2018 Digital Identity Trust Survey

How do you establish and maintain identity trust across all channels?

Tom Field
Senior Vice President, Editorial

2018 Digital Identity Trust Survey

Ninety-six percent of polled security leaders say that a frictionless digital customer experience is a priority for their organizations. And yet:

- 36 percent still rely on usernames and passwords to authenticate digital customers;
- 23 percent know that in the past year their organizations have suffered at least one cybersecurity incident as a result of unauthorized access to these accounts (17 percent are unsure).

These are but some of the findings of the 2018 Digital Identity Trust Survey, which explores the question: How can organizations establish true digital trust with their digital customers?

Roughly 150 security leaders participated in this survey, which was conducted to determine:

- To what degree are organizations currently establishing digital identity trust with new customers?
- What methods and tools are organizations using to validate the digital identity authenticity?
- •What investments are organizations making in emerging technologies, such as artificial intelligence, machine learning and blockchain, to improve their ability to establish and maintain digital identity trust for new and existing customers?

Ninety-six percent of respondents expect the same or increased budget for securing digital trust in the year ahead. Their top investment targets are to invest in new tools to improve security of user authentication and account access, as well as to create a frictionless customer experience. How will they meet these objectives? That is the key question to be answered in this report.

Read on for full survey results, as well as expert analysis of how to put this information to use to improve your organization's ability to ensure digital identity trust.

Best,

Tom Field
Senior *Vice President, Editorial*
Information Security Media Group
tfield@ismg.io

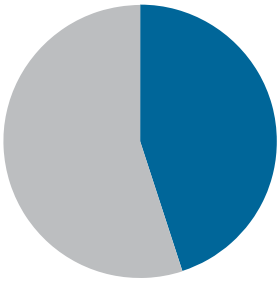
This survey, conducted online in the summer of 2018, generated nearly 150 responses from organizations of all sizes, primarily in the U.S. Specific vertical sectors surveyed include government, healthcare and retail. In general, the responses from each sector were aligned with one another. Where they vary significantly, the unique responses will be highlighted

About IBM Security:

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 60 billion security events per day in more than 130 countries and has been granted more than 8,000 security patents worldwide. For more information, please check www.ibm.com/security.

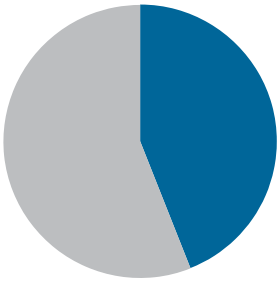
By the Numbers

Some statistics that jump out from this study:



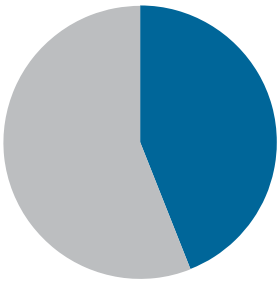
45%

of security leaders say their organization currently has a fair balance between cybersecurity and a frictionless digital customer experience.



44%

say their customers believe the organization's current digital enrollment process is too cumbersome or complex.



44%

say the single biggest driver to improve security within their digital channel is the increase in the number and sophistication of fraudsters.

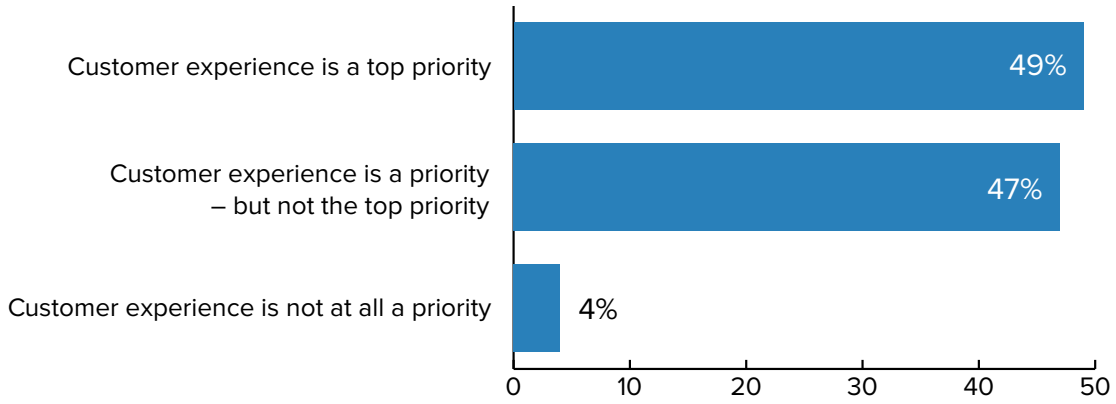
Baseline Questions

In this opening section, the report looks at the fundamentals of digital identity trust, including the balance between cybersecurity and a frictionless customer experience. Among the findings:

- 49 percent say that customer experience is their top priority;
- 40 percent say they have or may have in the past year suffered at least one cybersecurity incident as a result of unauthorized access to the customer digital application;
- 45 percent of those breached say they subsequently suffered direct losses because of fraud or indirect losses as a result of prospective customers abandoning the application because of the authentication process.

Read on for full results.

When it comes to cybersecurity, what value does your organization place on offering a frictionless, digital customer experience?

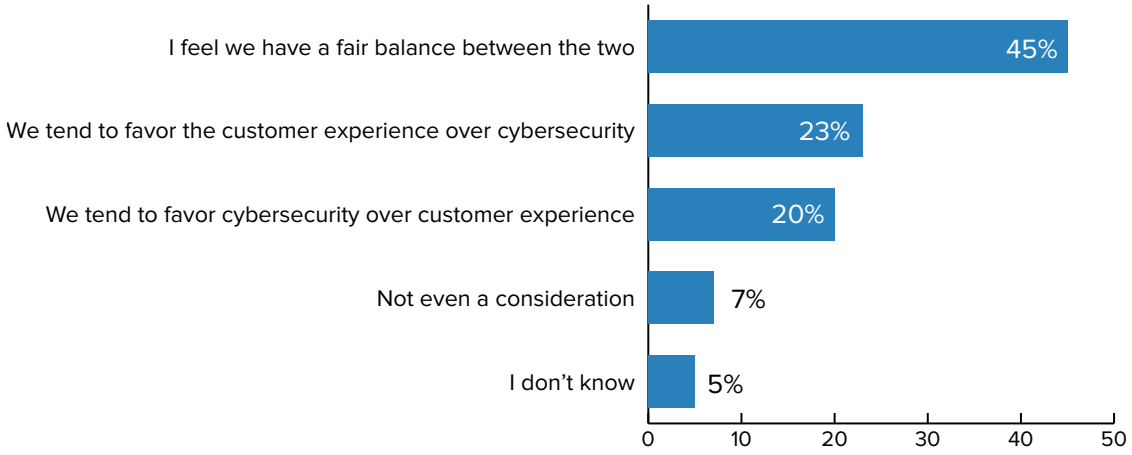


How much of a priority is the goal of enabling a frictionless, digital customer experience? For 49 percent of respondents it's a top priority. For nearly as many – 47 percent – it is a priority, but not the priority.

