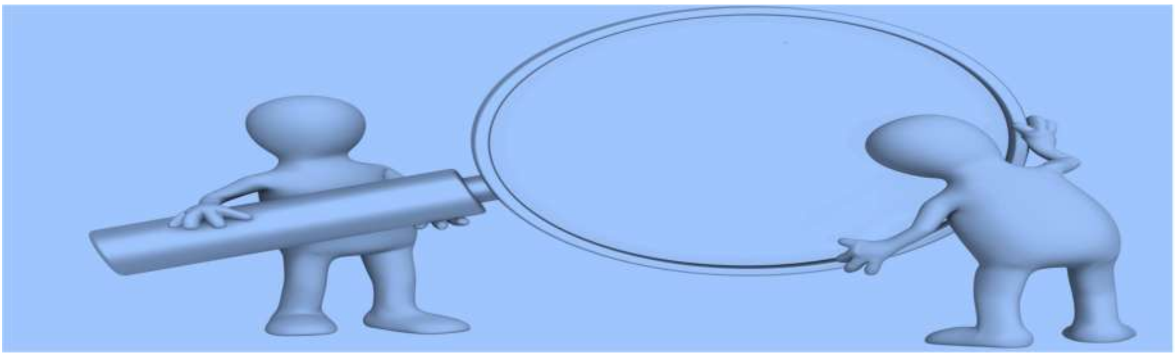


Getting to know you

Building online relationships with effective identity and access management

June 2015

The firewall-defined boundary that used to confine an organisation's IT assets and users has dissolved; identity has emerged as the new perimeter. This is not just a response to increased user mobility and the use of cloud-based services; it is also driven by a pervasive requirement to transact with external users.

To rise to the challenge most organisations are rethinking the way they manage identities. A primary requirement is to be able to federate identities from multiple sources, including the directories of customer and partner organisations, and, especially when it comes to consumers, social media.

The pressing need to effectively engage with outsiders has turned identity and access management (IAM) into a business priority, which means, when the case is well made, that funds are available. Organisations that are already reliant on transacting directly with consumers online are leading the way; the laggards may have no choice but to follow.

Bob Tarzey
Quocirca Ltd
Tel : +44 7900 275517
Email: Bob.Tarzey@Quocirca.com

Rob Bamforth
Quocirca Ltd
Tel: +44 7802 175796
Email: Rob.Bamforth@Quocirca.com

Executive Summary

Getting to know you

Building online relationships with effective identity and access management

All organisations now interact with external users and this has required a rethink of the way identities and access rights are managed. Identity is no longer just an IT security issue but a key business enabler, as all organisations work out how to effectively engage with customers and partners online. Those that transact the most with consumers are setting the direction; all will likely have to follow their example sooner or later.

Current IAM deployments are not fit for purpose

Most organisations have a range of identity and access management (IAM) capabilities in place. However, few consider their current tools to be entirely fit for purpose when it comes to managing external users.

All organisations have to deal with external users

Access to online resources has been opened up to broad constituencies of users including consumers, business customers, partners and contractors, as well as employees. Mobile access means users can be anywhere and applications are often running on remote cloud platforms. The days of the clearly defined, firewall-delimited, perimeter are over.

Legacy IAM systems need upgrading

Existing IAM deployments are often legacy systems, supplied along with an IT infrastructure stack that was not designed to manage external users. The identity elements are embedded and can be hard to replace, so they are being supplemented by new systems that are increasingly supplied as on-demand services (IAM-as-a-service/IAMaaS).

Sources of identity are many and varied

The extension of existing systems is often necessary to enable federated identity management; the integration of identities from multiple sources. This includes internal directories (primarily Microsoft Active Directory), partner directories, government databases and, especially amongst organisations that deal with consumers, social media.

Identities are a key business asset

Even though IAM systems are increasingly sourced from on-demand service providers and identities from other external sources, organisations want to be able to directly manage the relationships created and maintain a sense of ownership. Identities are seen as a key business asset and the primary data that is collected about new and prospective customers.

Trust in identity sources varies

Some sources of external identity are trusted more than others. Those organisations that transact with consumers extend their trust furthest; they see external identity sources, including social media, as an effective way to locate and engage with their targets. The consumer-facing majority are setting the on-going agenda for the future of IAM.

The case for investment in IAM is being made

The question will always be asked, "*we have already invested in IAM capability, so why not use that?*" However, the case for new investment is being made and accepted. Where the case is most pressing, the scrutiny is greatest; however, consumer-facing organisations see dedicated budgets for supporting online activities increase fastest.

Conclusions

Those responsible for delivering online resources in consumer-facing organisations have a convincing case for new IAM investment. Their dedicated budgets are more likely to increase compared to their non-consumer-facing counterparts. The laggards will have to catch up with the leaders at some point or lose sight of their organisation's perimeter altogether as transacting online becomes the norm.

Introduction – getting to know you

Some relationships are formed at breakneck speed; others mature more slowly. In business, whether the relationship is with another business or a consumer, love at first sight is unlikely; trust is built up over time as both parties find out more about each other. To achieve this there is an early need to be able to recognise an individual from one online visit to another, which requires capturing an electronic identity that can be recognised over and over again.

For the majority of organisations the need for identity and access management (IAM) tools is obvious, this is something they have had to do for years. Comprehensive IAM is more than just a directory of identities (nearly all organisations use Microsoft Active Directory, at least for internal users), it is the ability to proactively manage these identities; most obviously the tools to provision and de-provision users from IT resources. The majority of organisations have such basics in place (Figure 1)[1].

However, needs are getting more complex as identity management requirements extend beyond internal users to include employees from customers and partners, as well as consumers. How do you manage such diverse user groups and control their differing access rights whilst keeping relationships open and data safe? The answer is that many organisations are deploying additions to their base IAM platform such as federated identity management, reporting capabilities, and the ability to ensure governance and compliance objectives are met. This leads to a complex overall IAM toolset.

Another capability the majority now have in place is single sign on (SSO). At its most basic SSO is the ability to broker access between users and the resources, both of which can, these days, be anywhere. If that is true of the users and resources it can also be true of the IAM tools, especially SSO, and the procurement of on-demand IAM services, so-called IAM-as-a-service (IAMaaS), is becoming more widely accepted.

