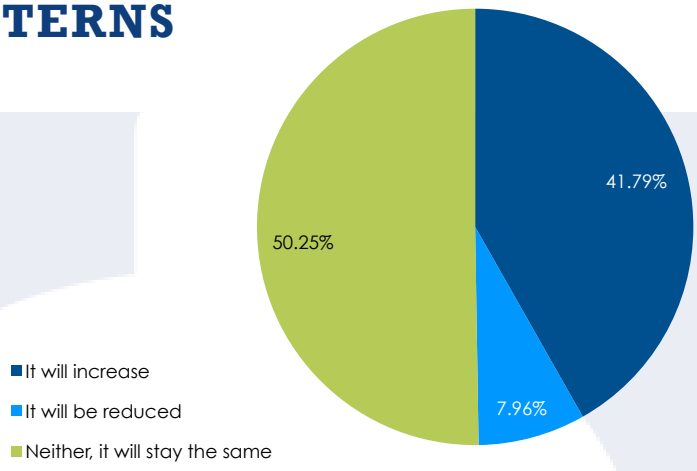

Fig. 16: Do you expect your investment budget for IAM to increase or decrease in 2016?

The results of this study reinforce the need for robust IAM solutions to cope with the added challenges of digital transformation.

The answers to IAM investment intentions proved interesting, with consumer identities coming into play.

Most IAM experts believe that any robust IAM system that is designed to cope with digital transformation must be able to handle consumer identities.

And the opinion of our security and information chiefs across Europe would seem to bear this out.

While endpoint security is included by 73% of respondents as a key factor in IAM investment planning, a close second at 65% is consumer identity applications and consumer identity.

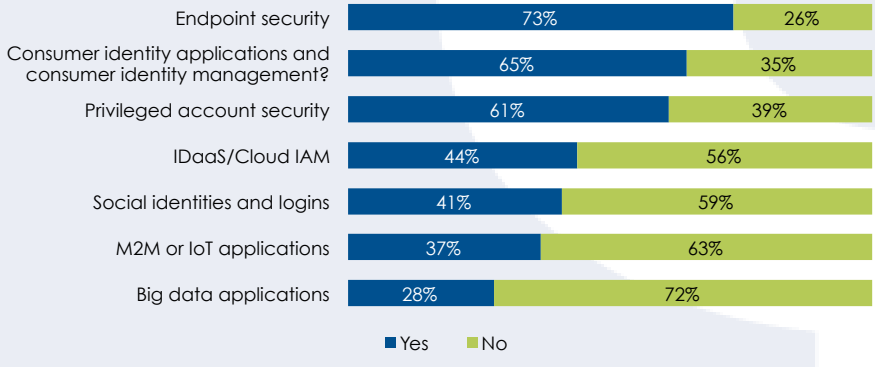

Fig. 17: Does your IAM investment planning include any of the following factors? (all sectors)