Only 4 percent of respondents say the customer experience is not a priority at all.

How much of a priority is the goal of enabling a frictionless, digital customer experience? For 49 percent of respondents it's a top priority.

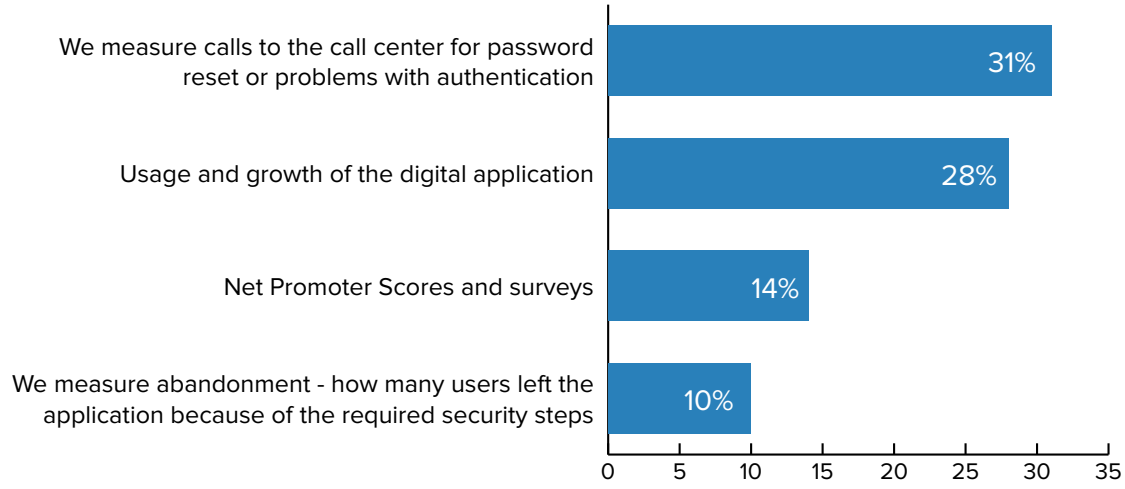
Currently, how would you say your organization balances cybersecurity with the digital customer experience?



Since the advent of the digital channel, organizations have struggled with providing the right mix of cybersecurity controls to protect identities and accounts without negatively impacting the customer experience.

Asked how their organizations currently strike that balance, 23 percent say they tend to favor the customer experience, while 20 percent come down on the side of cybersecurity. Forty-five percent feel they have a fair balance between the two.

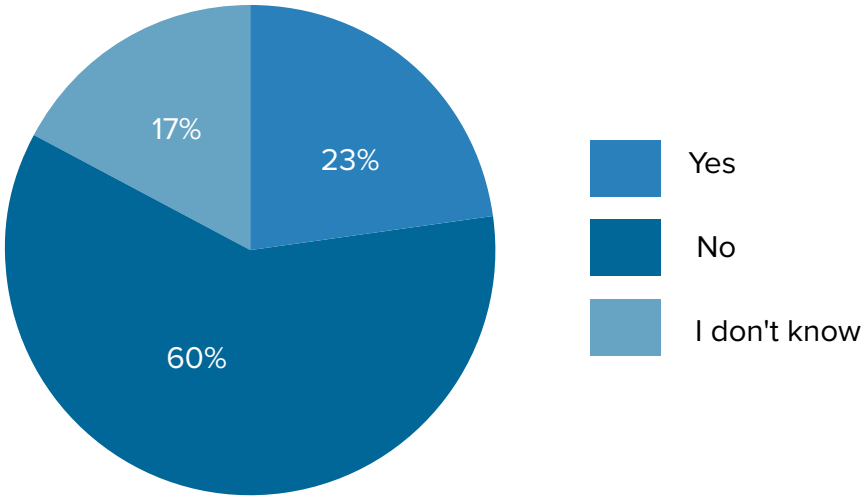
How does your organization measure customer satisfaction from the security of the digital customer experience? (Choose all that apply)



Measuring customer satisfaction with the security of the digital experience is a dawning practice for many enterprises. Currently, 31 percent do so by measuring the volume of calls to the call center for password resets or problems with authentication.

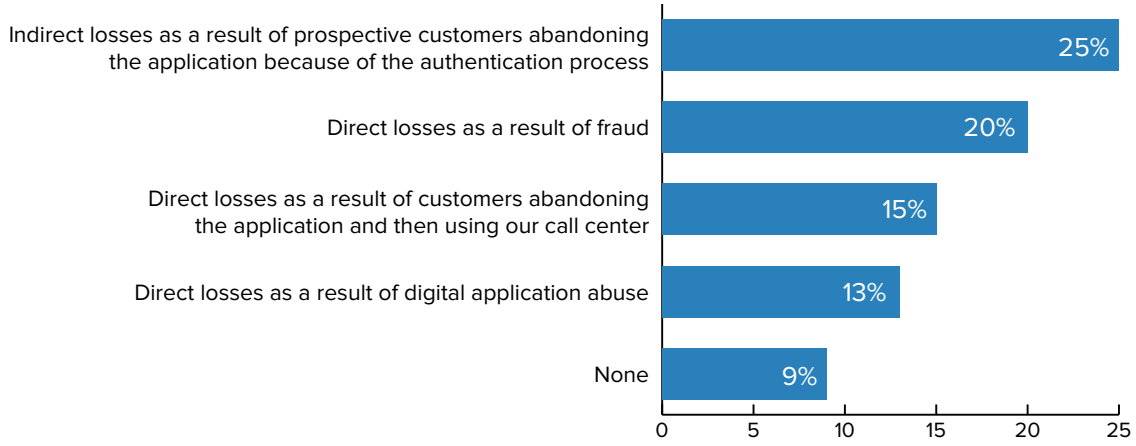
Twenty-eight percent measure satisfaction via usage and growth of the digital application.

Has your organization in the past year suffered at least one cybersecurity incident, as a result of unauthorized access to the customer digital application, that resulted in the compromise of customer accounts?