However, regardless of the high usage levels, many currently deployed IAM tools are not considered fit for purpose, especially when it comes to the challenge of managing external users (Figure 2). No single industry sector has cracked the problem, although transport organisations and retailers, which have high levels of external interaction, have come closest.

The aim of this report is to use new research to show why this is the case and what steps organisations need to take to improve matters. In short, what can the laggards learn from leaders?

Figure 1: Deployment of IAM capability – *overall*

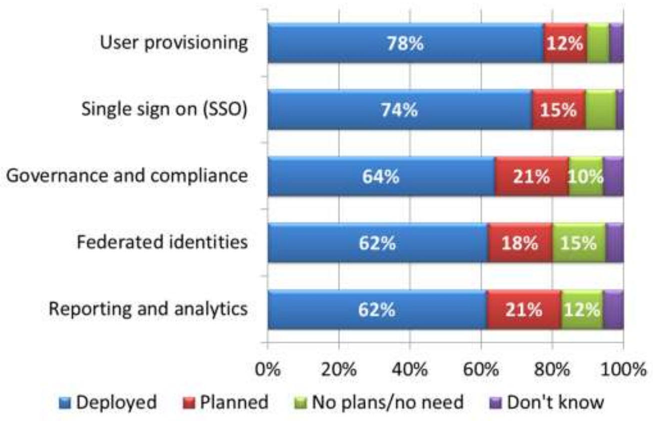
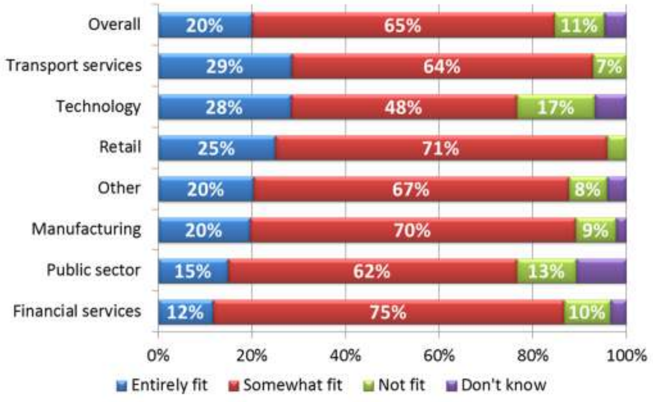


Figure 2: Fitness of purpose of IAM systems for managing external users



Establishing the identity perimeter

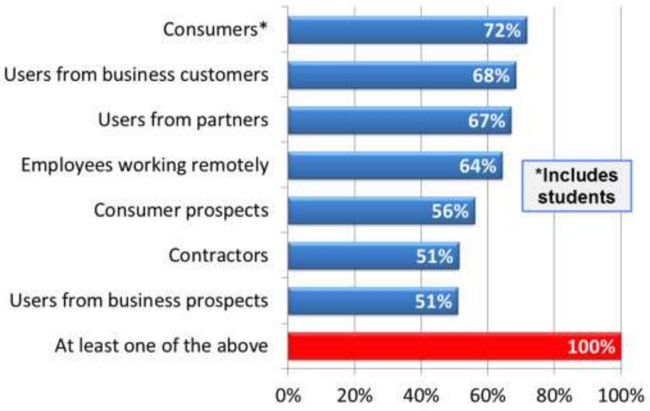
With the rise of mobile access and cloud computing, the firewall-defined traditional network edge has melted away. This theme was discussed in a previous Quocirca report *Identity is the new perimeter* [2].

It is not just the mobility of employees and the use of cloud applications that causes the redefinition of the corporate IT perimeter, but that need for external engagement. As the web passed its 25th anniversary in August 2014, all organisations now deal with some external users online (Figure 3). Of the 300 organisations interviewed for this report only 5 (1.67%) were not involved with transacting online with other businesses or consumers. Even this tiny minority had to manage contractors and/or remote employees. The need for multi-constituency identity management is pervasive, however many of the systems in place were not designed to meet this need.

A useful segmentation of the data is to look at those that deal with consumers – consumer-facing – and those that deal purely with other businesses and/or contractors – non-consumer-facing (Figure 4). It turns out that those that deal with consumers view identity management differently to those that do not – why should this be the case?

First, there is the volume involved; on average, consumer-facing organisations deal with three times as many users as their non-consumer-facing counterparts (Figure 5). The volumes are highest in financial services and transport, with the growth of online banking and booking/ticketing systems (Figure 6). Average volumes for retail are lower because of the many mid-market retailers that take advantage of the web to reach out to small communities of special interest buyers.