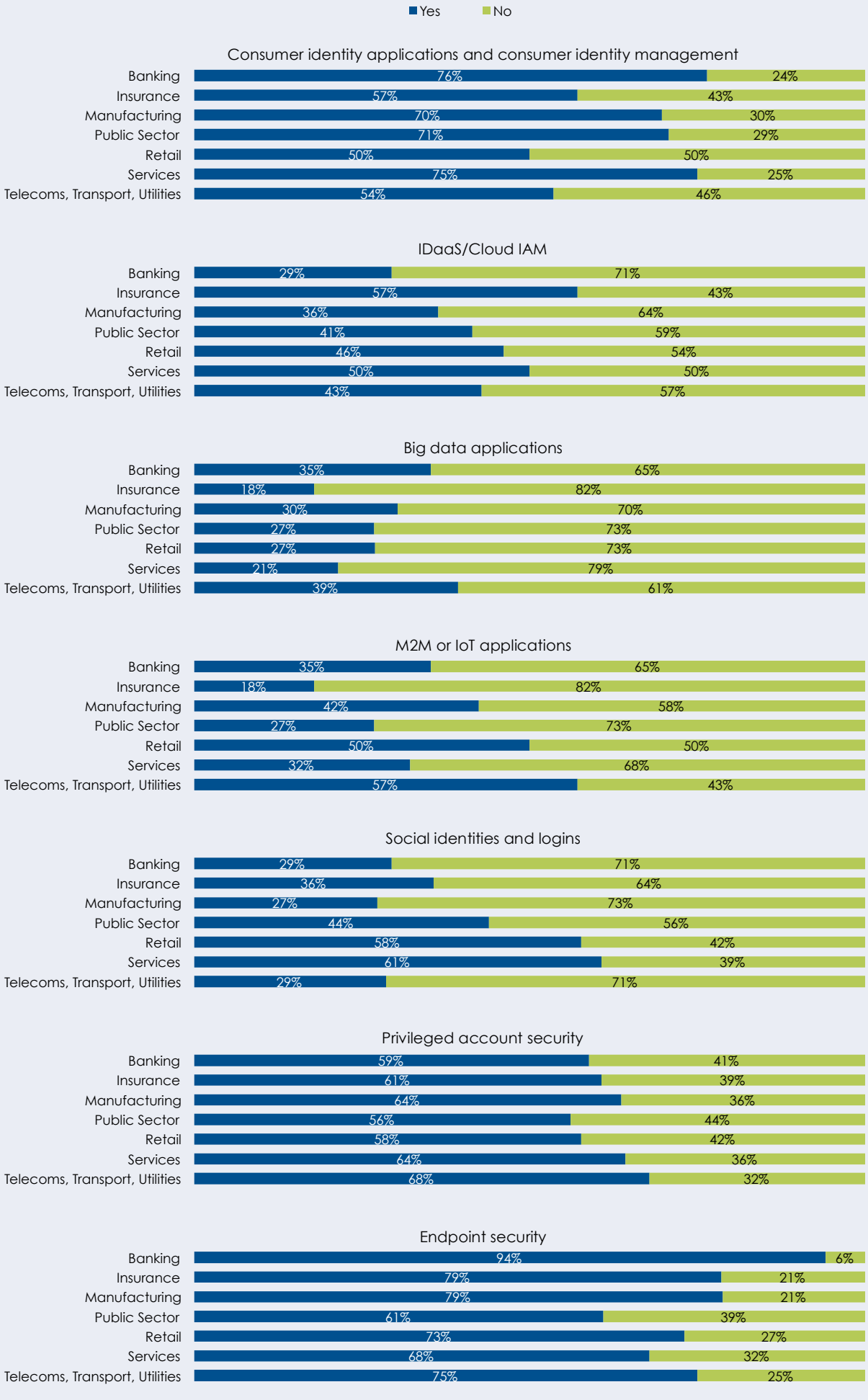

Fig. 18: Does your IAM investment planning include any of the following factors?

Even more intriguing is social identity and social logins which has been ticked by 41% of our sample. Clearly our representative sample is thinking very much outside what could be described as the conventional security box in formulating future IAM investment plans.

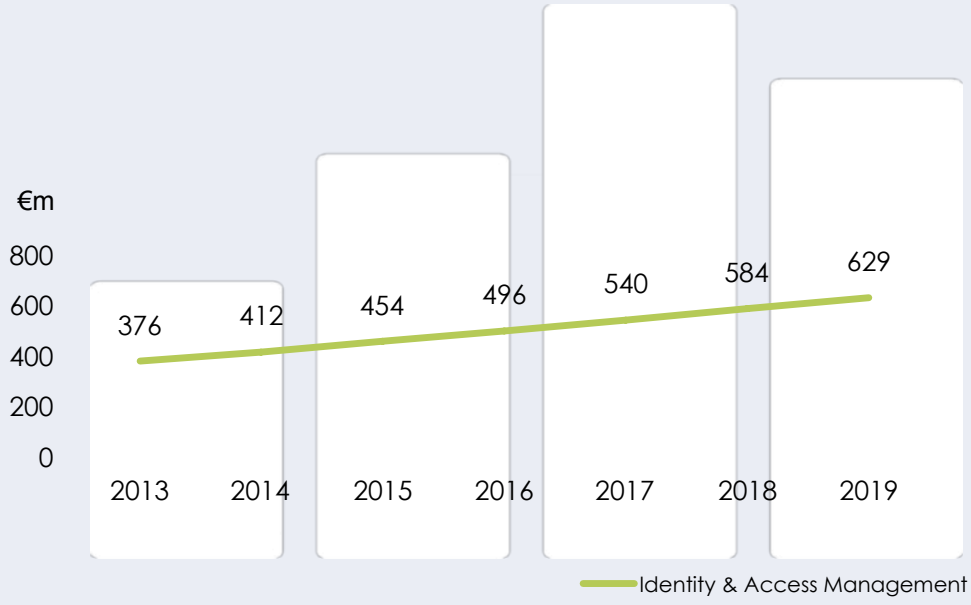

Fig. 19: Security market volumes in the UK

Even if their businesses are not yet at a stage of a fully realized digital transformation or even at the beginning, they are thinking of the importance of factoring in identities well beyond those of the traditional area of employees and privileged accounts.

