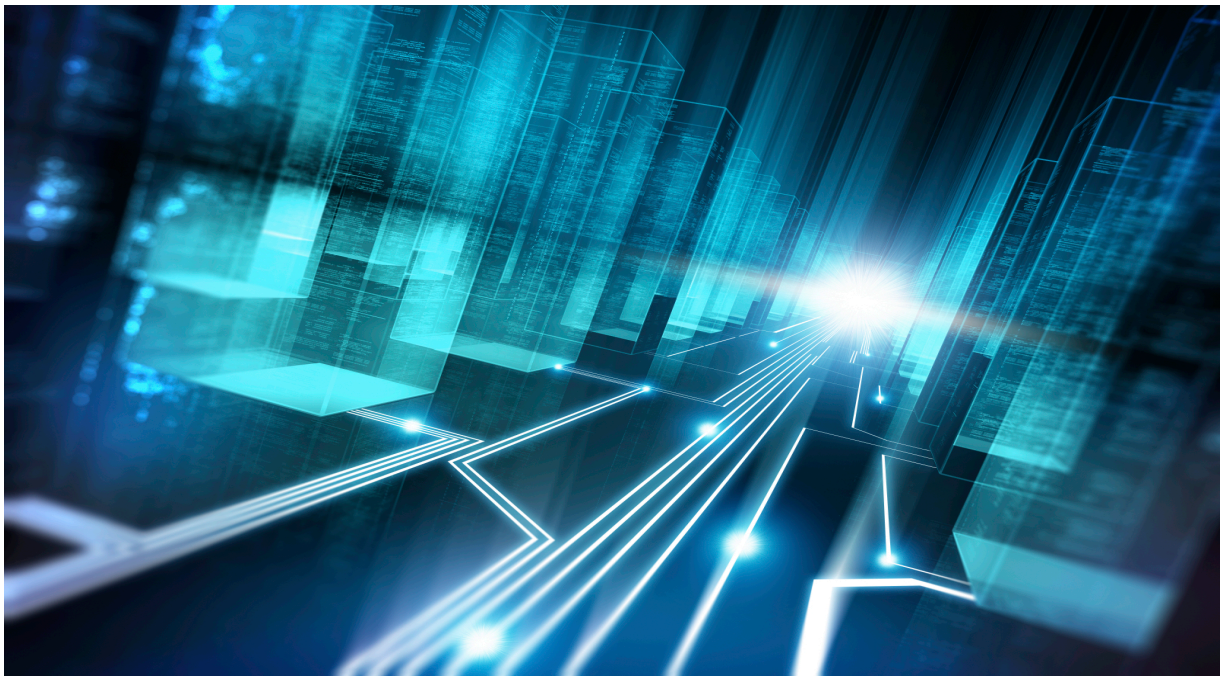


The Identity Imperative for the Open Enterprise: What IT Users & Business Users Think about Bring Your Own Identity (BYOID)

Sponsored by CA Technologies

Independently conducted by Ponemon Institute LLC

Publication Date: July 2014

The Identity Imperative for the Open Enterprise: What IT Users and Business Users Think about Bring Your Own Identity (BYOID)

Ponemon Institute: July 2014

Part 1. Introduction

Ponemon Institute is pleased to release the findings of *The Identity Imperative for the Open Enterprise: What IT Users and Business Users Think about Bring Your Own Identity (BYOID),* sponsored by CA Technologies. In this study, we surveyed 1,589 IT and IT security practitioners and 1,526 business users to understand current trends in Bring your Own Identity or BYOID, which is defined as the use of trusted digital or social networking identities.

This survey was conducted with IT users and business users at organizations with more than 1,000 employees in United States, Australia, Brazil, Canada, France, Germany, India, Italy and the United Kingdom. Almost all of the IT users surveyed report to the CIO (74 percent) or CISO (15 percent); the business users in this research report to the lines of business leader (55 percent), chief marketing officer (10 percent), with the rest dispersed across other business functions.

The majority of respondents in both groups have high levels of interest in BYOID, but IT users and business user groups have different views about the perceived potential value of BYOID. Generally speaking, the IT users view BYOID primarily for fraud reduction, risk mitigation and cost reduction while the business end users are more interested in how BYOID can streamline customer's experience and assist in targeted marketing campaigns.

Some of these differences can be expected because of the different job responsibilities of each group. These differences do not necessarily portend conflict, but rather show the need for collaboration between IT and the business functions to yield maximum benefits for any organization deploying a BYOID system. By developing a cross-functional BYOID strategy around several well-defined use cases, organizations can differentiate themselves from competitors and further grow their business.

An analysis of the research findings reveals the following important takeaways:

The Application Economy Drives BYOID Interest

In today's application economy, organizations need to securely deliver new apps to grow their business quickly. This can increase IT risks, which puts a premium on an organization's ability to simplify the user experience without sacrificing security. Using an existing digital or social identity issued by a trusted third party to access applications can help organizations meet the need for simplicity, security and a positive customer experience.

According to the survey findings, IT users say the primary value of BYOID is from strengthening the authentication process (67 percent) and reducing impersonation risk (54 percent). Business users believe the BYOID value comes from delivering a better customer experience (79 percent) and increasing the effectiveness of marketing campaigns (76 percent).

While IT sees value primarily in risk mitigation/cost reduction, business users see the value of BYOID in improving the consumer experience to increase customer loyalty and generating new revenue streams. This underscores the need for IT and business collaboration to address the challenge that today's organizations face: how to secure the business while simultaneously empowering it.

Mobile and Web Users Drive BYOID

Today's IT organizations must deliver secure access to a highly distributed and growing user population. These users expect to access information anywhere, anytime from multiple

devices. This is changing how user identities should be managed and is affecting the demand for BYOID.

When IT practitioners and business users were polled on their level of interest in accepting identities for different user populations such as job prospects, employees, contractors, retirees, website customers or mobile customers, mobile and web customers received the most interest, far exceeding that of the other populations.

Fifty percent of IT respondents and 79 percent of business respondents have very high or high interest in BYOID for website user populations. Similarly, 48 percent of IT respondents and 82 percent of business respondents have very high or high interest in BYOID for mobile user populations.

BYOID Requires Security Enhancements to Drive More Adoption

While the survey results indicate interest in BYOID from both IT users and business users, both groups identified features that could contribute to broader BYOID adoption. When asked which features would most likely increase BYOID adoption within their organization, IT users' top features are identity validation processes (73 percent) and multi-factor authentication (66 percent). Business users say both identity validation processes and simplified user registration at 71 percent are the most popular features for increasing adoption.

The study also indicates a high level of interest for some level of accreditation of the identity providers with 59 percent of IT saying it is essential or very important and another 21 percent saying it is important. Only 27 percent of business respondents say accreditation is essential or very important. However, an additional 48 percent believe it's important.

Part 2. Key Findings

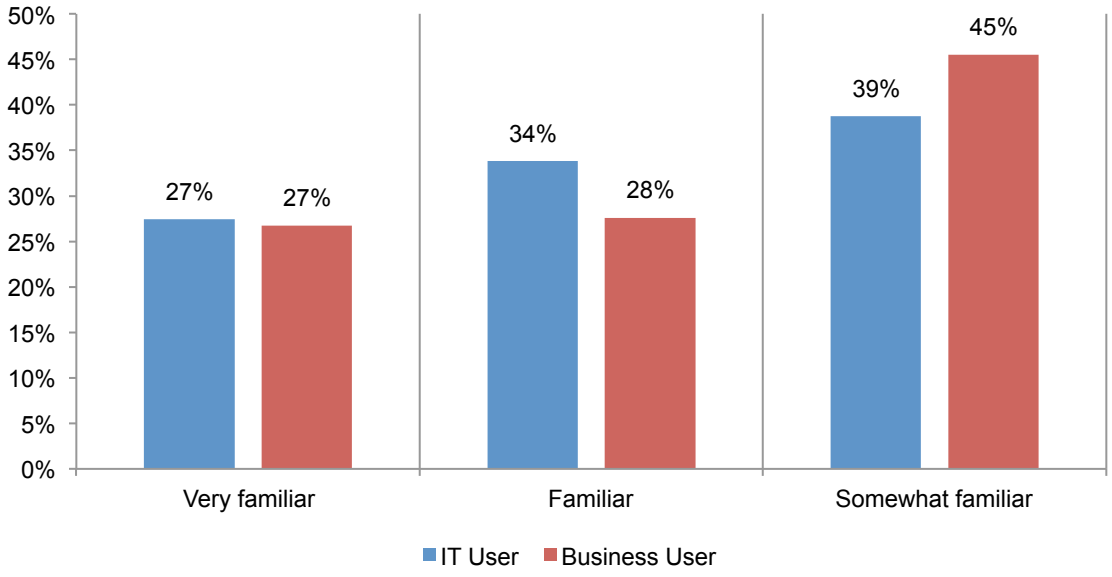
In the following sections, we present the key findings of this study in detail. The complete audited findings are presented in the appendix of this report. We have organized the report into the following four themes:

- Current global status of BYOID
- Quantifying the value of BYOID
- Perceptions about digital identity providers
- Reducing barriers to broader BYOID adoption

Current Global Status of BYOID

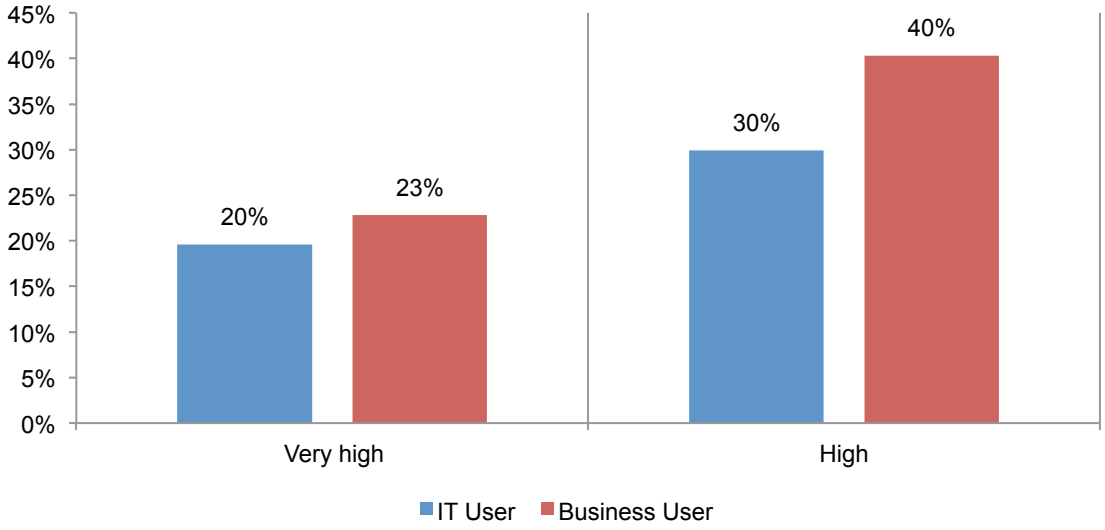
There is a high global awareness of BYOID. According to Figure 1, 61 percent of IT users say they are very familiar or familiar and 55 percent of business users say they have a high level of familiarity with BYOID.

Figure 1. Level of familiarity with the term BYOID



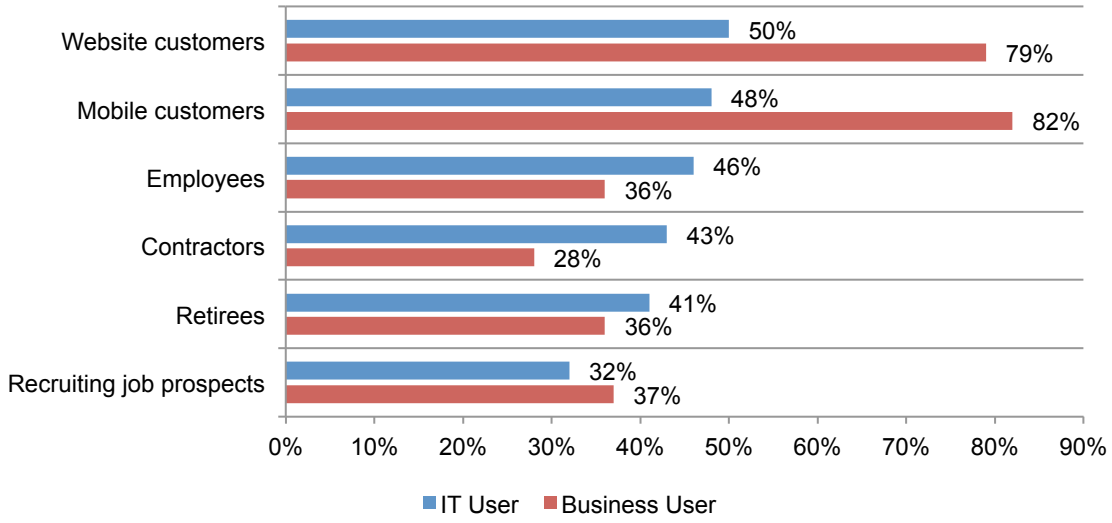
There is global Interest in BYOID. Interest in BYOID is high across all surveyed geographies. When asked what describes their organization's level of interest, 50 percent of IT users and 63 percent of business users say it is either very high or high, according to Figure 2. This indicates that BYOID is not purely a tech trend, but something that has value to business users as well.

Figure 2. Level of interest in BYOID



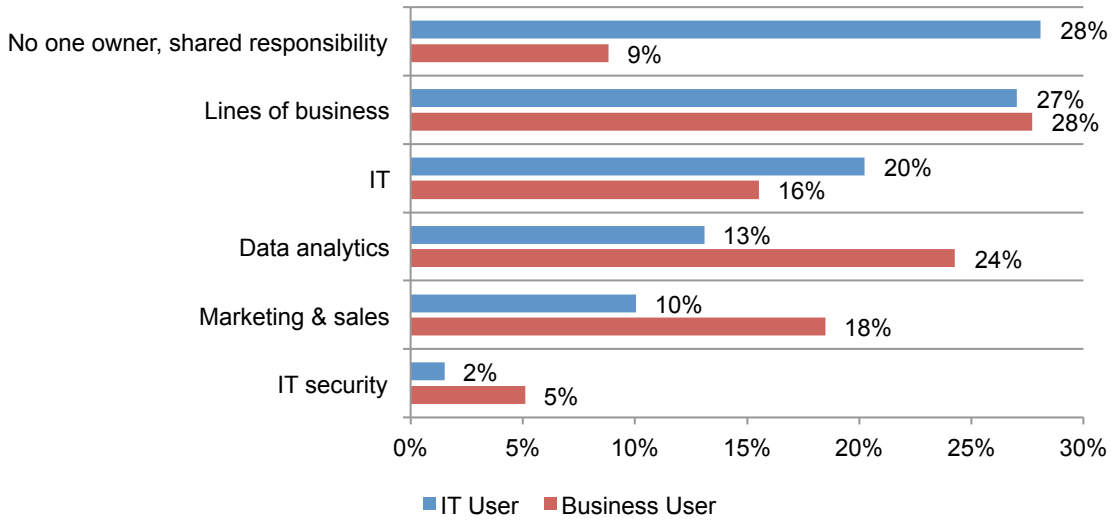
BYOID deployment using social IDs is still in its infancy, but interest is high, especially for mobile and web customer populations. As shown in Figure 3, customers engaging with the business via the Web and mobile devices are the highest rated for targeted digital identity engagement, eclipsing other populations such as job recruits, employees, contractors and retirees. This interest in mobile customers reflects the continued growth of mobile apps and devices as an increasingly popular way for customers to engage with organizations. Moreover, respondents probably see BYOID as greatly simplifying the user experience on mobile devices.

Figure 3. Level of interest in accepting digital identities from various populations
Very high and high response combined, more than one response permitted