Figure 3: External users interacted with online



*Includes students

Figure 4: External interaction by industry sector

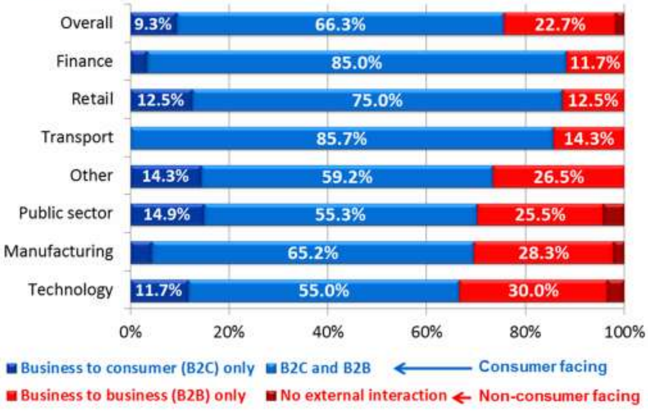
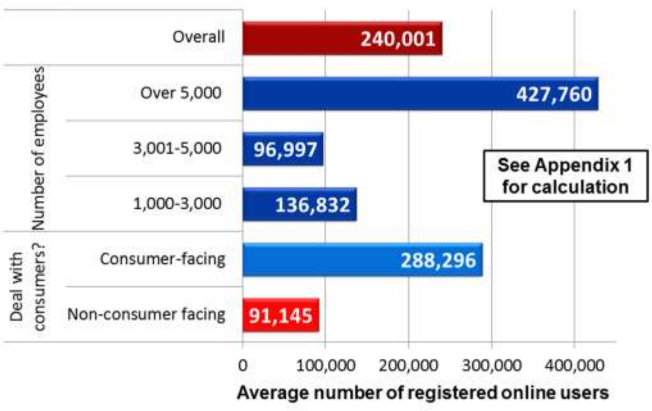
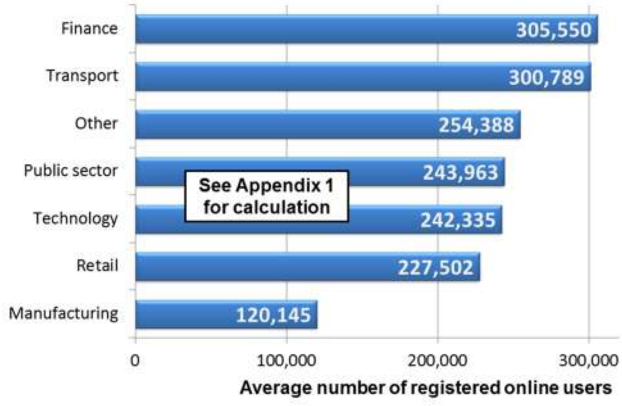


Figure 5: Number of registered external users



See Appendix 1 for calculation

Figure 6: Number of registered external users ***By industry sector***



See Appendix 1 for calculation

As online resources have moved from being purely informational to highly transactional there is more need to register users and capture information about them. All organisations recognise the importance of their online presence (Figure 7), but this is true more so of consumer-facing organisations, especially in two areas; online payments and social media (Figure 8).

Most consumers will pay for goods and services online as they go, whereas many business-to-business relationships may operate via credit arrangements. The high level of social media use is interesting; it is not just that this has become an important channel for reaching consumers, it is also fast becoming a way to identify them and it helps overcome complexity of access, a second reason why consumer-facing organisations are taking a different view of identity management.

Business users are more tolerant of complex, inflexible time consuming processes; after all it is their employer's time being wasted not their own. Consumers expect things to be as easy as possible and find creating and managing lots of identities a burden. They already have their own social identities from Facebook, LinkedIn, Twitter and so on, which they are more and more comfortable with using for gaining access to other online services.

To capitalise on this and safely extend the perimeter of the modern organisation requires a new approach to IAM. Most legacy systems are not designed for managing external users, federating identities from various sources and certainly not for integrating social identities. However, for the majority, these older IAM systems are the current starting point.

Figure 7: Importance of online services for interacting with external users

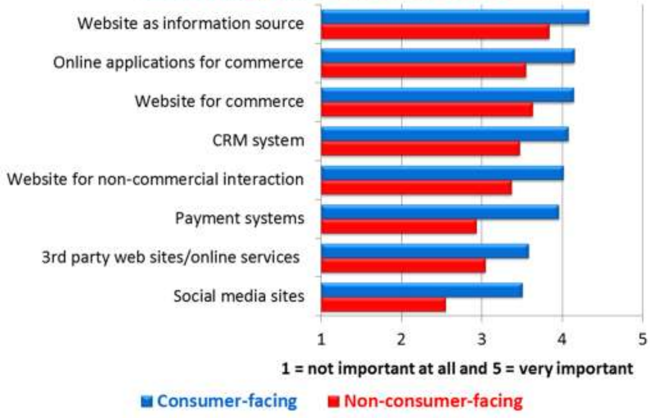
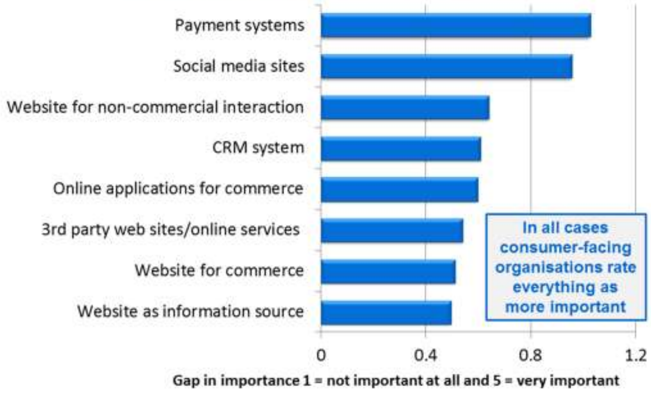


Figure 8: Importance of online services for interacting with external users *GAP ANALYSIS*



In all cases consumer-facing organisations rate everything as more important

Extending current IAM deployments

The fact that having IAM in place is nothing new for most organisations can be a problem. Many are attempting to adapt existing systems to purposes for which they were not designed – such as external users, federated identity management and the integration of social identities (Figure 9). Typically these are stack-IAM systems, those that come along with the software provided by broad-base infrastructure vendors such as IBM and Oracle.

That stack-IAM is hard to bend to new requirements is evident from the fact that those using it for external user management are more likely to have acquired additional IAM technology. Those extending stack-IAM to deal with outsiders have an average of 2.1 IAM suppliers, whilst those using it just for internal purposes have just 1.8 (Figure 10). A second reason for this supplier complexity in some organisations will be merger and acquisition activity.

It makes sense to use legacy capabilities that are part of the incumbent technology stack, especially existing directories such as Microsoft Active Directory, which is still rated the most important source of identity (Figure 11). However, other sources of identity are becoming more important, especially for consumer-facing organisations that recognise the importance of social identity, government databases (that contain citizen data), the directories of partners, and those of professional organisations (Figure 12).