Asked whether their organizations have suffered at least one recent incident as a result of unauthorized access to the customer digital application – and resulting in compromised accounts – 60 percent of respondents say no. But nearly one-quarter of respondents – 23 percent –say yes, and another 17 percent do not know. This suggests the total number of organizations with breaches could be significantly higher than 23 percent.

What direct and indirect financial losses has your organization absorbed as a result of unauthorized access to customer digital accounts? (Choose all that apply)

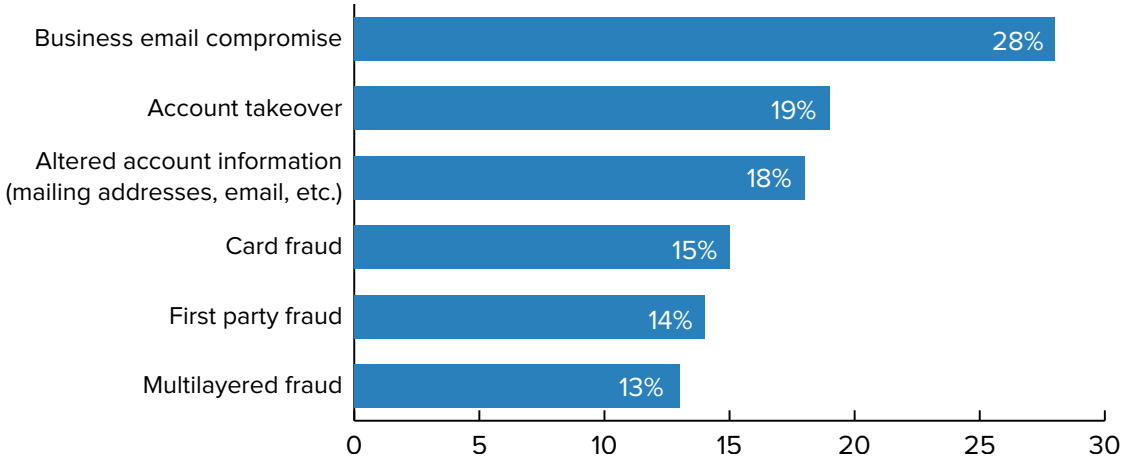


As for the impact of such cybersecurity incidents, it can be broken down into direct and indirect losses.

Directly, 48 percent of organizations have seen losses as a result of fraud, digital application abuse and customers abandoning the application and then using the call center.

Indirectly, 25 percent report customers abandoning the application altogether because of the authentication process.

What type(s) of business impacts have been felt as a result of unauthorized access to customer digital accounts? (Choose all that apply)



Poking further into fraud, the survey finds that 28 percent of respondents whose organizations have been breached report incidents of business email compromise as a result of unauthorized access to customer digital accounts.

Further, 19 percent report incidents of account takeover, while 18 percent say they have detected altered account information, i.e. changed mailing addresses or contact information.

In the next section, the report looks at what organizations do to establish digital identity trust.

28 percent of respondents whose organizations have been breached report incidents of business email compromise as a result of unauthorized access to customer digital accounts.

Establishing Digital identity Trust

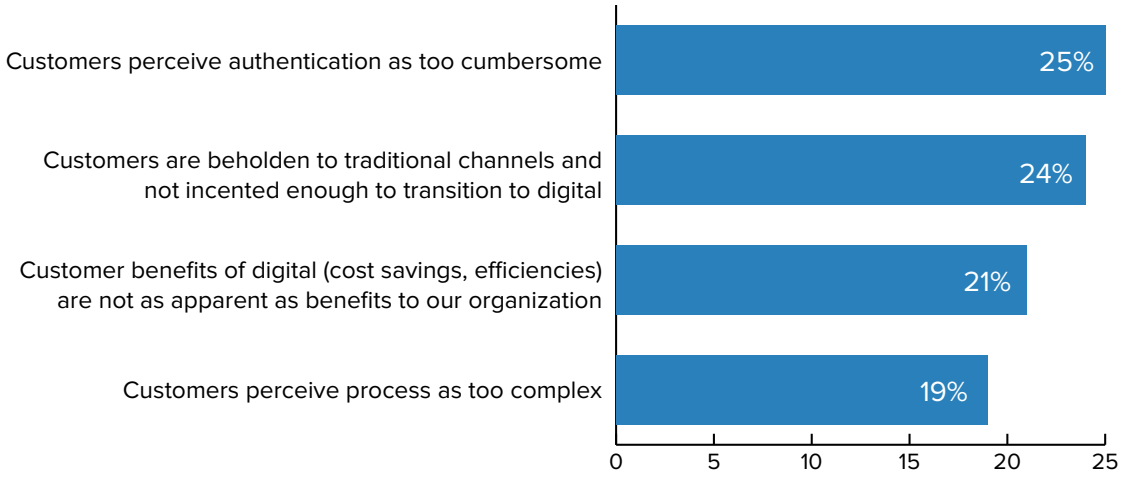
This portion of the report looks at two main questions: What are organizations doing now to establish digital identity trust? And what do they hope to do differently in the immediate future?

Some statistics of note:

- 37 percent of respondents still authenticate digital customers by username and password alone;
- 44 percent do not measure the success of their authentication methods.

Delve further and you will see the challenges organizations are attempting to overcome to both enroll new customers and serve their existing ones digitally.

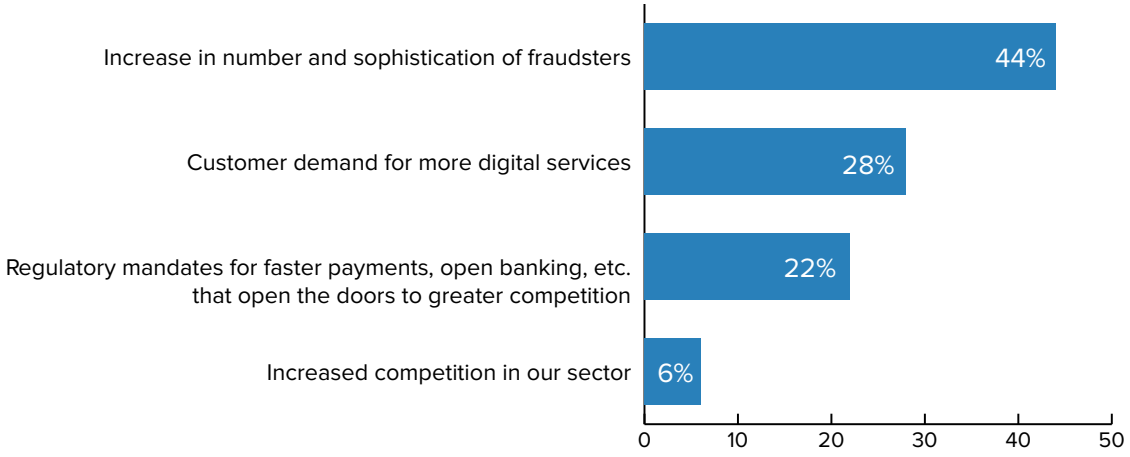
What is the main pain point in your organization's digital enrollment process today?