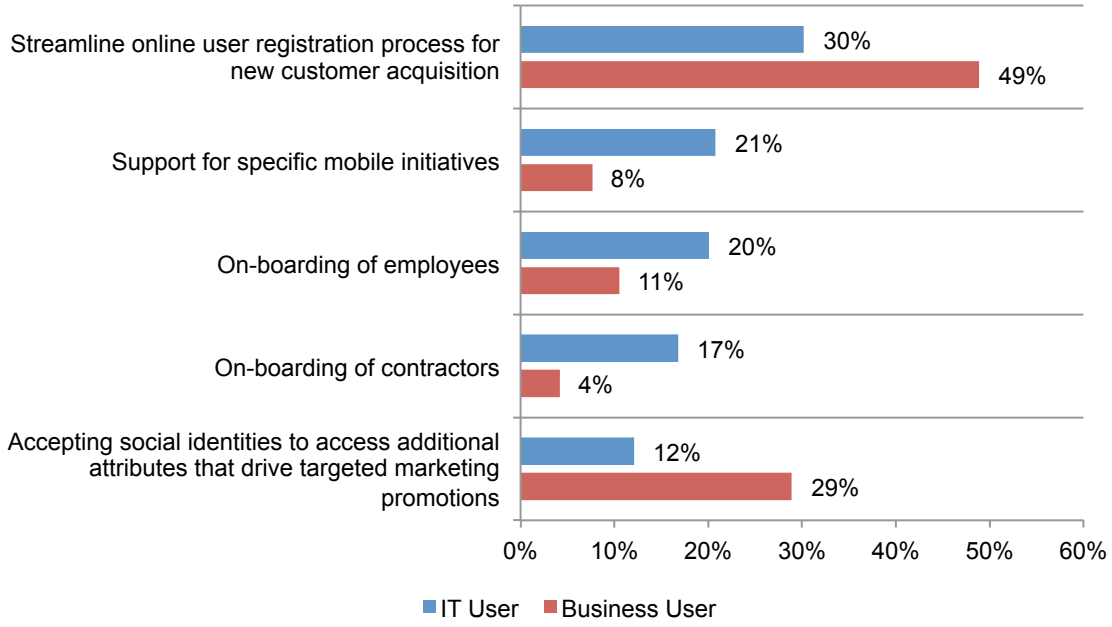
Ownership of digital identities is dispersed throughout organization. According to Figure 4, IT users say such ownership is most likely shared throughout the organization, lines of business or IT. Business users say it is lines of business, data analytics and marketing and sales. These results reinforce the need for collaboration across IT and business functions. Organizations might want to consider creating cross-functional alliances to encourage cooperation and teamwork to achieve greater value from BYOID.

Figure 4. Who controls or "owns" digital identities in your organization?



The most common BYOID use case involves making registration easier for users. As shown in Figure 5**,** Both IT users and business users view the ability to streamline the user registration process for customers as the most convincing case to adopt BYOID. Business users' second highest priority BYOID use case is to access additional identity attributes for targeted marketing purposes.

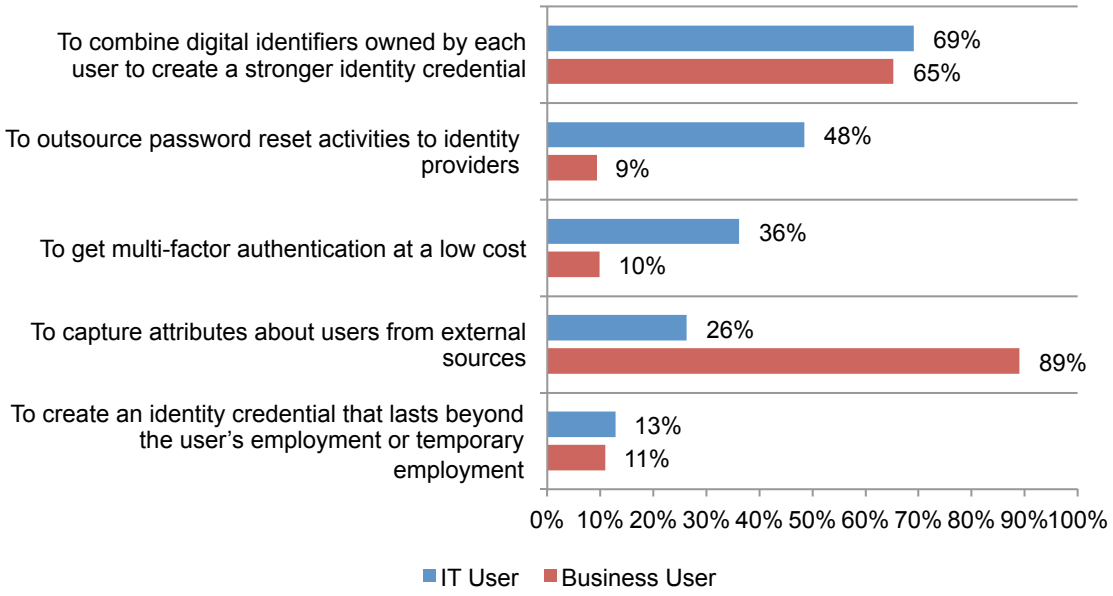
Figure 5. The benefits of BYOID use within the organization



Quantifying the Value of BYOID

IT users and business users have divergent reasons for valuing and adopting BYOID. IT users are primarily interested in using BYOID to combine digital identifiers owned by each BYOID user to create a stronger identity credential (69 percent of IT users). By contrast, the most popular reason for business users to adopt BYOID is to capture attributes about individuals from external sources (89 percent), as shown in Figure 6.

Figure 6. Main reasons for BYOID adoption in the organization today
More than one response permitted



When asked how BYOID adds value to the organization, both groups have vastly different answers, as seen in Figure 7. IT users see the primary value of BYOID coming from strengthening the authentication process (67 percent) and reducing the cost of insecurity (54 percent), whereas business users say the value of BYOID is delivering a better customer experience (79 percent) and increasing the effectiveness of marketing campaigns (76 percent).

Figure 7. How the creation and/or use of digital identities add value
More than one response permitted

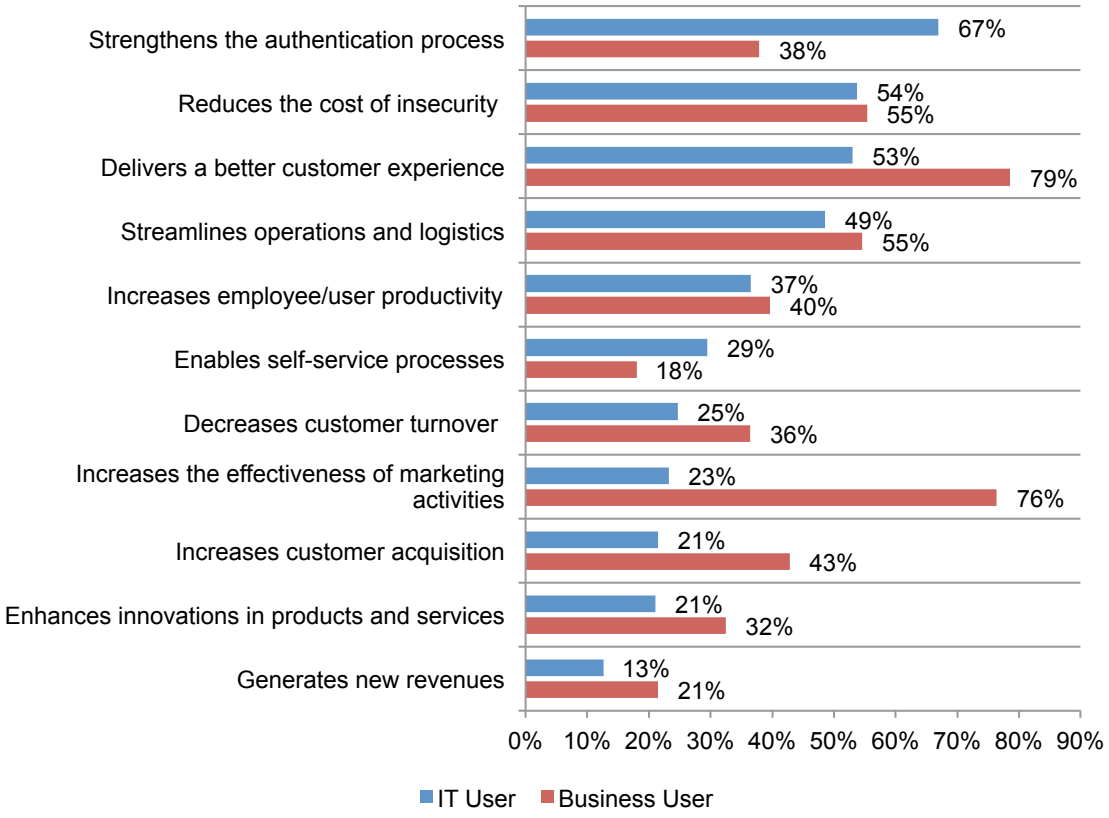
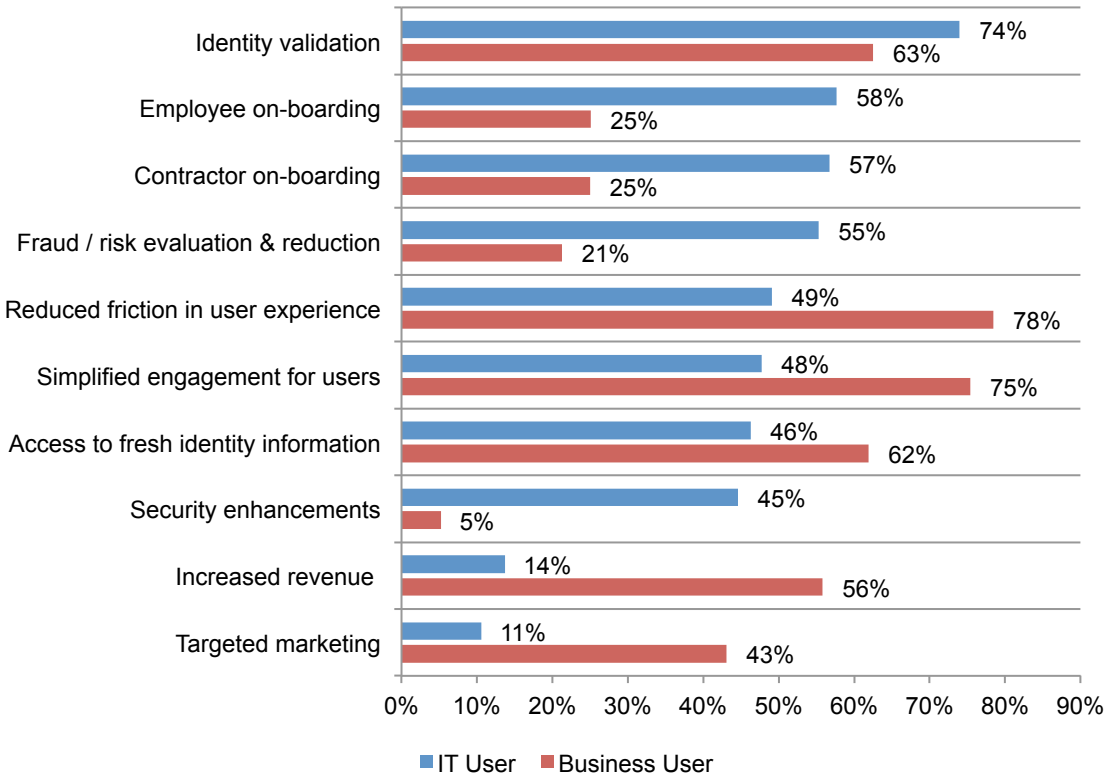