Figure 9: Use of stack-IAM *(tools integrated into technology stack, e.g. from Oracle and IBM)*

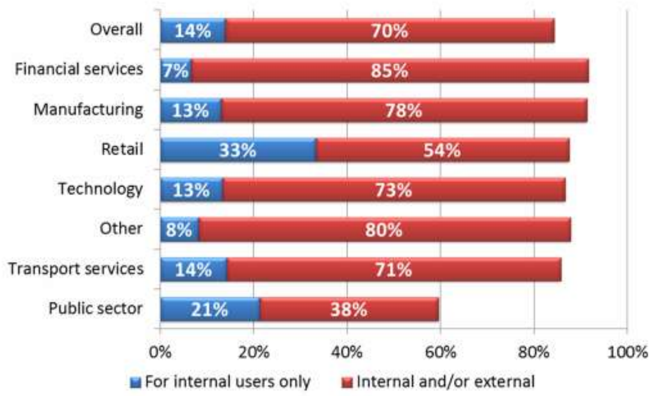


Figure 10: Number of IAM vendors against status with regard to the use of stack-IAM

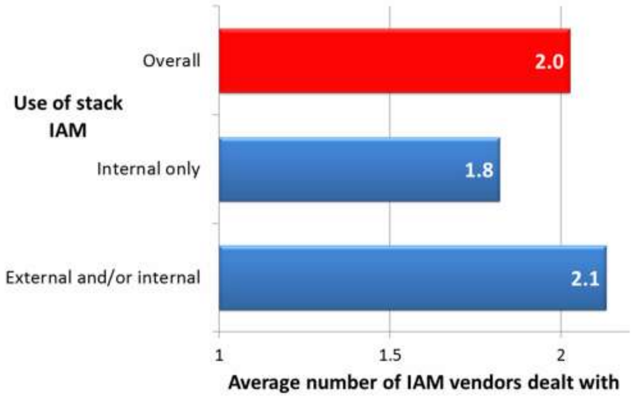


Figure 11: Importance of identity sources for external users

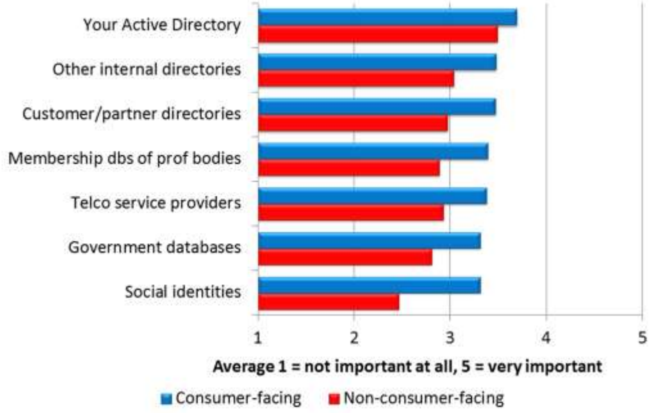
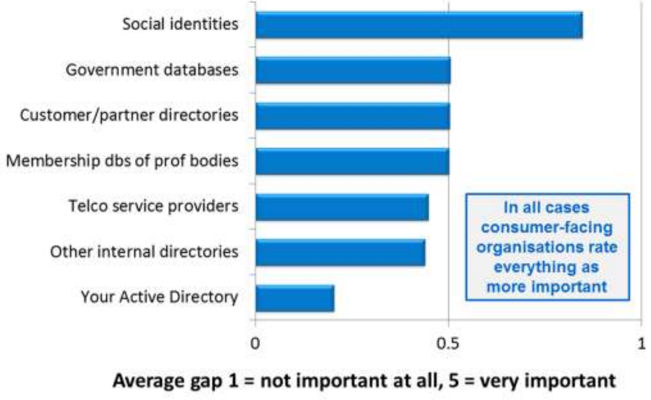


Figure 12: Importance of identity sources for external users – ***GAP ANALYSIS***



In all cases consumer-facing organisations rate everything as more important

Bringing new products in-house is not the only way to extend IAM systems. It is more likely that an organisation will turn to cloud-based services and create a hybrid mix of on-premise and on-demand technology to meet their requirements (Figure 13). Consumer-facing organisations are making this move fastest, for example with SSO and federated identity management (Figure 14). New suppliers are being brought into the IAM mix to help manage outsiders and to capitalise on and establish trust in new identity sources. Furthermore, even if the IAM systems are managed and owned by third parties, the sense of ownership of the relationship needs to remain with those providing online services to consumers and/or other businesses.

Figure 13: How aspects of IAM are deployed

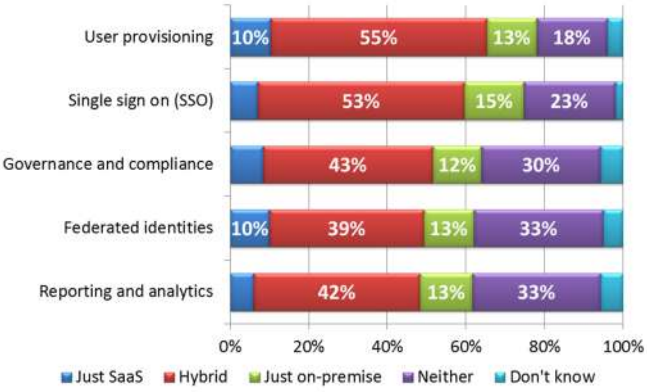
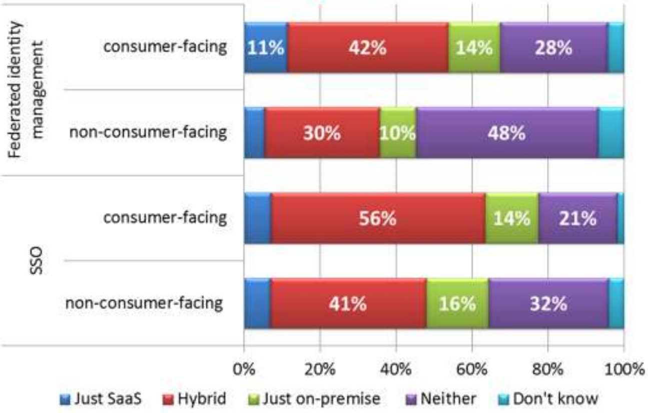


Figure 14: Deployment of SSO and federated identity management



Identity ownership and trust

Abdication to third party providers of cloud-based IAM services is not total. The majority of organisations procuring such services still feel they should own and manage the actual identities and therefore relationships (Figure 15). Whilst it may make sense for third parties to run the technology, the identities themselves are a key business asset that most want to maintain direct control of.