Here is the crux of the problem for organizations seeking that balance between cybersecurity and a frictionless customer experience: 43 percent of customers find the digital enrollment process to be too complex or the authentication process is too cumbersome.

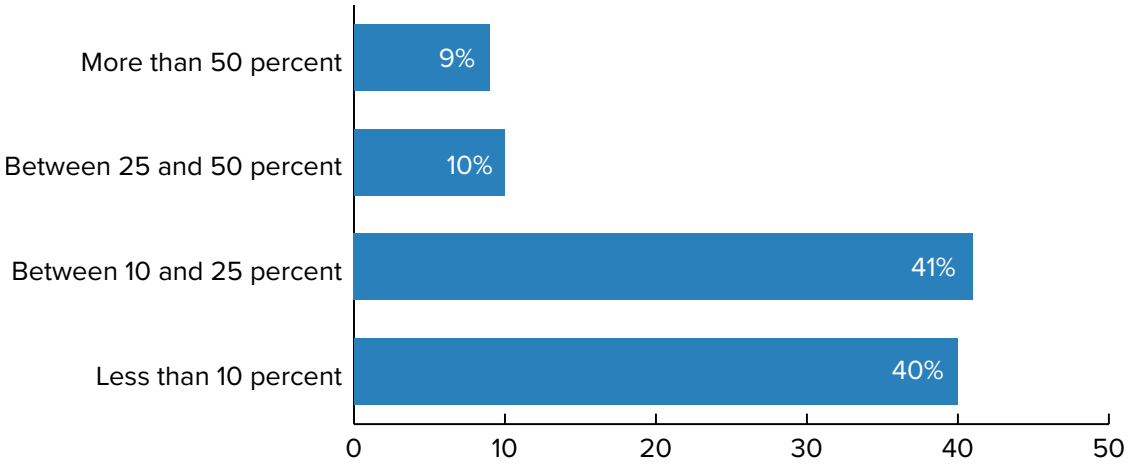
43 percent of customers find the digital enrollment process to be too complex, or else the authentication is too cumbersome.

Which one factor is the biggest driver behind your organization's desire to improve security within its digital channel?



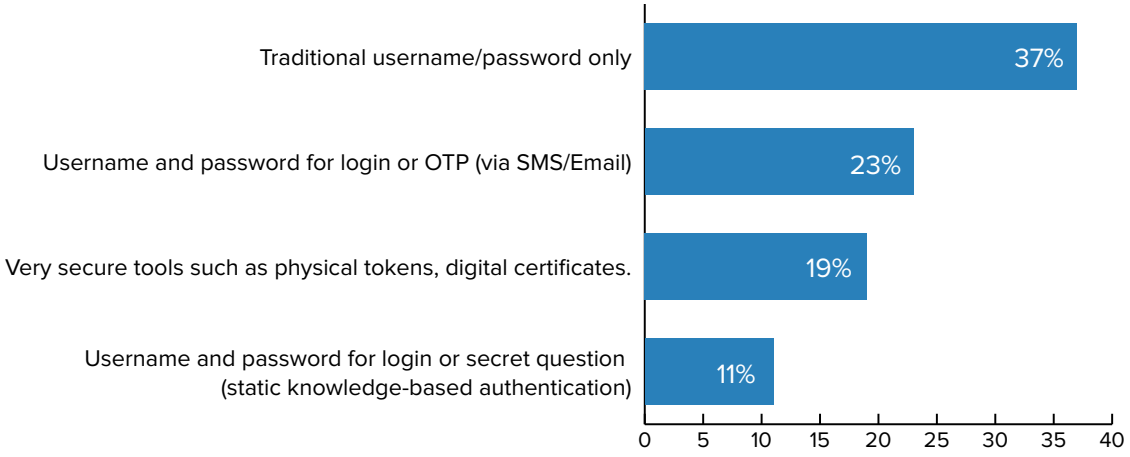
Customer concerns aside, organizations are still driven to improve security within the digital channel for two primary reasons: the increase in the number and sophistication of fraudsters (cited by 44 percent) and customer demand for more digital services (28 percent).

In the coming year, how much of your organization's growth is expected to come as a result of your digital strategy?



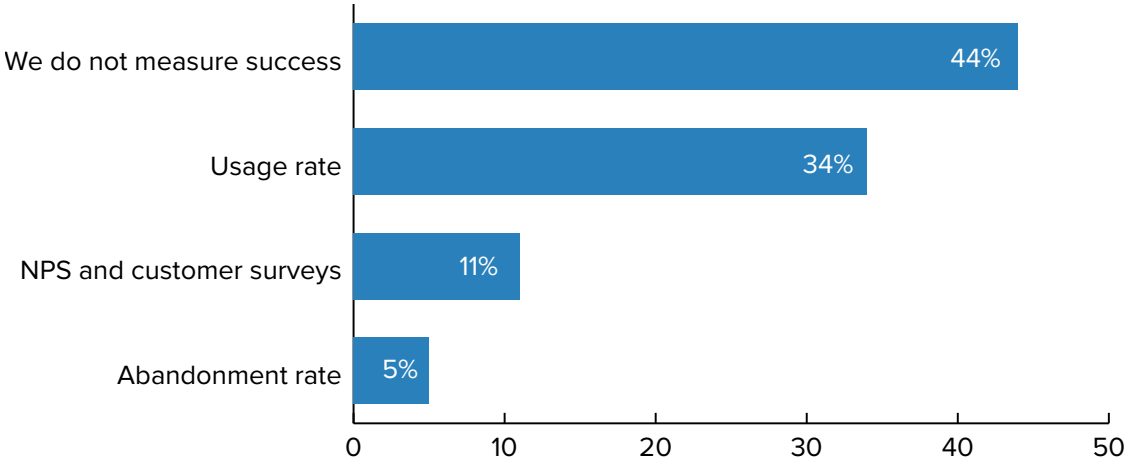
Looking ahead, 60 percent of respondents say that 10 percent or more of their organization's growth is expected to come as a result of their digital strategy, which means it's time to focus on issues such as enrollment, authentication and friction.