Overall, there was a healthy and pleasing response for all the digital triggers in the survey including M2M and IoT, which suggest a high level of digital awareness in our sample.

It's when we look at how security planners intend to manage these new digital challenges for future IAM solutions that we get an interesting picture.

In other areas of cyber security, managed security services providers (MSSPs) have long been trusted to take care of day to day running of applications such as web or email filtering.

Yet trust in MSSPs is not yet fully forthcoming for IAM solutions if our respondents across all sectors and countries are to be believed.

Just 15% of respondents plan to outsource IAM fully to an MSSP, while 57% would partly outsource it – something that MSSPs need to take heed of. What can they do to convince our sample that IAM is safe in the hands of an MSSP?

A cloud based identity as a service (IDaaS) solution is seen as less of risk with 28% willing to outsource that, and 58% to partly outsource some of the identity function.

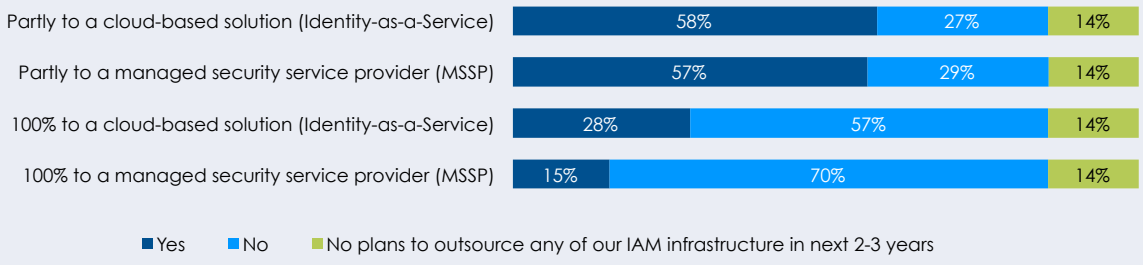

Fig. 20: Do you plan to outsource any of your IAM infrastructure in the next 2-3 years?

It should be pointed out that by relying on an MSSP, the client allows it to take more control - which is a bigger risk, whereas IDaaS is more about a platform under control of the outsourcer.

Furthermore, the lower numbers are most likely due to the fact that it is hard to manage everything from the cloud or an MSSP – think of IAM for legacy apps for example.

Most organizations plan running some or part of their IAM in the cloud, however most will leave some IAM on-premises, which is most likely due to the need of supporting existing on-premise applications. The existence of multi-vendor legacy IAM solutions may be a factor here.

Furthermore, IDaaS is best suited for managing access to cloud applications and managing access for new groups of users such as customers, while established on-premise IAM is optimized for the more complex requirements.

Cost reduction is less a target than in former days. Organizations are increasingly looking at business enablement, by supporting mobile workforces (69% rate this very important/important), enabling new digital services (72%), and managing consumer identity access (66%).

15%

of European businesses plan to outsource IAM fully to an MSSP.

CONCLUSION

Our study has revealed an encouraging awareness of the need for digital transformation of their business by our representative sample of senior information and security executives across Europe.

We are seeing too that those verticals seemingly resistant to digital transformation, such as insurance, are starting to shift as market conditions change and challengers emerge. This will mean that security across all sectors will at some point need to adapt to digital transformation, and probably earlier than later.

But instead of remaining in their security silos, simply looking to lock everything down as before, our study shows that our information executives are aware of the business benefits that digital transformation presents, and that if their organizations are to compete they need to embrace that change.

This does not mean that they are not concerned about security in the digital age. They certainly are. And they are acutely aware that Identity and Access Management solutions will need to step up to the plate if new identities from consumers, and even those of things and sensors, are to be securely managed.

Most breaches today are the result of banal mistakes by employees clicking on rogue links in emails, downloading malicious attachments, or simply not following security policies and training lessons.

People won't change in the digital age but the consequences and risks of these happening are even greater as the threat vector broadens across multiplying identities and objects. In the digital age, the insider threat will need to be managed ever more securely.

As new levels of access are likely to form part of digital transformation, the need for a secure and enhanced IAM solution must be factored in from the start.