There is a tension emerging here. How can an organisation make use of identities coming from third parties but maintain control? A capability is needed for various external identities to be co-ordinated from a central system and integrated with other information such as resource access rights; this is the concept of federated identity management. For federation to be effective, trust in external identity sources needs to increase (Figure 16).

Some, for example customer and partner directories, are already seen as fairly safe, as are government databases (especially by public sector organisations). Social media is lowest on the list. This should improve with familiarity and as social media sites adopt standards.

The majority of organisations now recognise the value of various IAM standards (Figure 17). LDAP (light directory access protocol) may top the list, but this may be down to familiarity. Microsoft Active Directory is an LDAP based directory and its challenge/response system is considered too insecure by many for managing external identity sources; too much information has to be shared. This is leading to growing interest in other more secure standards.

These include OAuth – a framework for the open but secure sharing of identity data that uses tokenisation – and OpenID Connect, which layers on top of OAuth and provides a way of authenticating users from one system to another without the need to share passwords. Google, Facebook and Twitter now all support OAuth, allowing their identities to be more easily used for authentication by those providing other services whilst still protecting the personal details they hold on their users. Other standards including SCIM, SAML, REST and FIDO are all gaining attention (see Table 1).

Figure 15: Views on ownership of the identities of external users

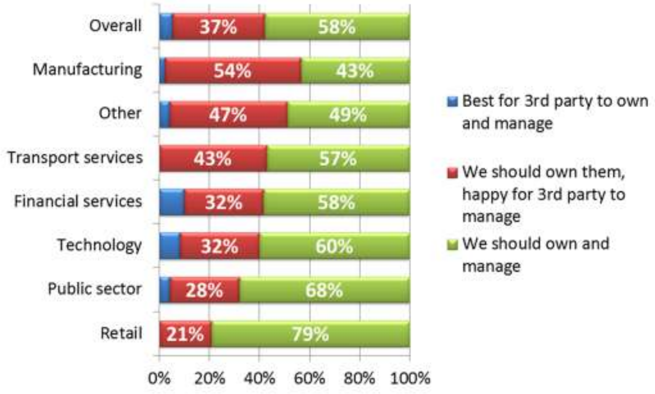


Figure 16: Trust in identity sources

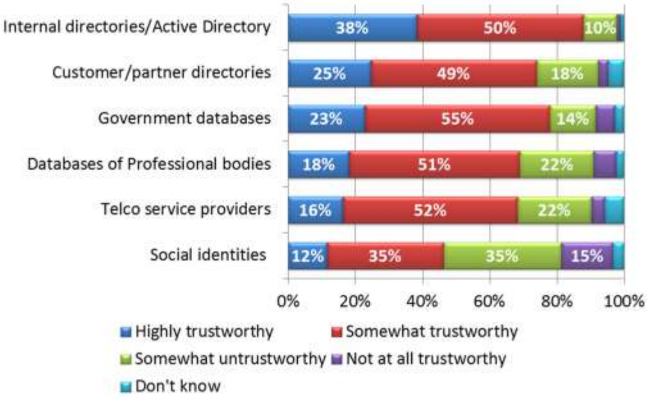


Figure 17: Importance of IAM standards
See table 1 for definitions

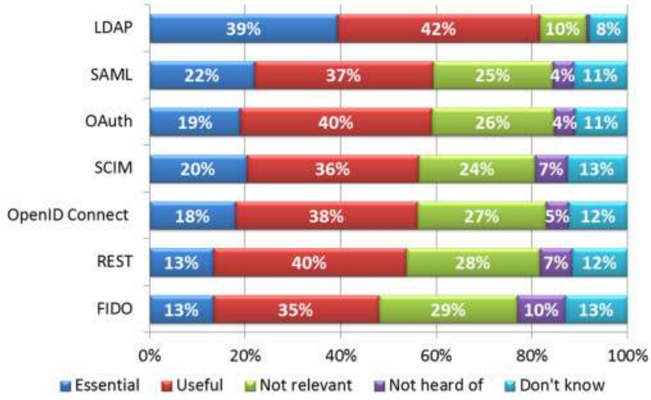


Table 1: IAM Standards

LDAP (lightweight directory access protocol) – a standard for storing, reading and sharing identity data; Active Directory is LDAP compliant.

SAML (security assertion mark-up language) – an open standard for securely exchanging authentication and authorisation data, for example between an SSO system and an application. SAML has been well vetted and provides a secure approach for the exchanging of identities.

REST (representational state transfer) – a standard for accessing web-enabled applications. Many of the resources that SSO systems need to provide access to will have APIs (application programming interfaces) that are REST compliant. REST has superseded older standards such as WSDL (web services description language) and SOAP (simple object access protocol), as it is simpler to use.

SCIM (system for cross-domain identity management) – a standard designed to make managing user identity in cloud-based applications and services easier when interfacing with SAML and REST compliant applications.

OAuth (open authentication) – a standard that enables users to access resources without having to directly disclose their login credentials; instead they use tokens.

OpenID Connect – an emerging standard that extends the consumer-oriented OpenID specification to support more complex use cases, including REST-based calls.

FIDO (fast identity online) – allows users to use their preferred method for strong authentication to various resources.

The transport sector is in the vanguard when it comes to trusting in social identities (Figure 18). This may be because the risk of someone trying to travel in another's name is relatively unlikely compared to attempts to gain access to a bank or retail account. Technology organisations also have quite a lot of confidence in social identities, perhaps because they understand them better. The public sector is the most suspicious.

Not all social identities are equal; some are trusted more than others (Figure 19). Microsoft tops the list, most organisations having used its products for years, and this may reflect general familiarity rather than specific trust in it as a provider of social identity. PayPal and Amazon are also high on the list; they both handle financial transactions already and are expected to be secure.