How does your organization currently authenticate digital customers? (Choose all that apply)



As a benchmark, more than one-third of respondent organizations still use usernames and passwords to authenticate digital customers. Nearly one-quarter combine username/password with one-time password via SMS or email.

How does your organization currently measure the success of these authentication methods?

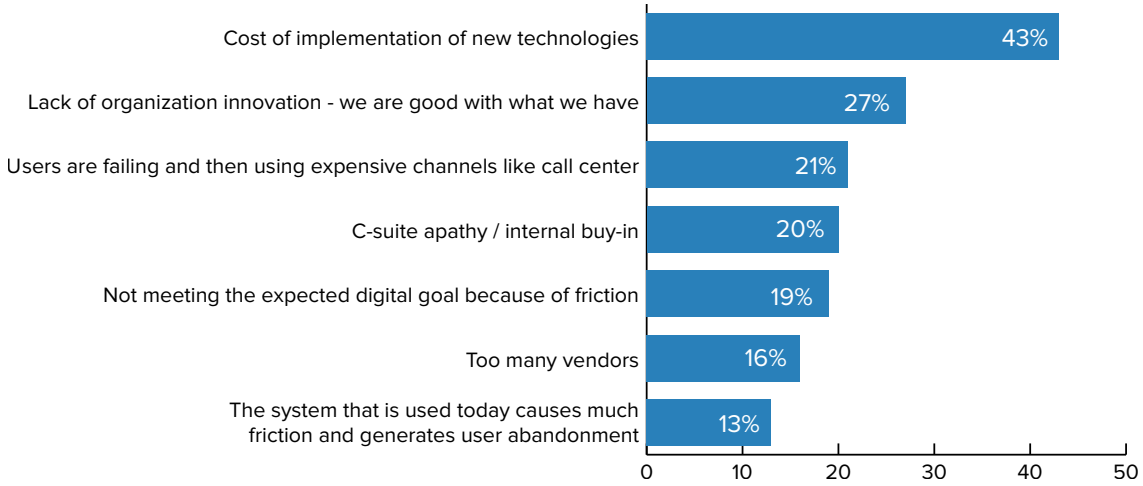


Forty-four percent of respondents do not measure the success of their current authentication methods. But 34 percent track the usage rate.

When examining retail respondents solely, the results vary significantly:

- 50 percent measure success via usage rate;
- Only 25 percent say they do not measure success at all.

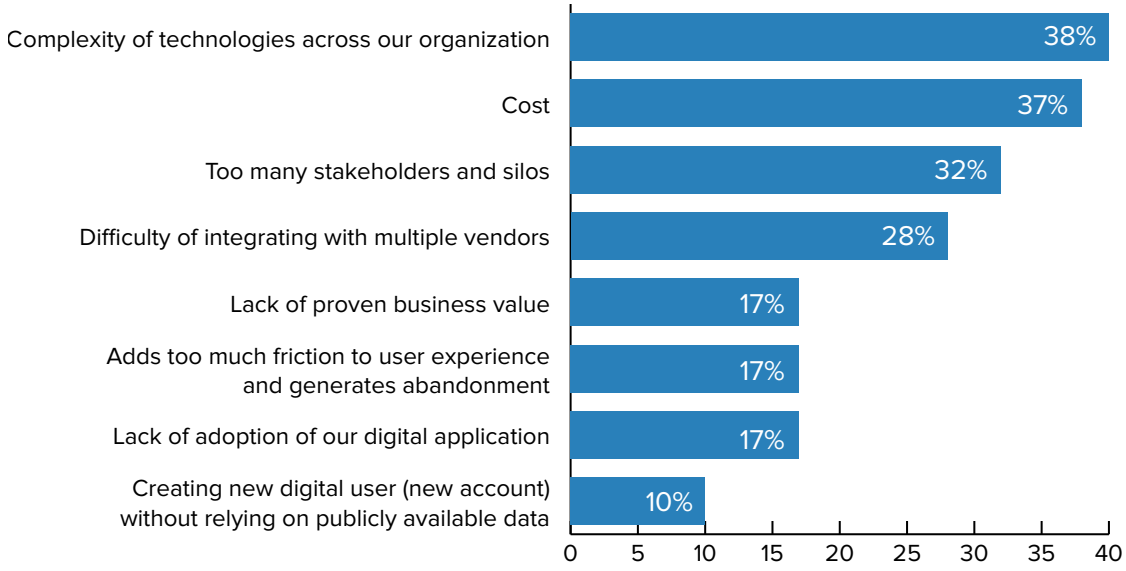
What are your organization's greatest challenges to establishing digital trust today for new customers enrolling, opening an account, etc.? (Choose all the apply)



The three main barriers to establishing digital trust for new customers:

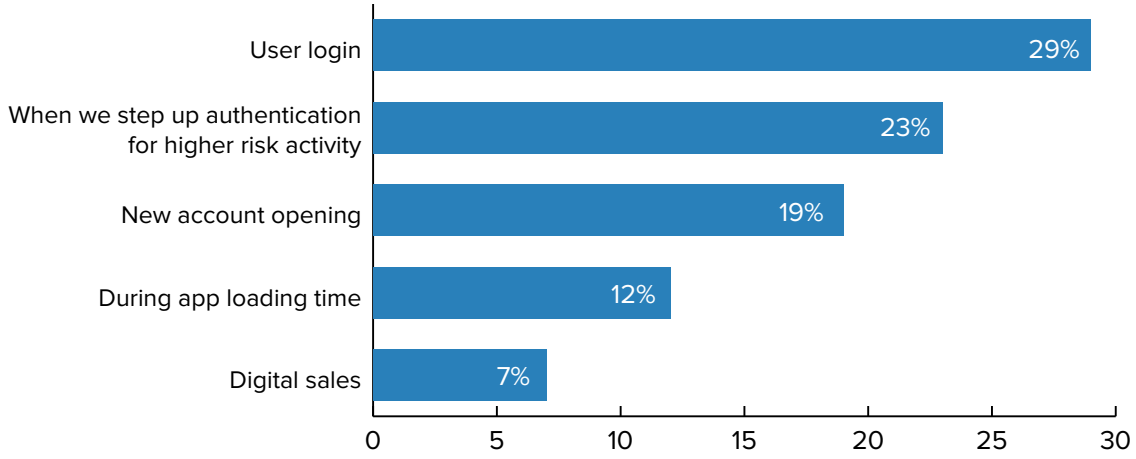
- Cost of implementing new technologies – 43 percent;
- Lack of organization innovation – 27 percent;
- Users fail and then turn to other channels – 21 percent.