Can our CIOs and CISOs manage this and how far will IAM vendors and MSSPs offering IDaaS respond?

There is a new trend already well underway across Europe, and one that threatens to undermine even the most stringent information officer and best in class IAM installations: the growth of Shadow IT.

Digitally led services and software are now easily, and cheaply, available to lines of businesses outside the remit of the IT department. Our study demonstrates that there is great concern about how Shadow IT will impact on the efficacy of legacy IAM, and how it must be factored into future investments.

Again, how this can be achieved is a challenge for both users and suppliers. A conversation between the two sides would be a good

start, as well as a realistic audit of Shadow IT by the organizations concerned.

In a business world increasingly under scrutiny from regulators, a public worried about data privacy, and shareholders concerned about the damage breaches can do to a business, risk and compliance must also be factored into IAM decisions in the digital age.

There is a concern that in the rush to digitally transform, other lines of the business will overlook or neglect security investment. There will be an extra pressure for IT and security chiefs to ensure that this doesn't happen when choosing new IAM solutions for multiple identities and devices.

Investment is forthcoming but IT and Security chiefs need to make the clarion call that investment needs to be focused, that new solutions and IAM policies are needed to cope. In short, IAM for the digital age.

Identity and access management will move center stage as the main defense against cyber attacks in the digital age, even as businesses move to more intelligence based approach to cyber security and threat management of other vulnerabilities.

But if European business chiefs fail to control the identity of people and objects accessing data and infrastructure, they will be failing their business and its future security and growth.

APPENDIX

RESEARCH METHODOLOGY

PAC conducted the survey during March 2016. After qualifying, 202 senior information security leaders from across Europe completed our survey. The executives are employed in banking, insurance, manufacturing, retail, services, telecoms, transport and the public sector and are based in the Benelux and Nordic regions, Switzerland, France, Germany and the UK.

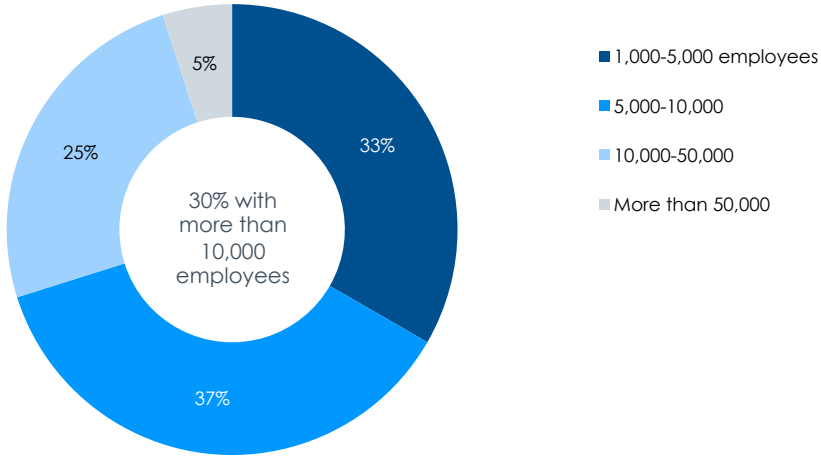

Fig. 21: How many employees work at your company?

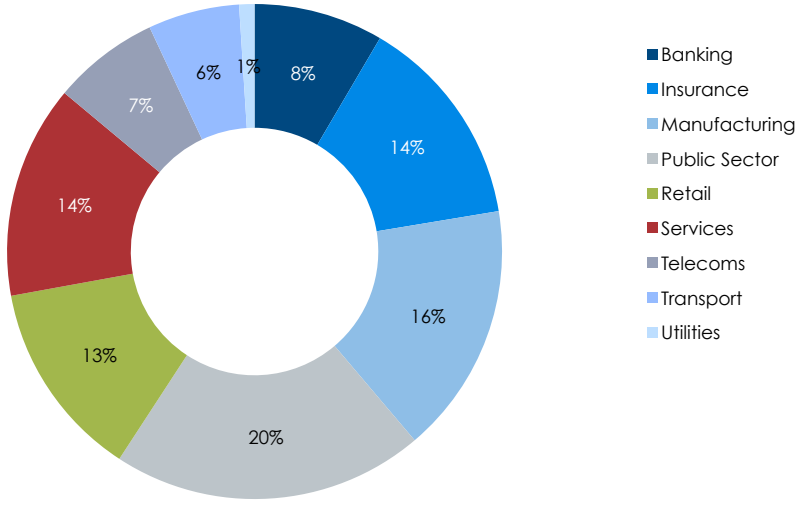

Fig. 22: What is the main activity of your company?