Figure 18: Trust in social identities

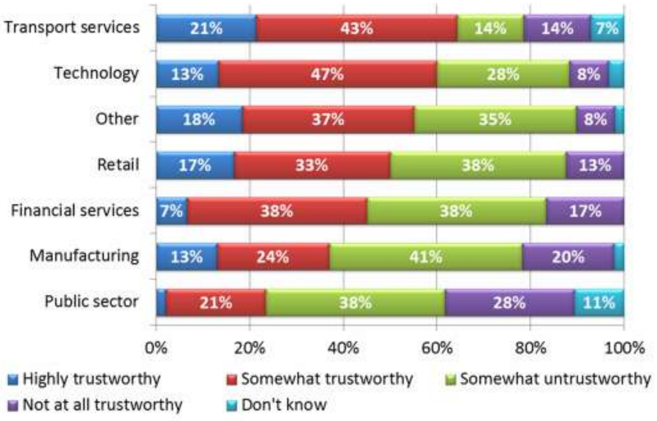
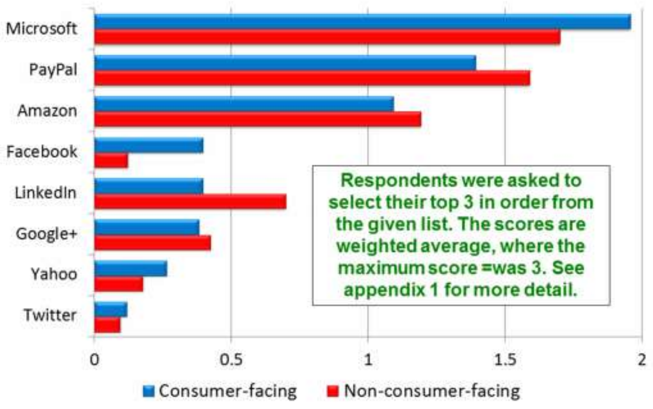


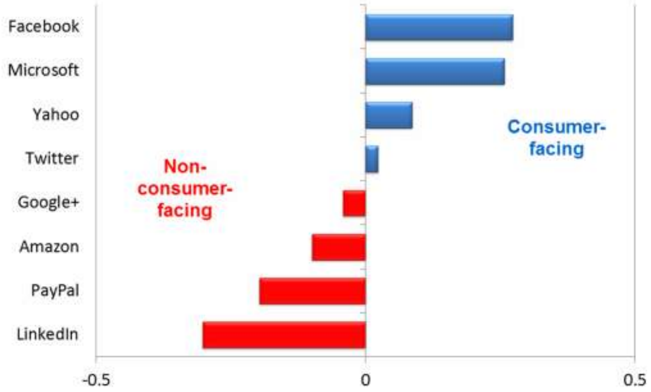
Figure 19: Most trusted social identities



Respondents were asked to select their top 3 in order from the given list. The scores are weighted average, where the maximum score =was 3. See appendix 1 for more detail.

There is a lot less trust in the rest, although consumer-facing organisations, recognising the value of Facebook's widespread use, are more likely to trust it (Figure 20).

Figure 20: Most trusted social identities
GAP ANALYSIS



All this may seem irrelevant to non-consumer-facing organisations, but they are not setting the agenda. As the majority of organisations that do deal with consumers turn more and more to social media, all organisations may find that they have no choice. The concept of bring-your-own-identity (BYOID) may be forced on them from the consumer market as the idea extends to employees.

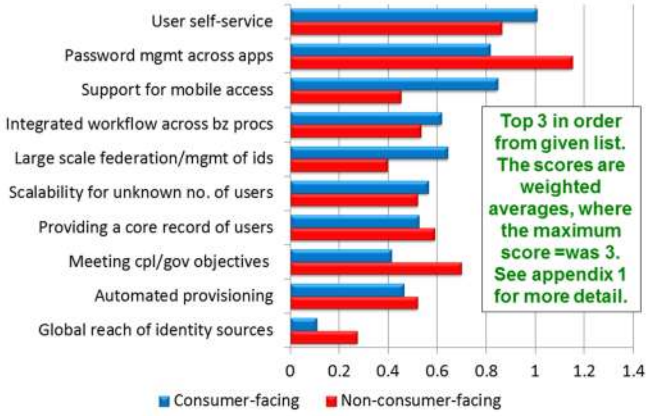
There is an old world analogy with passports. A new hire is not issued national identity travel documents by a new employer, they supply their own and take them from one job to another. There may be a future where this is also true for online identities. If the time comes when we all fully own our own digital identities, then from an identity management perspective all users will start as outsiders and IAM systems will need to be purely focussed on managing identities from external sources.

Investing to support external users

For all organisations the IAM capabilities that top the list of priorities when it comes to dealing with external users are self-service and password management across applications (Figure 21). This helps cut out the most resource intensive problem – users forgetting their access credentials – but also enables self-provisioning of new resources. Beyond this, significant differences emerge between consumer-facing and non-consumer-facing organisations (Figure 22). For the former, volume and mobility issues are more important, whilst for the latter it is more about compliance and scope of access.

The barriers to investment are not overwhelming (Figure 23). Proving a return-on-investment and securing budget are seen as the toughest issues, but even these are, on average, considered more or less neutral on a scale of 1 to 5. That there is any doubt at all may be because the question is being asked; "*we have already invested in IAM capability, so why not use that?*" In all areas consumer-facing organisations report finding that justifying investment is harder. This may just be because their need for new capability is more pressing, especially as they are more likely to have IAM capabilities in place (Figure 24); i.e. they are pushing their case hardest.

Figure 21: Most important IAM features for managing external users



Top 3 in order from given list. The scores are weighted averages, where the maximum score =was 3. See appendix 1 for more detail.