What are your greatest challenges to ensuring digital trust today for registered customers? (Choose all that apply)



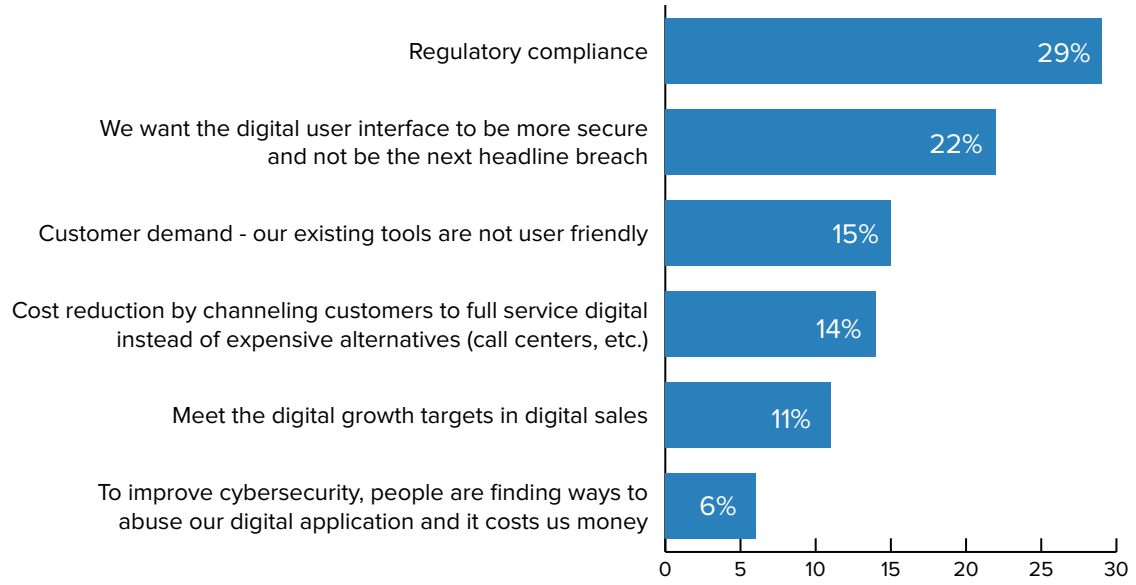
For registered customers, 38 percent of respondents say their greatest challenge in ensuring digital trust is the complexity of technologies across the organization, while 37 percent cite cost.

For new or existing customers, where do you currently see your greatest digital application abandonment rates?



A key metric to watch is abandonment rate. Twenty-nine percent see their greatest digital application abandonment at the user login stage. For 23 percent, it's when they step up the authentication process for higher risk activity.

What is your single biggest driver to improve the practice of digital trust across your enterprise? (Choose all that apply)



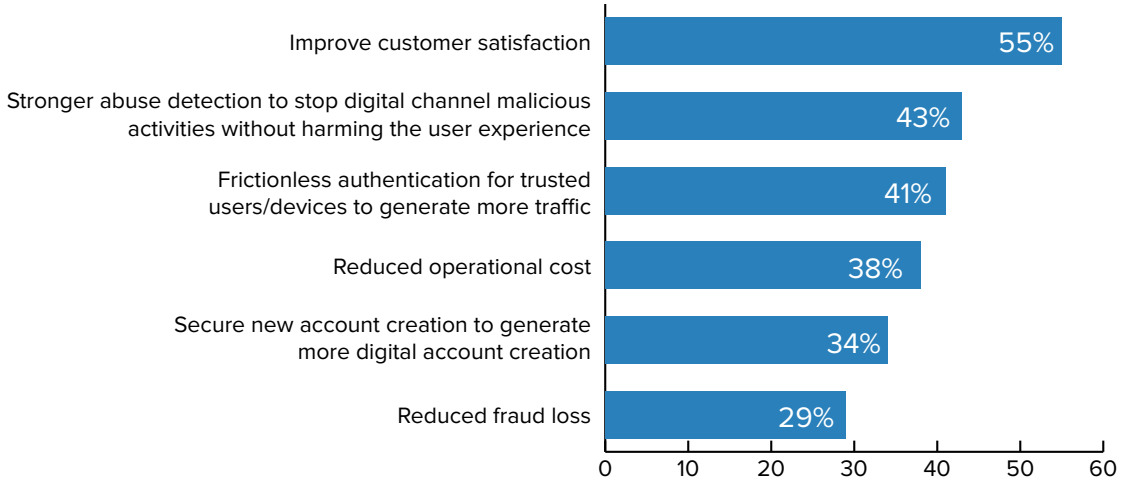
In the wake of Europe's PSD2 and GDPR initiatives, organizations are increasingly sensitive to secure digital experiences, and so it comes as no surprise that 29 percent of respondents cite "regulatory compliance" as their single biggest driver to improve digital trust across the enterprise.

For 22 percent, the motivation is solely for the digital interface to be more secure – and not responsible for the next big breach headline in the news.

Here again, the retail sector has a slightly different view. Its top drivers:

- 35 percent want the digital interface to be more secure and not be the next breach headline;
- Only 10 percent cite regulatory compliance as a driver.

What outcome do you expect by investing further in establishing/ensuring digital trust? (Choose all the apply)



And by improving digital trust, 55 percent of respondents hope to likewise improve customer satisfaction, while 43 percent aim to stop malicious activities on the digital channel without harming the digital experience.

With these objectives in mind, look to the next section, which shows where organizations will invest in digital trust in 2019.

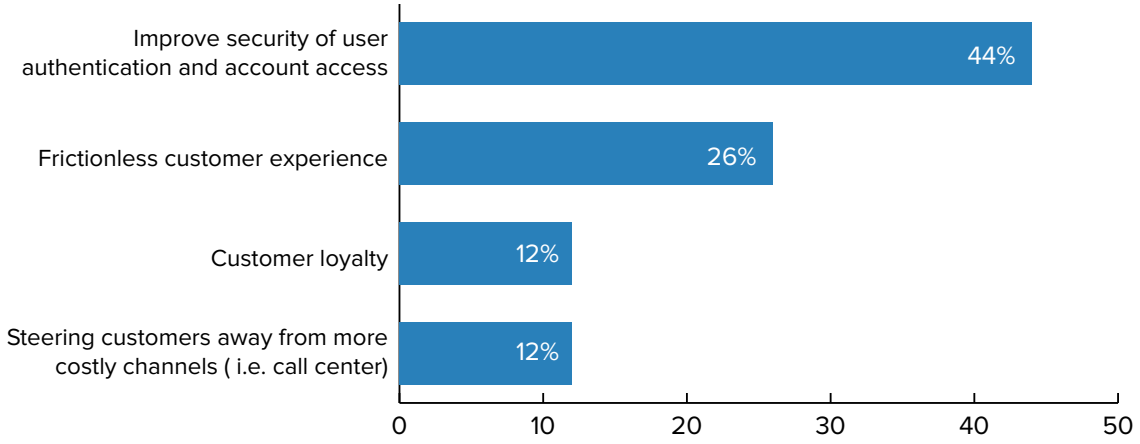
And by improving digital trust, 55 percent of respondents hope to likewise improve customer satisfaction.