Figure 8 shows other BYOID benefits of interest. In the case of IT users, it is identity validation, employee and contractor on-boarding and reduction of fraud. Business users see the primary benefits as improving the customer experience such as reducing friction in the customer's experience and simplifying engagement.

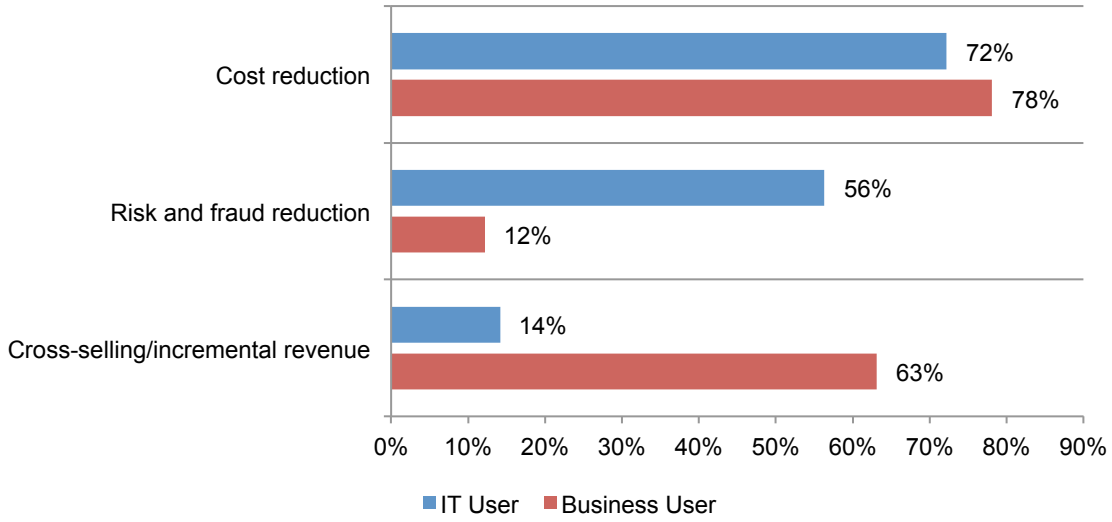
Figure 8. BYOID benefits of most interest to the organization
More than one response permitted



There is a gap between the IT users and business users in the adoption of measures to determine the value of digital identities. More business users (59 percent of respondents) than IT users (27 percent of respondents) say their organizations attempt to measure the added value resulting from the creation and/or use of digital identities.

According to Figure 9, if organizations do measure the added value of digital identities, the primary metric is cost reduction (72 percent of IT users and 78 percent of business users). Cost reduction from BYOID is due to minimizing the overhead and resources associated with managing forgotten passwords and sign-in problems. In large business-to-consumer websites with millions of customers, these savings can be significant and can enable the organization to redeploy those assets to support other revenue generating initiatives.

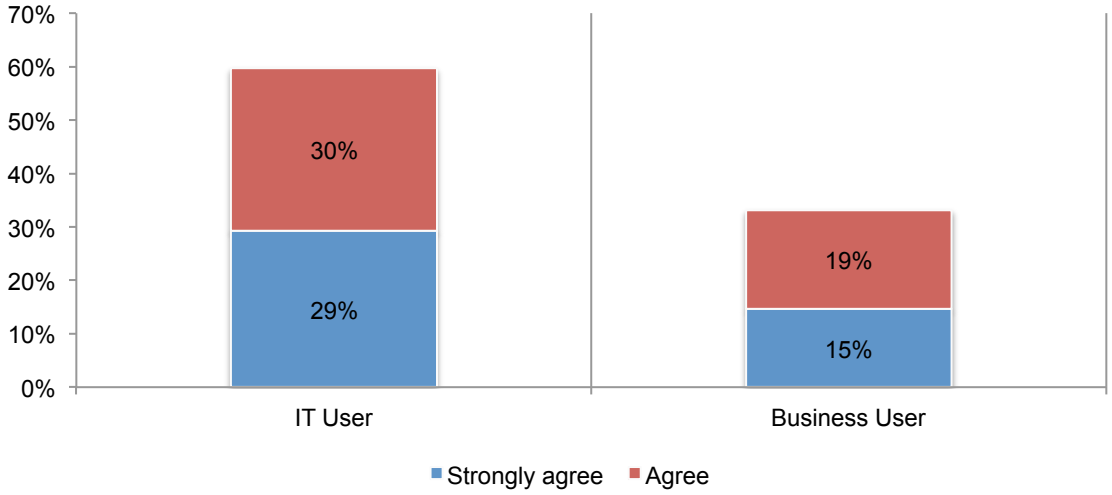
Figure 9. Measures to determine added value
More than one response permitted



Perceptions about Digital Identity Providers

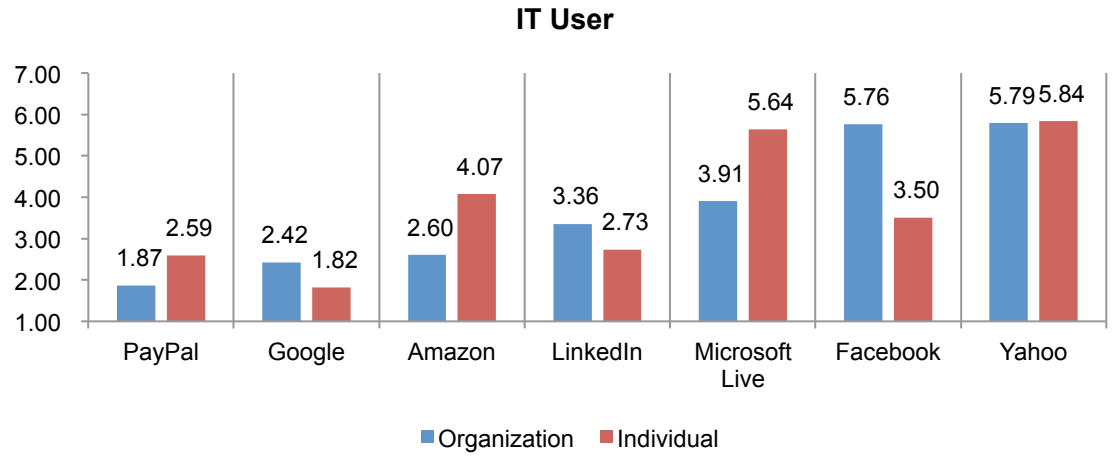
Trusted third party identity providers increase confidence. According to Figure 10, IT users are more likely to agree that their organization would be able to offer more online services and programs if those digital identities were validated by a trusted third party (59 percent of IT users strongly agree or agree and 34 percent of business users strongly agree or agree).