Figure 22: Most important IAM features for managing external users ***GAP ANALYSIS***

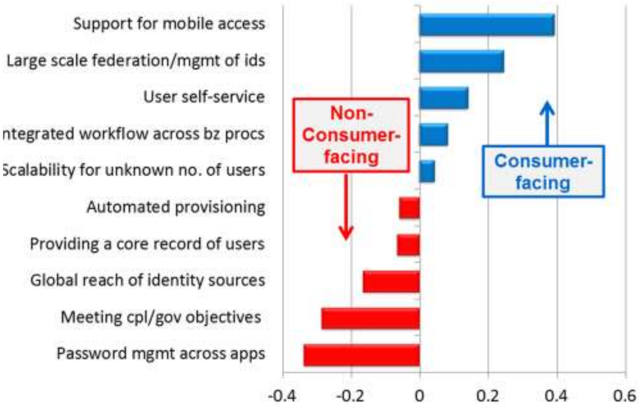


Figure 23: Barriers to IAM investment for the management of external users

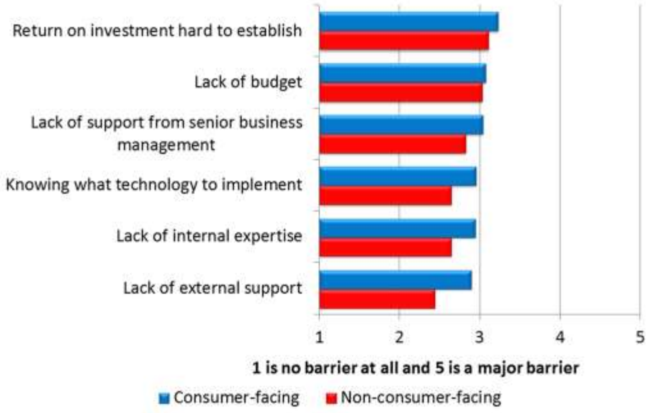
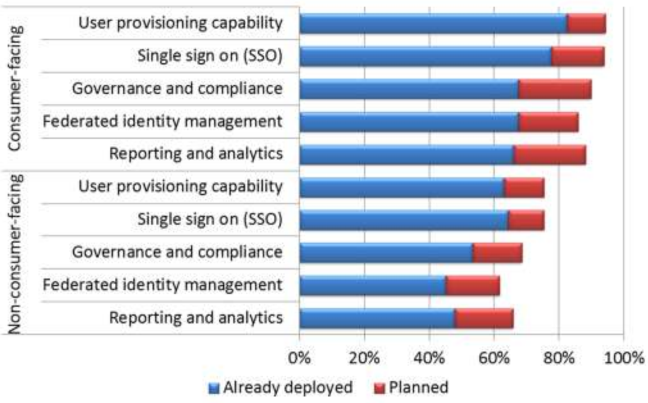


Figure 24: Deployment of IAM capability
Consumer-facing versus non-consumer-facing

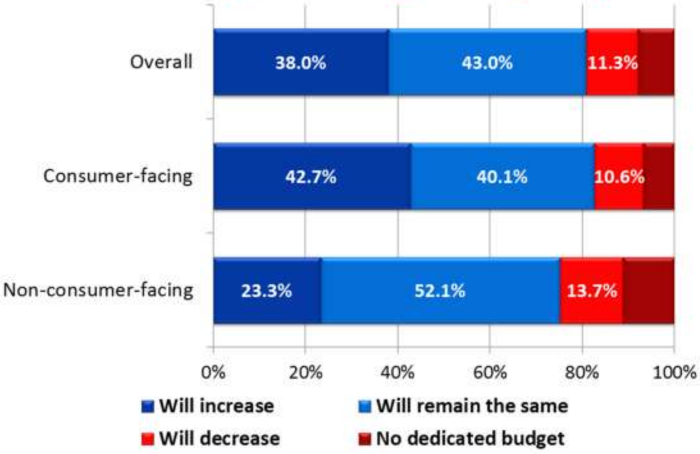


Conclusion

Identity is the ultimate way to gain control over a mobile, cloud-connected user base that includes employees, consumers, and users from business customers and partners. Those charged with the task know the capabilities they need are available, but not always in the systems they have in-house. The case needs to be made to upgrade, supplement or replace existing IAM systems as there is a perception that legacy systems should be up to the job – in many cases they are not.

The good news is that those responsible for delivering online resources in consumer-facing organisations are getting their case across. Their dedicated budgets for IAM are more likely to increase than average, compared to their non-consumer-facing counterparts (Figure 25). The laggards will have to catch up with the leaders at some point or lose sight of the organisation's perimeter altogether.

Figure 25: Dedicated budgets for supporting online resources – expected change during next year



Appendix 1 - calculations

Calculation of transaction volumes

For the data used in Figures 5 and 6 the original question was put to respondents as follows:

What best represents the number of individual external users that your organisation has a relationship with that requires them to register in some way for access to certain online resources?

1. Tens (10s)
2. Hundreds (100s)
3. Thousands (1,000s)
4. Tens of thousands (10,000s)
5. Hundreds of thousands (100,000s)
6. Millions (1,000,000s)
7. Don't know

To calculate an average number the following figures were used:

- Tens set as 50
- Hundreds as 500
- Thousands as 5,000
- Tens of thousands 50,000
- Hundreds of thousands 500,000
- Millions as 2,000,000 (this figure may be on the low side)
- Don't know, just 2/300 responses – ignored

Calculation of weight averages for top 3 most trusted identities and top 3 IAM features

For the data used in Figures 19 and 20 the original question was put to respondents as follows:

Which of the following three websites would you trust most as a source of identity?
Please rank your top three answers in order of how trustworthy they are

- Amazon
- Microsoft
- Yahoo
- Facebook
- Google+
- Twitter
- LinkedIn
- PayPal

The website ranked first was given a score of 3, second a score of 2 and third a score of 1. Non selected websites were scored 0. For each website the average score was then calculated. If all had ranked the same website as most important it would have scored 3 on average, if none had selected a given website it would have scored 0.

For the data used in Figures 21 and 22 the original question was put to respondents as follows:

Which of the following three features of an IAM system are most important to your organisation for managing external users?

- Automated provisioning
- Integrated work flow across business processes
- User self-service (e.g. for password reset or requesting access to applications and resources)
- Password management across applications
- Support for mobile access
- Scalability to manage an unknown number of users
- Large scale federation/management of identities
- Providing a core record of who a user is across the business
- Meeting compliance/governance objectives
- Global reach of identity sources

The choice ranked first was given a score of 3, second a score of 2 and third a score of 1. Non selected features were scored 0. For each feature the average score was then calculated. If all had ranked the same feature as most important is would have scored 3 on average, if none had selected a given feature it would have scored 0.