Investing in Digital Trust

Two significant numbers to bear in mind when reviewing this section:

- 96 percent of respondents expect the same or increased funding for digital trust initiatives in the year ahead;
- 52 percent intend to invest those funds in new authentication methods.

As you plan for 2019, what is your single biggest goal for investing in new digital trust technologies?



Asked what their single biggest goal is when planning 2019 investments in digital trust technologies, 44 percent of respondents cite improving security of user authentication and account access.

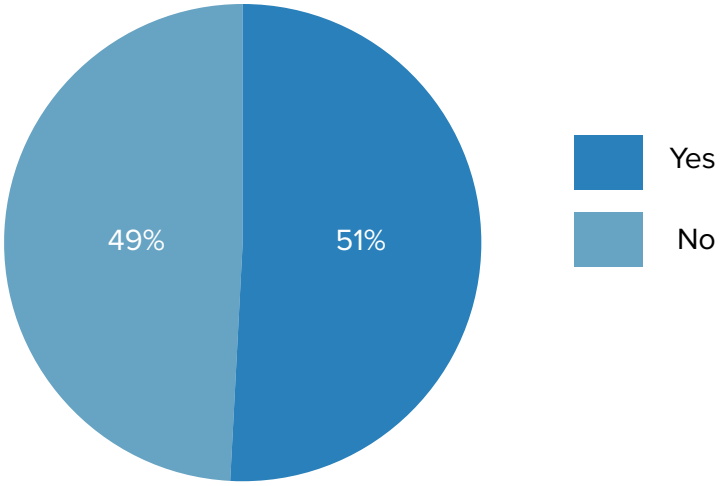
For 26 percent, the goal is the frictionless customer experience.

Retail again has a unique view:

- 35 percent want that frictionless customer experience;
- 30 percent favor customer loyalty;
- 30 percent want to improve the security of user authentication and account access.

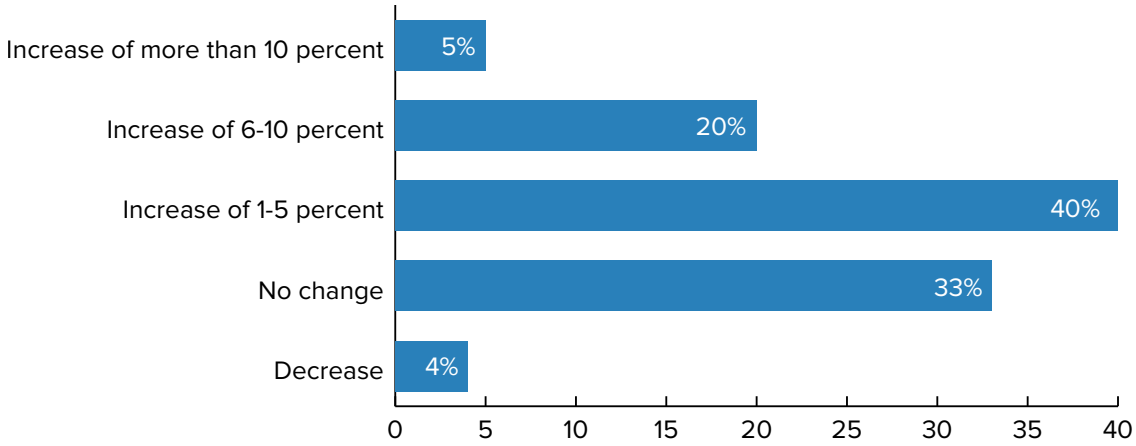
Asked what their single biggest goal is when planning 2019 investments in digital trust technologies, 44 percent of respondents cite improving security of user authentication and account access.

Has your organization budgeted specifically for improving digital trust for 2019 – to make digital a preferred, secure channel and to keep customers from falling back on other, more expensive channels (i.e. call center)?



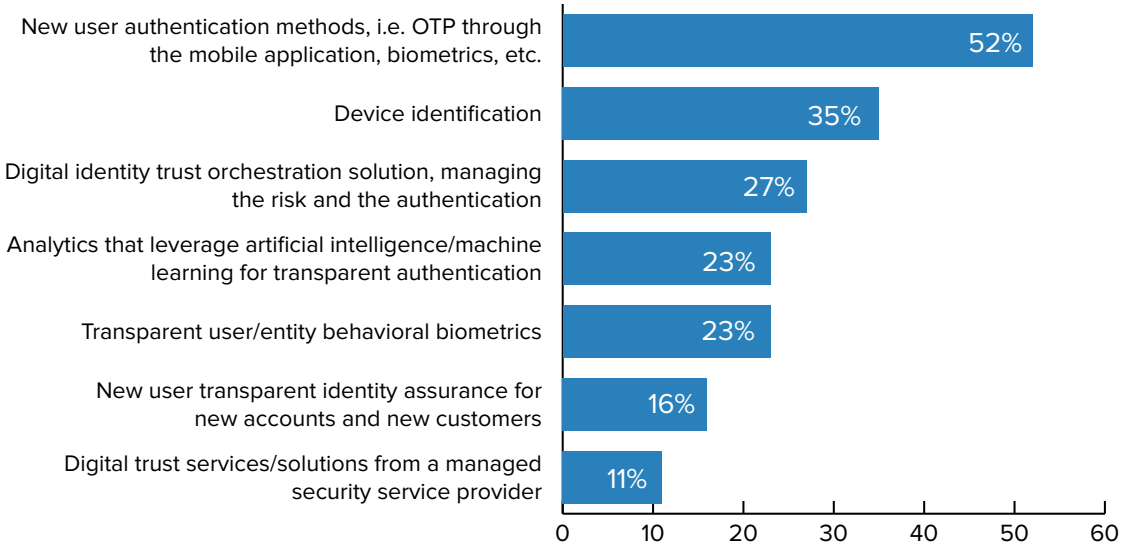
Just over half of organizations have a budget specifically allocated for digital trust initiatives.