Figure 10. Agreement about the use of a trusted third party to validate digital identities



Who are the preferred digital identity providers? Respondents were asked to prioritize a list of identity providers for use as both an individual consumer and for use at their business. [1] As shown in Figures 11 and 12, IT users rank PayPal, Google and Amazon as their employers' top three preferred identity providers to their organization. Yahoo was ranked the lowest priority. The same IT users ranked Google, LinkedIn and PayPal as their personally preferred identity provider for accessing services as individuals.

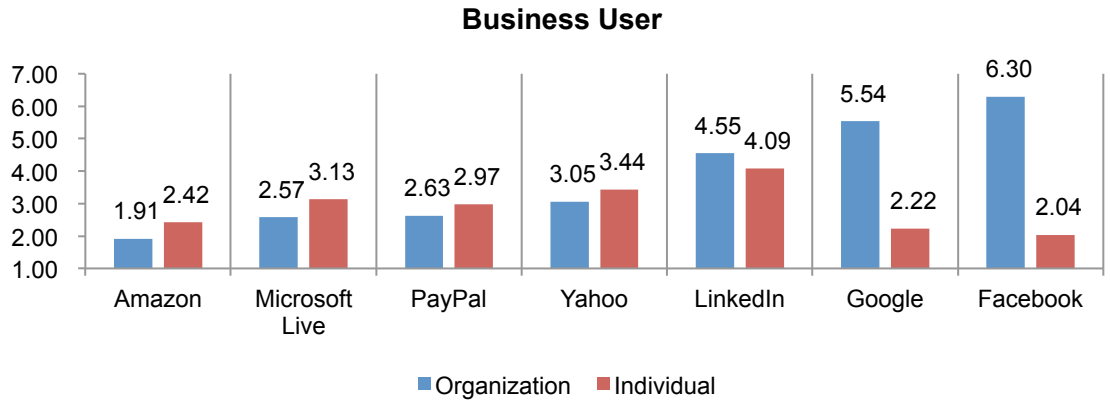
Figure 11. IT users rank identity providers
NOTE: 1 = of most interested to 7 = of least interest



[1] It is also worth noting that this research limits responses to the most common online identities. It is not a comprehensive list because many banks, financial institutions and governmental entities are identity providers for consumers around the globe.

Business users rank Amazon Microsoft Live and PayPal as their employers' top three identity providers. As individuals, business users ranked Facebook, Google and Amazon as their most popular providers.

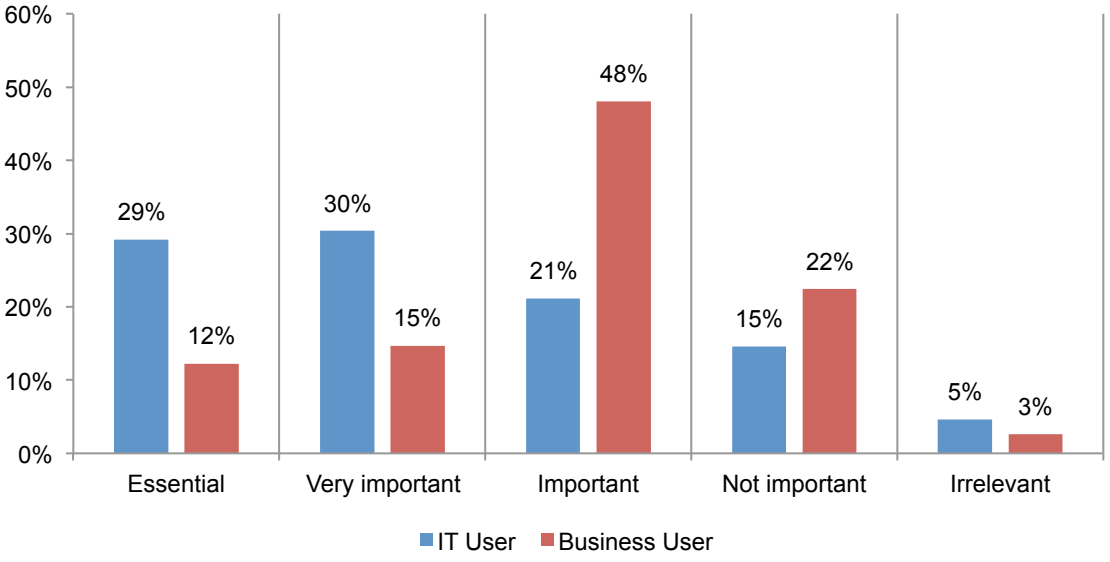
Figure 12. Business users rank identity providers
NOTE: 1 = of most interested to 7 = of least interest



Formal accreditation of the identity provider can be important. IT users are much more interested in identity providers having some formal accreditation, with 59 percent claiming it was essential or very important (Figure 13) and another 21 percent say it is important. Only 27 percent of business users believe formal accreditation is essential or very important.

As discussed previously, the different perceptions about preferred identity providers could explain the need for formal accreditation. It seems an independent validation of a given identity provider could increase overall confidence in a given identity and affect an organization's willingness to expand BYOID usage.

Figure 13. How important is formal accreditation of the BYOID identity provider?



Reducing barriers to broader BYOID adoption.

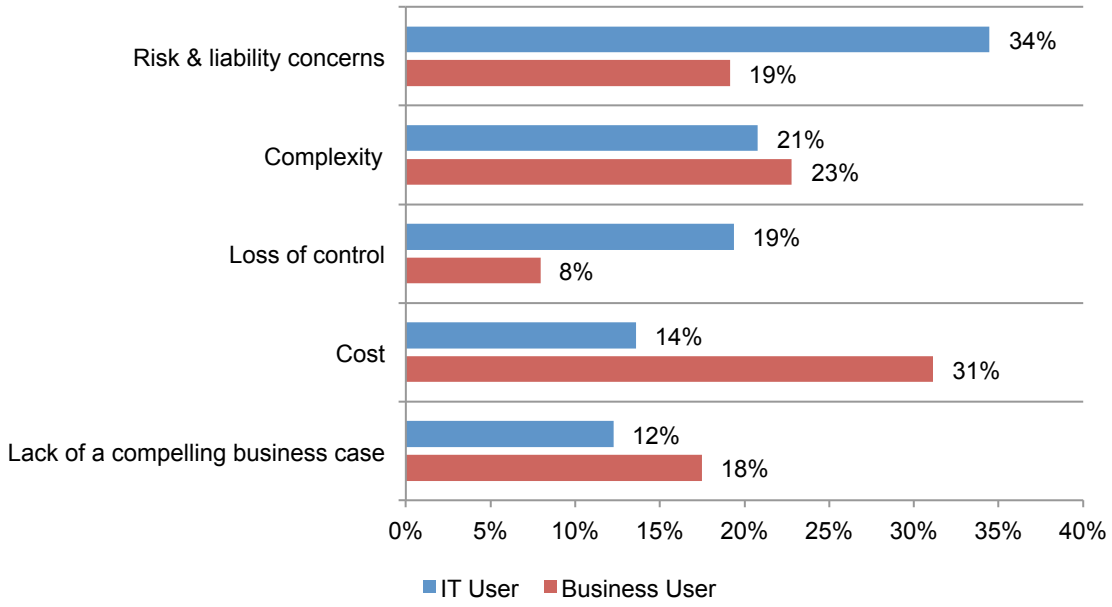
IT users have legitimate risk and liability concerns. While BYOID delivers business value, it is not without risk and liability concerns that may inhibit broader adoption.

First, some business users still resist utilizing a third party identity due to privacy concerns and a need to maintain anonymity. Some are also concerned about using a third party identity for certain transactions or scenarios. They might be perfectly satisfied with using social login to access a newspaper, but will not do the same to access their online banking account.

Organizations that accept third party identities also worry about instances where an identity is compromised and non-legitimate access is granted to applications or customer data. This adds to the complexity of how liability is handled in the event of a data breach or compromise.

Figure 14 reveals the barriers to BYOID that need to be addressed. Thirty-four percent of IT users say risk/liability concerns followed by complexity (21 percent) and loss of control (19 percent) are barriers to deployment. When asked to identify the most significant inhibitor to BYOID deployment in their organization, 31 percent of business users cite cost, followed by complexity (23 percent) and risk/liability concerns (19 percent).

Figure 14. Barriers to BYOID deployment



Identity validation processes increase adoption. When asked to identify which features would most likely increase BYOID adoption within an organization, IT users cite the following: the identity validation process (73 percent), multi-factor authentication (66 percent) and fraud risk engines (57 percent) as greatest areas of interest, according to Figure 15. In comparison, features business users are most interested in include: identity validation process (71 percent), simplified user registration (71 percent) and fraud risk engines (37 percent).