TABLE OF FIGURES

ABOUT KPMG

Today, cyber attacks have become a business reality. Technological advances and changing working practices have created additional opportunities for cyber criminals and hacktivists. Organizations are in a position where they're 'losing control.'

Passwords are being shared; there are silo solutions per application or platform which give rise to countless authentication methods and password regimens; authorizations are multi-layered and duties are no longer clearly segregated; there is a lack of insight into the authorizations granted by the management; the helpdesk costs to change passwords, demonstrate compliance with access governance, protect high-privileged accounts, provide rapid provisioning and de-provisioning and authorizations are high.

The list of weak points are endless.

To address these issues many organizations have projects underway to improve user management, access governance, privileged access management, federation services, Role Based Access Control and provisioning: the ingredients of Identity and Access Management (IAM).

KPMG's Global Cyber Security practice offers many years of experience and extensive expertise in all aspects of IAM:

- An in-depth **understanding** of current and future IAM trends impacting business across multiple sectors
- **Expert knowledge** on compliance laws, business, privacy and regulatory risks
- **Strengths in IAM strategy assessments, program advisory, project management and implementation** across a broad range of IAM tools.
- **Extensive capabilities** in security assessment and certification; security architecture development and implementation; security and technology governance; IT infrastructure and controls; and operations and project risk management

About the KPMG Global Cyber Security Practice

KPMG's 2,200+ network of cyber security professionals' work with companies around the globe to help them safeguard their entire organization. By addressing people, privacy, information governance and business resilience, we help our clients to implement a firm-wide approach to doing business in the digital world. We give leadership a new perspective to help them to take control of cyber risk in a unique and positive way, and empower them to grow, transform and innovate their business.

For more information visit the KPMG Cyber Security website.

Contact:

John Hermans
Cyber Security Lead,
Europe Middle East & Asia
KPMG in The Netherlands

hermans.john@kpmg.nl

Prasad Jayaraman
Global Lead, Identity &
Access Management
KPMG in the US

prasadjayaraman@kpmg.com

Manoj Kumar
Principal Advisor,
Cyber Security
KPMG in the UK

manoj.kumar@kpmg.co.uk

www.kpmg.com

ABOUT CYBERARK

CyberArk is the only security company laser-focused on striking down targeted cyber threats, those that make their way inside to attack the heart of the enterprise. Dedicated to stopping attacks before they stop business, CyberArk is trusted by the world's leading companies — more than 40% of the Fortune 100 — to protect their highest-value information assets, infrastructure and applications.

For over a decade CyberArk has led the market in securing enterprises against cyber attacks that take cover behind insider privileges and attack critical enterprise assets. Today, only CyberArk is delivering a new category of targeted security solutions that help leaders stop reacting to cyber threats and get ahead of them, preventing attack escalation before irreparable business harm is done.

At a time when auditors and regulators are recognizing that privileged accounts are the fast track for cyber attacks and demanding stronger protection, CyberArk's security solutions master high-stakes compliance and audit requirements while arming businesses to protect what matters most.

With offices and authorized partners worldwide, CyberArk is a vital security partner to 2,500 global businesses, including:

- More than 40% of the Fortune 100
- 17 of the world's top 20 banks
- 20% of the Global 2000
- 8 of the world's top 16 pharmaceutical companies
- 75 of the leading energy companies

CyberArk has offices in the U.S., Israel, U.K., France, Germany, Netherlands and Singapore and serves customers in more than 65 countries.

Find us on Linked: www.linkedin.com/company/cyber-ark-software

Follow us on Twitter: @CyberArk

Contact:

Amanda Coles
EMEA Marketing Director

M: +44 (0) 7943 046139

amanda.coles@cyberark.com

www.cyberark.com

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.

What We Do

Today, SailPoint helps organizations around the world securely and effectively deliver and manage user access from any device to data and applications in the datacenter, on mobile devices, and in the cloud. SailPoint's products allow companies to mitigate the risks associated with access by delivering:

- **Identity Governance** – streamline compliance processes and improve audit performance through automated access certifications, policy management and audit reporting.
- **Provisioning** – deliver access to business users while reducing costs and tightening security with self-service access request and automated provisioning.
- **Password Management** – strengthen password policies and reduce IT and helpdesk costs with intuitive self-service password management.
- **Access Management** – increase end user productivity with convenient single sign-on (SSO) to cloud and web applications—from any device, anywhere in the world.
- **Identity Intelligence** – get the big picture with centralized visibility to access privileges across the organization and the right information to enable effective business decisions.