References

1 - These figures are similar to those from Quocirca's 2013 report Digital identities and the open business http://quocirca.com/content/digital-identities-and-open-business

2 – The identity perimeter http://quocirca.com/content/identity-perimeter

Appendix 2 - demographics

Figure 26: Countries
(actual sample numbers)

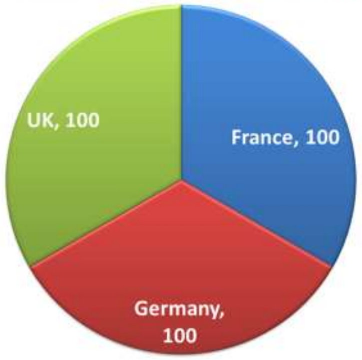


Figure 27: Number of employees
(actual sample numbers)

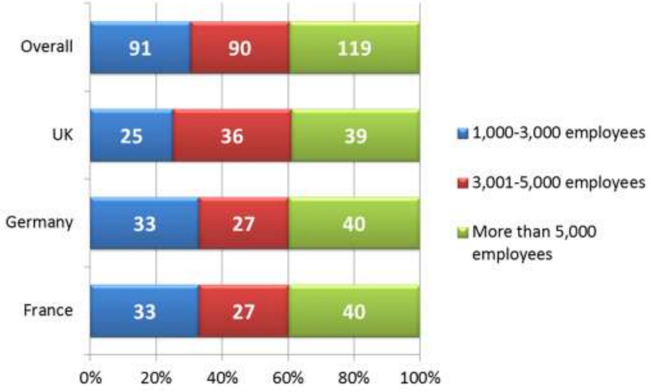


Figure 28: Industry sectors

Please note the small size of some samples, in particular pharmaceuticals which is added to "others" in the further analysis

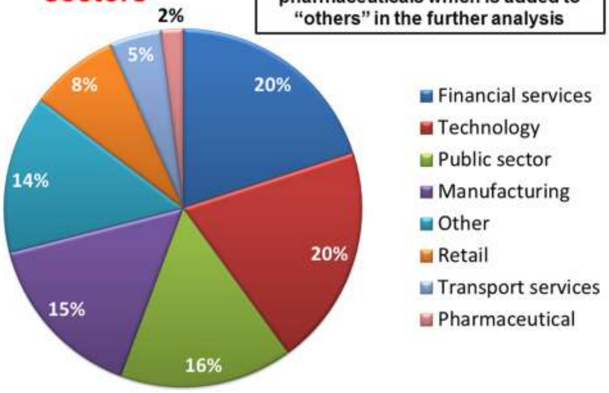


Figure 29: Industry sectors, by country
(actual sample numbers)

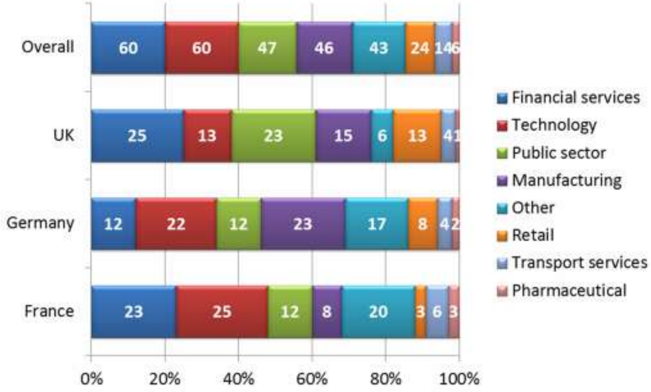
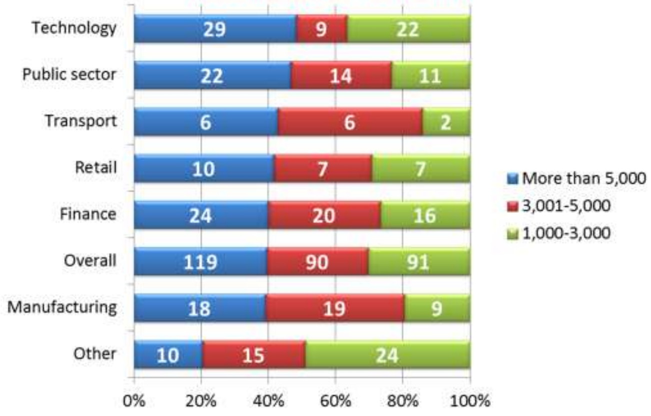


Figure 30: Industry sectors, by number of employees
(actual sample numbers)



About Ping Identity | The Identity Security Company

Ping Identity is the pioneer and largest independent provider of next-generation identity security solutions. With more than 1,200 customers worldwide including half of the Fortune 100, Ping Identity is transforming the way hundreds of millions of people live and work every day by making their favourite apps more convenient and secure to access from any device, anywhere. Visit pingidentity.com for more information.

About Quocirca

REPORT NOTE:
This report has been written independently by Quocirca Ltd to provide an overview of the issues facing organisations seeking to get the most out of their online domains.

The report draws on Quocirca's extensive knowledge of the technology and business arenas, and provides advice on the approach that organisations should take to create a more effective and efficient environment for future growth.

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first-hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to provide advice on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, IBM, CA, O2, T-Mobile, HP, Xerox, Ricoh and Symantec, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca's work and the services it offers can be found at http://www.quocirca.com

Disclaimer:
This report has been written independently by Quocirca Ltd. During the preparation of this report, Quocirca may have used a number of sources for the information and views provided. Although Quocirca has attempted wherever possible to validate the information received from each vendor, Quocirca cannot be held responsible for any errors in information received in this manner.

Although Quocirca has taken what steps it can to ensure that the information provided in this report is true and reflects real market conditions, Quocirca cannot take any responsibility for the ultimate reliability of the details presented. Therefore, Quocirca expressly disclaims all warranties and claims as to the validity of the data presented here, including any and all consequential losses incurred by any organisation or individual taking any action based on such data and advice.