Figure 15. Features most likely increase BYOID adoption
More than one response permitted

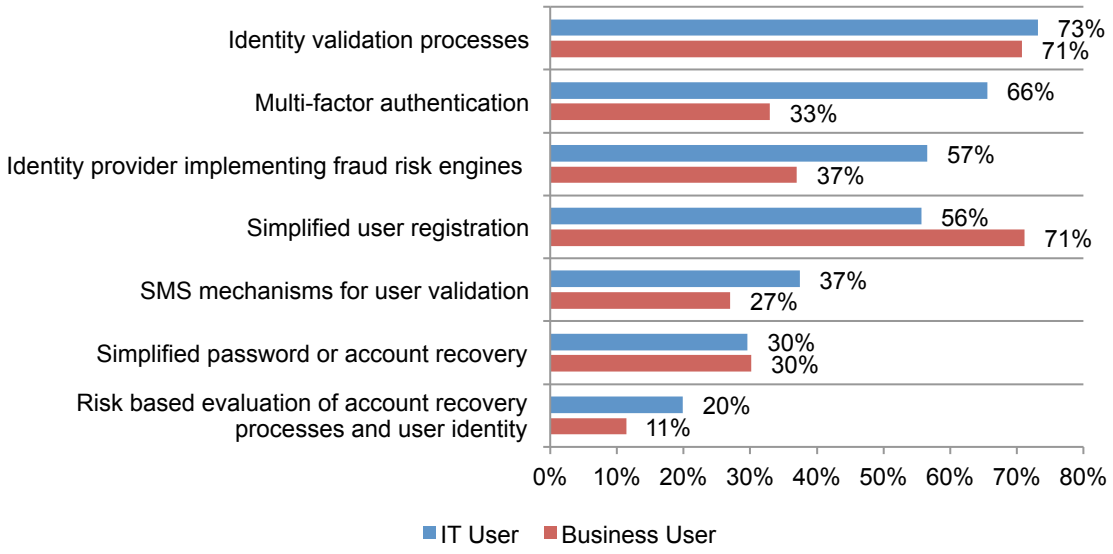
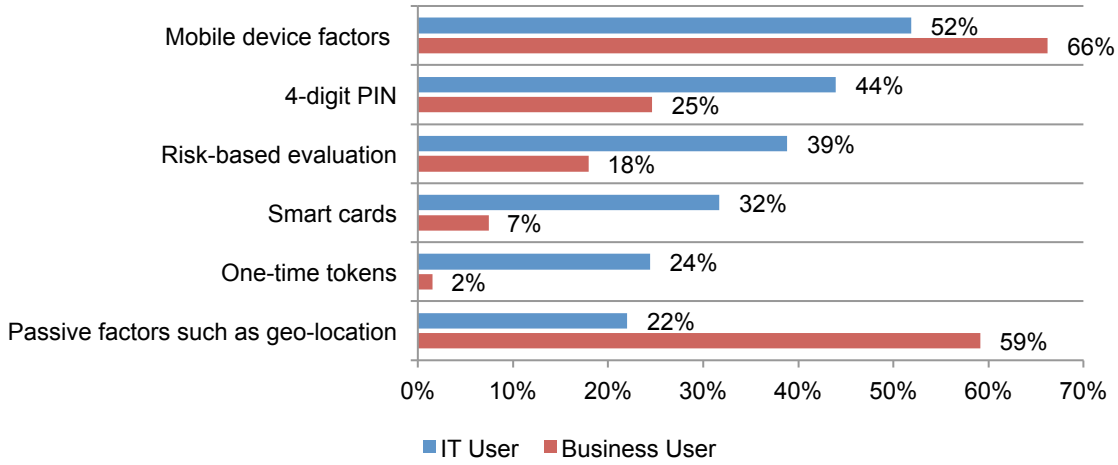


Figure 16 shows that to increase control or scrutiny, both the majority of IT users and business users would like to have mobile device factors added to the digital identity. IT users would also like 4-digit PINs and risk-based evaluations. Business users prefer to add passive factors such as geo-location tracking. This is consistent with the overall theme in this survey around simplifying the user experience as passive factors do not require minimal action by the end-user, yet can still reduce risk.

Figure 16. Factors to add to digital identity to increase control or scrutiny
More than one response permitted



Other data can increase the value of BYOID. Both groups identify other information that would be valuable to organizations accepting digital identities. According to Figure 17, having access to other data from the identity provider such as history of password resets and account abuse are of greatest interest as this data can help identify potentially fraudulent activity. Since frequent password resets attempts could be evidence of a compromised or hacked account, this data indicates that both business users and IT users agree that password reset data could be helpful for fraud detection purposes.

Figure 17. Useful digital identity characteristics known to the identity provider
More than one response permitted

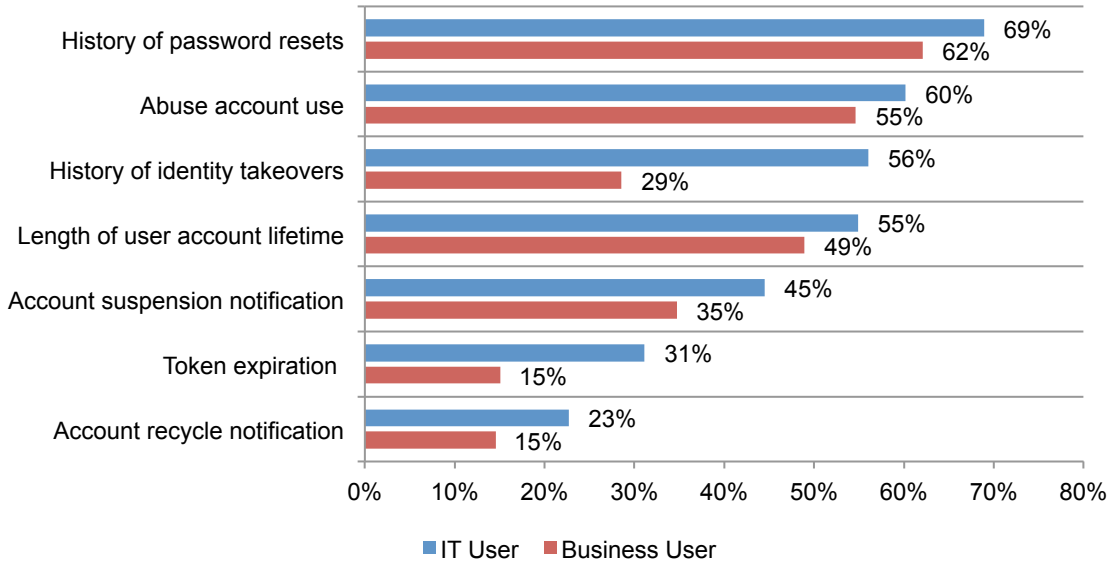
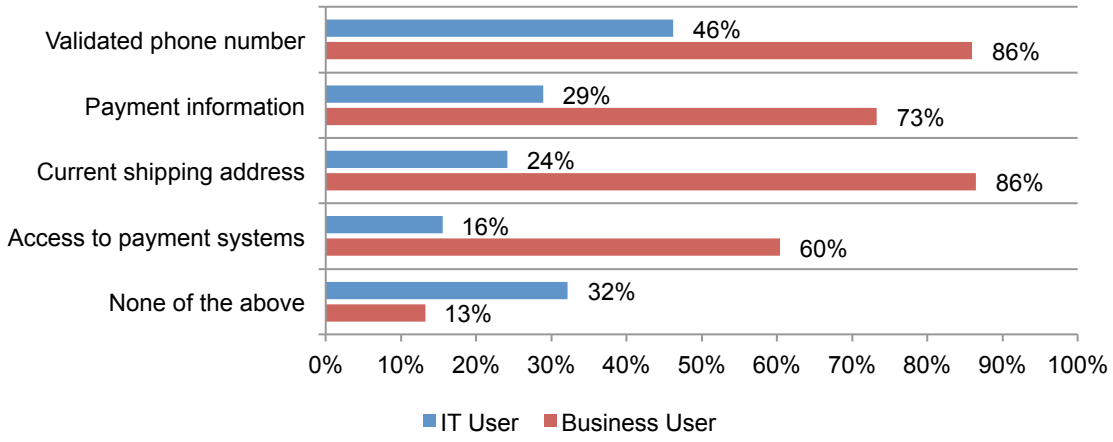


Figure 18 shows that when asked to identify what additional information or services would increase the value of a BYOID identity provider, IT users top choice is validated phone number (46 percent) whereas business users select current shipping address and validated phone number (both 86 percent). While this supplemental data can help with security, it can also help with personalization and marketing because phone numbers and shipping addresses can be used for other business benefits.