Contact:

Reuben Braham
Director of Marketing
EMEA & APAC

reuben.braham@sailpoint.com

Jon Burghart
VP EMEA, SailPoint

jon.burghart@sailpoint.com

Peter Wilson
UK Channel &
Alliance Manager

peter.wilson@sailpoint.com

ABOUT PAC

Founded in 1976, Pierre Audoin Consultants (PAC) is part of CXP Group, the leading independent European research and consulting firm for the software, IT services and digital transformation industry.

CXP Group offers its customers comprehensive support services for the evaluation, selection and optimization of their software solutions and for the evaluation and selection of IT services providers, and accompanies them in optimizing their sourcing and investment strategies. As such, CXP Group supports ICT decision makers in their digital transformation journey.

Further, CXP Group assists software and IT services providers in optimizing their strategies and go-to-market approaches with quantitative and qualitative analyses as well as consulting services. Public organizations and institutions equally base the development of their IT policies on our reports.

Capitalizing on 40 years of experience, based in 8 countries (with 17 offices worldwide) and with 140 employees, CXP Group provides its expertise every year to more than 1,500 ICT decision makers and the operational divisions of large enterprises as well as mid-market companies and their providers. CXP Group consists of three branches: Le CXP, BARC (Business Application Research Center) and Pierre Audoin Consultants (PAC).

For more information please visit: www.pac-online.com

PAC's latest news: www.pac-online.com/blog

Follow us on Twitter: @PAC_Consultants

Contact:

Matthieu Page
Account Manager

CXP Group – Digital Business Services BU (PAC UK)

+44 (0)20 7553 3961

m.page@pac-online.com

ABOUT KUPPINGERCOLE

Europe's leading Analysts on the topics of Information Security in the era of Digital Transformation

KuppingerCole, founded in 2004, is an international and independent Analyst organization headquartered in Europe. The company specializes in offering neutral advise, expertise, thought leadership and practical relevance in Information Security, Identity & Access Management (IAM), Governance (IAG), Risk Management & Compliance (GRC) as well as all areas concerning the Digital Transformation. KuppingerCole supports companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges. Maintaining a balance between immediate implementation and long-term viability is at the heart of KuppingerCole's philosophy.

Research

As a core element of KuppingerCole's research the company provides different types of reports with thought leadership and a vendor-neutral view on the status of the markets, products, and vendors. KuppingerCole's qualified analysts continuously research and update the company's online research library, and perform manufacturer-independent advisory services.

Events

Further, KuppingerCole organizes conferences, workshops, and webcasts in all fields of identity focused on information security, IAM, Cloud, Digital Risk and Digital Transformation. KuppingerCole's yearly European Identity & Cloud Conference is Europe's leading event for thought leadership and best practice in this area and covers the latest and future topics regarding the challenges in digital business.

Advisory

KuppingerCole is the best advisory partner in making your business successful in the era of Digital Transformation.

For more information about KuppingerCole and our services please feel free to contact us at any time.

Contact:

Petra Ehweiner
Product Manager
KuppingerCole

+49 (0)211 237077-19

pe@kuppingercole.com

DISCLAIMER, USAGE RIGHTS, INDEPENDENCE AND DATA PROTECTION

The creation and distribution of this study was supported by KPMG, CyberArk and SailPoint (among others).

For more information, please visit www.pac-online.com.

Disclaimer

The contents of this study were compiled with the greatest possible care. However, no liability for their accuracy can be assumed. Analyses and evaluations reflect the state of our knowledge in April 2016 and may change at any time. This applies in particular, but not exclusively, to statements made about the future. Names and designations that appear in this study may be registered trademarks.

Usage rights

Independence and data protection

This study was produced by Pierre Audoin Consultants (PAC) in cooperation with KuppingerCole. The sponsors had no influence over the analysis of the data and the production of the study.

The participants in the study were assured that the information they provided would be treated confidentially. No statement enables conclusions to be drawn about individual companies, and no individual survey data was passed to the sponsors or other third parties. All participants in the study were selected at random. There is no connection between the production of the study and any commercial relationship between the respondents and the sponsors of this study.

A CXP GROUP COMPANY