Figure 18. Information or services that increase the value of the BYOID provider
More than one response permitted



Part 3. Conclusion

In today's application economy, the old network perimeter is no longer relevant—today's IT organizations must deal with highly distributed identities across the entire business environment that come from many sources.

In addition, mobile employees and customers are redefining the challenge of delivering secure access to applications quickly. Users need to be able to access information anywhere, anytime, and from a range of different devices. These factors cause a dramatic shift in the role of security and how user identities should be managed. Previously, managing digital identities was traditionally viewed as a cost center. However, the rapid proliferation of web and mobile applications has transformed managing identities from a cost center to value center.

BYOID is a promising trend that offers simpler user engagement and acquisition without significant infrastructure or management costs. As the findings of this research reveal, the level of interest in BYOID indicates that this trend has traction among IT and the lines of business. This means that organizations should begin assessing how BYOID fits into their organization's long-term plans.

To achieve BYOID adoption, organizations should encourage greater cooperation and collaboration between IT users and business uers. The purpose should be to align the business goals in a manner that leverages BYOID without sacrificing security or increasing risk exposure to an unacceptable level. Consummating this IT and business collaboration around BYOID can help organizations successfully grow and meet new business initiatives.

In the short term, organizations should consider taking these three concrete steps to assess if and how BYOID would fit into the current organizational strategy:

1. **Engage IT and business in collaborative discussion around BYOID.** Your organization may already be utilizing BYOID for some specific initiatives, but to achieve maximum gain,

organizations should conduct an overall assessment of current and future business initiatives to determine potential fit for BYOID.

This exercise could include basic simulation/modeling of a new online initiative with BYOID and without BYOID. This will help address key questions: Will supporting BYOID increase new customer acquisition? Are the costs of continuing to require users to create and maintain their own accounts more than the incremental value that is generated from BYOID?

2. **Conduct BYOID risk assessment.** An important first step would be to convince a cross-functional team with business, legal and privacy expertise to understand the underlying risk and liability issues.

   This may require engaging with an outside firm or auditor. Given that online users could literally be from all over the world and subject to a wide range of privacy regulations, it is important to understand the risks involved so business can make best decision around BYOID. These discussions could include such questions, “Is accepting an identity from identity provider X acceptable?” and “What is minimum level of assurance we’d expect form identity provider X.”

3. **Monitor BYOID trends.** BYOID continues to be an active area with new developments both from vendors and public/private sectors. Some of these developments fall into enhancement of existing standards, and they also cover a lot of the business enablement and risk/liability issues that were covered in this report. Leveraging other industry work in BYOID can help enhance your own efforts and ensure that best practices are always being utilized.

Part 4. Methods

A sampling frame of 55,020 IT and IT security practitioners (IT users) and 56,518 business users located in the United States, Australia, Brazil, Canada, France, Germany, India, Italy and the United Kingdom were selected as participants to this survey. Table 1 shows 1,800 IT practitioners and 1,714 business users returned their survey responses. Screening and reliability checks required the removal of 399 surveys. Our final sample consisted of 1,589 IT practitioner surveys and 1,526 business user surveys.

Table 1. Survey response	IT User	Business User
Total sampling frame	55,020	56,518
Total returns	1,800	1,714
Rejected or screened surveys	211	188
Final sample	1,589	1,526
Response rate	2.9%	2.7%

Table 2 reports the respondent's organizational level of their current position within the organization. By design, 60 percent of IT respondents and 58 percent of user respondents are at or above the supervisory level.

Table 2. Current position within the organization	IT User	Business User
Senior executive/VP	6%	2%
Director	16%	14%
Manager	22%	27%
Supervisor	15%	16%
Staff/technician	36%	37%
Consultant/contractor	4%	5%
Total	100%	100%

As shown in Table 3, 74 percent of the IT respondents report directly to the CIO and 15 percent report to the CISO. Fifty-five percent of the User's report to the lines of business leaders and 10 percent report to the chief marketing officer.

Table 3. Primary person reported to within the organization	IT User	Business User
CEO/executive committee	3%	1%
Chief operating officer	1%	5%
Chief information officer	74%	7%
Chief information security officer	15%	0%
Chief marketing officer	1%	10%
Leader of product engineering	0%	6%
Leader of data analytics	0%	6%
Leader of sales	1%	8%
Leader of R&D	0%	2%
Lines of business leader(s)	5%	55%
Other	0%	1%
Total	100%	100%

Table 4 reports the industry classification of respondents' organizations. This table identifies financial services (18 percent) as the largest segment for both IT and user respondents. This is followed by retail for IT respondents (14 percent), and industrial, technology and software at 9 percent each for user respondents.

Table 4. Industry focus	IT User	Business User
Financial services	18%	18%
Retail	14%	6%
Services	13%	7%
Health & pharmaceuticals	8%	6%
Technology & software	8%	9%
Entertainment & media	6%	7%
Public sector	6%	8%
Hospitality	5%	6%
Consumer products	5%	6%
Transportation	4%	5%
Energy & utilities	3%	5%
Industrial	3%	9%
Communications	3%	6%
Education & research	3%	3%
Total	100%	100%

As shown in Table 5, all of the IT respondents and 97 percent of the user respondents are from organizations with a worldwide headcount of 1,000 or more employees.

Table 5. Worldwide headcount of the organization	IT User	Business User
Less than 1,000	0%	3%
1,001 to 5,000	43%	45%
5,001 to 25,000	33%	33%
25,001 to 75,000	17%	18%
More than 75,000	6%	2%
Total	100%	100%

Part 5. Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT or IT security practitioners and business users. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in June.

	Consolidated	
Survey response	IT User	Business User
Total sampling frame	55,020	56,518
Total returns	1,800	1,714
Rejected or screened surveys	211	188
Final sample	1,589	1,526
Response rate	2.9%	2.7%

Q1. What best describes your level of familiarity with the emerging trend in identity management termed "Bring Your Own Identity" or BYOID?	IT User	Business User
Very familiar	27%	27%
Familiar	34%	28%
Somewhat familiar	39%	45%
Not familiar or no knowledge (stop)	0%	0%
Total	100%	100%

Q2. What best describes your organization's level of interest in BYOID?	IT User	Business User
Very high	20%	23%
High	30%	40%
Moderate	35%	23%
Low	16%	14%
None (stop)	0%	0%
Total	100%	100%

Q3. What are the main reasons for BYOID adoption in your organization today? Please select all that apply.	IT User	Business User
To combine digital identifiers owned by each user with corporate factors to create a stronger identity credential	69%	65%
To create an identity credential that lasts beyond the user's employment or temporary employment	13%	11%
To outsource password reset activities to identity providers	48%	9%
To capture attributes about users from external sources	26%	95%
To get multi-factor authentication at a low cost	36%	10%
Other	1%	0%
Total	194%	185%

Q4. Who controls or "owns" digital identities in your organization?	IT User	Business User
IT	20%	16%
IT security	2%	5%
Lines of business	27%	28%
Marketing & sales	10%	18%
Data analytics	13%	24%
Research & development	0%	0%
No one owner, shared responsibility	28%	9%
Other	0%	0%
Total	100%	100%

Q5. How would you rate your organization's level of interest in accepting digital identities for any of the following user populations?		
Q5a. Recruiting job prospects	IT User	Business User
Very high	12%	12%
High	20%	25%
Moderate	34%	44%
Low	24%	12%
None	10%	6%
Total	100%	100%

Q5b. Employees	IT User	Business User
Very high	21%	14%
High	25%	22%
Moderate	30%	38%
Low	12%	15%
None	12%	11%
Total	100%	100%

Q5c. Contractors	IT User	Business User
Very high	20%	10%
High	23%	18%
Moderate	35%	49%
Low	13%	11%
None	9%	11%
Total	100%	100%

Q5d. Retirees	IT User	Business User
Very high	19%	14%
High	22%	22%
Moderate	30%	31%
Low	16%	18%
None	13%	15%
Total	100%	100%

Q5e. Website customers	IT User	Business User
Very high	22%	36%
High	28%	43%
Moderate	28%	9%
Low	14%	9%
None	8%	3%
Total	100%	100%

Q5f. Mobile customers	IT User	Business User
Very high	22%	41%
High	26%	41%
Moderate	28%	7%
Low	14%	8%
None	10%	4%
Total	100%	100%

Q6. Please rate the following statement using the scale provided below: *"My organization would be able to offer more online services and programs if those digital identities were validated by a trusted third party such as Google, Facebook, Yahoo, Microsoft or LinkedIn."*	IT User	Business User
Strongly agree	29%	15%
Agree	30%	19%
Unsure	22%	33%
Disagree	15%	26%
Strongly disagree	3%	8%
Total	100%	100%

Q7a. Is your organization using or considering the use of digital identities produced by trusted identity provides such as Google, Facebook, Yahoo, Microsoft or LinkedIn?	IT User	Business User
Yes	44%	30%
No	40%	45%
Unsure	16%	25%
Total	100%	100%

Q7b. If yes, what best describes your organization's timeframe for deployment?	IT User	Business User
Already deployed	16%	12%
Less than 6 months	18%	21%
6 to 12 months	17%	18%
12 to 24 months	19%	22%
More than 24 months	7%	5%
Never (no timeframe as yet)	23%	21%
Total	100%	100%

Q8. Please rank the following identity providers in order of interest to your **organization**. 1 = of most interested and 7 = of least interest. If possible, please avoid ties.	IT User	Business User
Google	2.42	5.54
LinkedIn	3.36	4.55
Yahoo	5.79	3.05
Microsoft Live	3.91	2.57
Facebook	5.76	6.30
Amazon	2.60	1.91
PayPal	1.87	2.63

Q9. Please rank the following identity providers in order of interest to you as an **individual** accessing other organizations or service providers. 1 = of most interested and 7 = of least interest. If possible, please avoid ties.	IT User	Business User
Google	1.82	2.22
LinkedIn	2.73	4.09
Yahoo	5.84	3.44
Microsoft Live	5.64	3.13
Facebook	3.50	2.04
Amazon	4.07	2.42
PayPal	2.59	2.97

Q10. How do the creation and/or use of digital identities **add value** to your organization? Please select all that apply.	IT User	Business User
Strengthens the authentication process	67%	38%
Reduces the cost of insecurity (impersonation risk)	54%	55%
Delivers a better customer experience	53%	79%
Increases the effectiveness of marketing activities	23%	76%
Increases employee/user productivity	37%	40%
Increases customer acquisition	21%	43%
Streamlines operations and logistics	49%	55%
Decreases customer turnover (churn)	25%	36%
Enhances innovations in products and services	21%	32%
Enables self-service processes	29%	18%
Generates new revenues	13%	21%
Other	1%	2%
Total	393%	496%

Q11a. Does your organization attempt to measure the added value resulting from the creation and/or use of digital identities?	IT User	Business User
Yes	27%	59%
No	62%	38%
Unsure	11%	3%
Total	100%	100%

Q11b. If Yes, how do you measure this added value? Please select all that apply.	IT User	Business User
Cost reduction	72%	78%
Risk and fraud reduction	56%	12%
Brand loyalty	0%	1%
Cross-selling/incremental revenue	14%	63%
Other	0%	8%
Total	143%	163%

Q12. In your opinion, how will the added value resulting from the creation and/or use of digital identities change over the next 24 months?	IT User	Business User
Increase	47%	59%
Stay the same	34%	26%
Decrease	4%	1%
Unsure	16%	14%
Total	100%	100%

Q13. In your opinion, how will the total cost incurred by your organization to create, use and maintain digital identities change over the next 24 months?	IT User	Business User
Increase	33%	49%
Stay the same	48%	28%
Decrease	3%	2%
Unsure	16%	21%
Total	100%	100%

Q14. Which of the following features would most likely increase BYOID adoption within your organization? Please select all that apply.	IT User	Business User
Multi-factor authentication	66%	33%
Identity validation processes	73%	71%
Identity provider implementing fraud risk engines	57%	37%
Simplified user registration	56%	71%
SMS mechanisms for user validation	37%	27%
Simplified password or account recovery	30%	30%
Risk based evaluation of account recovery processes and user identity	20%	11%
Total	338%	280%

Q15. What factors would you add to a digital identity to increase control or scrutiny by your organization?	IT User	Business User
4-digit PIN	44%	25%
Passive factors such as geo-location	22%	59%
One-time tokens	24%	2%
Smart cards	32%	7%
Mobile device factors	52%	66%
Risk-based evaluation	39%	18%
Total	213%	177%

Q16. As a BYOID relying party, what characteristics about digital identity known to the identity provider would be useful?	IT User	Business User
History of password resets	69%	62%
History of identity takeovers	56%	29%
Abuse account use	60%	55%
Account suspension notification	45%	35%
Account recycle notification	23%	15%
Token expiration	31%	15%
Length of user account lifetime	55%	49%
Total	338%	259%

Q17. What additional information or services would increase the value of the BYOID identity provider? Please select all that apply.	IT User	Business User
Current shipping address	24%	86%
Validated phone number	46%	86%
Payment information	29%	73%
Access to payment systems	16%	60%
None of the above	32%	13%
Total	147%	319%

Q18. Which BYOID benefits are of most interest to your organization? Please select all that apply.	IT User	Business User
Targeted marketing	11%	43%
Fraud / risk evaluation & reduction	55%	21%
Identity validation	74%	63%
Employee on-boarding	58%	25%
Contractor on-boarding	57%	25%
Reduced friction in user experience	49%	78%
Simplified engagement for users	48%	75%
Increased revenue	14%	56%
Security enhancements	45%	5%
Access to fresh identity information	46%	62%
Other	1%	1%
Total	455%	456%

Q19. How important is formal accreditation of the BYOID identity provider?	IT User	Business User
Essential	29%	12%
Very important	30%	15%
Important	21%	48%
Not important	15%	22%
Irrelevant	5%	3%
Total	100%	100%

Q20. What is the minimum level of assurance you would be willing to accept from a BYOID identity provider?	IT User	Business User
None (no assurance necessary)	21%	41%
Single factor remote authentication using a wide range of available authentication technologies	30%	38%
Provides multi-factor remote authentication using soft cryptographic tokens, hard cryptographic tokens, and/or one-time password tokens	26%	13%
Provides multi-factor remote authentication only using hard cryptographic tokens	22%	8%
Total	100%	100%

Q21. What use case would you choose to demonstrate the benefits of BYOID within your organization?	IT User	Business User
Streamline online user registration process for new customer acquisition	30%	49%
Accepting social identities to access additional attributes that drive targeted marketing promotions.	12%	29%
On-boarding of contractors	17%	4%
On-boarding of employees	20%	11%
Support for specific mobile initiatives	21%	8%
Total	100%	100%

Q22. In your opinion, what is the most significant inhibitor to BYOID deployment?	IT User	Business User
Cost	14%	31%
Complexity	21%	23%
Lack of a compelling business case	12%	18%
Risk & liability concerns	34%	19%
Loss of control	19%	8%
Other	0%	1%
Total	100%	99%

Q23. What is your preferred payment method for BYOID services?	IT User	Business User
Flat fee per user	21%	44%
Fee per transaction	26%	17%
Single annual fee regardless of user size	53%	37%
Other	0%	2%
Total	100%	100%

Your role and organization

D1. What organizational level best describes your current position?	IT User	Business User
Senior executive/VP	6%	2%
Director	16%	14%
Manager	22%	27%
Supervisor	15%	16%
Staff/technician	36%	37%
Consultant/contractor	4%	5%
Total	100%	100%

D2. Check the **Primary Person** you or your leader reports to within the organization.	IT User	Business User
CEO/executive committee	3%	1%
Chief operating officer	1%	5%
Chief information officer	74%	7%
Chief information security officer	15%	0%
Chief marketing officer	1%	10%
Leader of product engineering	0%	6%
Leader of data analytics	0%	6%
Leader of sales	1%	8%
Leader of R&D	0%	2%
Lines of business leader(s)	5%	55%
Other	0%	1%
Total	100%	100%

D3. What industry best describes your organization's industry focus?	IT User	Business User
Financial services	18%	18%
Retail	14%	6%
Services	13%	7%
Health & pharmaceuticals	8%	6%
Technology & software	8%	9%
Entertainment & media	6%	7%
Public sector	6%	8%
Hospitality	5%	6%
Consumer products	5%	6%
Transportation	4%	5%
Energy & utilities	3%	5%
Industrial	3%	9%
Communications	3%	6%
Education & research	3%	3%
Total	100%	100%

D5. What is the worldwide headcount of your organization?	IT User	Business User
Less than 1,000	0%	3%
1,001 to 5,000	43%	45%
5,001 to 25,000	33%	33%
25,001 to 75,000	17%	18%
More than 75,000	6%	2%
Total	100%	100%

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.