How do you expect your budget dedicated to digital trust to change in 2019?



Forty percent of respondents expect an increase of 1 percent to 5 percent in their budget dedicated to digital trust, while 20 percent say the budget will grow by 6 percent to 10 percent.

Which specific technology investments will you make in 2019 to improve digital trust for your organization's customers? (Choose all the apply)



The top three targets of these new funds:

- New user authentication methods, i.e. OTP through the mobile app, biometrics, etc.;
- Device identification;
- A digital trust orchestration solution.

With these responses in mind, look now at the overarching conclusions about this survey, as well as expert analysis on how to put these results to use in your organization.

Conclusions

In concluding this survey report, it is helpful to look back at the introduction, where three key statistics were shared:

- 96 percent of polled security leaders say that a frictionless digital customer experience is a priority for their organizations;
- 37 percent still rely on usernames and passwords to authenticate digital customers;
- 23 percent know that in the past year their organization has suffered at least one cybersecurity incident as a result of unauthorized access to these accounts (17 percent are unsure).

In light of these statements, analysis of the entire survey response leads to three conclusions about the future of digital identity trust:

It's About the Customer

Yes, the customer wants a frictionless experience, and they don't have patience for a cumbersome authentication process. But they also want to know that their credentials and accounts are safe.

Customers may abandon digital applications if the enrollment or authentication process seem complex – but they may abandon faster if there is a high-profile breach or if their own credentials are compromised. As the survey shows, customers are demanding new digital services, and enterprise growth is going to come in large part from this digital channel. Organizations need to invest in new tools and technologies that can balance security with the all-important customer experience.

It's About Security

Organizations have legacy investments in usernames and passwords and other conventional forms of authentication, but the fraudsters have proven more than adept at circumventing these controls to compromise credentials and accounts. The future of digital identity trust is in multifactor authentication and in technologies such as artificial intelligence and machine learning, as well as device identification and behavioral biometrics, which can help benchmark typical customer behavior – and help better detect anomalous activity.

Technology investment need not mean greater complexity. Smart investments, in fact, can make the entire process far easier for the customer – and more secure for the enterprise.

It's About the Future

"Digital transformation" is one of today's most popular buzz terms. Enterprises globally are moving their critical business applications to the cloud and expanding their digital channels for customers and partners alike. Fraudsters likewise are following this migration, taking advantage of lax security and a wealth of PII available to them from prior breaches.

It's worth noting: 44 percent of survey respondents say the single biggest driver to improve security within their digital channel is the increase in the number and sophistication of fraudsters. Pressure is going to increase in 2019 both to expand the digital channel and to secure it.

Organizations in the government, healthcare and retail sectors should learn from the financial services example. Digital is no longer an add-on option; it's a necessity for enterprises that want to thrive and serve their customers evolving needs. Cybersecurity and the frictionless customer experience need not be mutually exclusive. The progressive enterprise can – and should - have both.

In the final section of this report, Christine DeFazio of survey sponsor IBM Security analyzes the results and discusses how best to put them to work in the year ahead.

2018 Digital Identity Trust Survey

How to Put These Research Results to Work and Affect Change

NOTE: In preparing this report, ISMG's Tom Field sat down with Christine DeFazio of survey sponsor IBM Security to discuss the survey findings and how organizations can best put them to use to improve digital trust and security. This is an excerpt of that conversation.

Initial Reaction

TOM FIELD: We got together months ago to talk about what we thought respondents were going to say in this survey. So my first question for you is: What's your gut reaction – what stood out to you from the responses, and what surprised you?

CHRISTINE DEFAZIO: What I found really interesting was the disconnect between what organizations think they're providing in terms of security and customer experience and what customers' actions are actually telling us. Organizations are trying to ease this burden of security with authentication methods like one-time passwords, but customers are not seeing the benefits. And the worst part is they are still really frustrated. An interesting stat was that 48 percent are abandoning at login or new account creations. It's great to see investments are being made with regards to establishing digital identity trust. But current practices are failing and resulting in significant financial loss – and it's not just from fraud. And at the same time, these outdated or inefficient authentication methods are actually enabling malicious actors, making it easier for them to commit crimes. It's a double whammy of bad news all around. No one here is winning except for the fraudsters, which is not ideal.

Why Usernames and Passwords?

FIELD: Security pundits have said the password is dead, and yet we find so many organizations remain dependent on simple usernames and passwords. Why it there still this dependency even though we know better?

DEFAZIO: This is mostly due to the fact that it's what everyone was once considering a best practice. It's what customers expect; it's that painful, inconvenient account access process.

Many organizations are transitioning between a focus on stopping fraud at any cost to a focus on the need to build digital identity trust, allowing customer experience to drive the digital transformation, rather than security concerns. Organizations are just now starting to change their ways of thinking. They are just catching up to the idea that these usernames and passwords are outdated and truthfully difficult for their users to have to deal with.

Christine DeFazio

"Organizations are trying to ease this burden of security with authentication methods like one-time passwords, but customers aren't seeing the benefits."

Biggest Barriers to Digital Trust

FIELD: In your experience, what are the biggest barriers that prevent organizations from strengthening authentication for their digital channels?

DEFAZIO: There are a few reasons organizations have not made the switch to more advanced security measures. One of those is fear of a cumbersome customer experience. There is the lack of knowledge around what other transparent options are available. And then there is the amount of overall financial loss that's actually happening within the organization. Then, of course,

there are worries about the cost of any changes and barriers with stakeholder buy-in.

We are seeing this apparent lack of awareness of the severity of what is happening throughout the customer journey. I do not think it is an unwillingness to change per se, but it's more like an opportunity to really investigate what's broken. Without an ongoing, continuous, holistic view into customers' interactions and behaviors, these organizations are going to remain at risk with regards to abandonment, churn and, more importantly, the inability to grow digitally.

Driving Security

FIELD: What factors do you see pushing organizations now to strengthen these authentication methods for their digital channels?

DEFAZIO: So the biggest drivers for strengthening authentication across their digital channels are the impacts organizations fear they will see if they do not address it now – things like financial loss, data breaches, customer churn and brand reputation risk. That's big one: the inability to drive digital growth. I'd say these are the biggest threats.

And then another major factor is the need for digital expansion in order to stay competitive. These big organizations are out there trying to compete with digital native startups and deliver the experience customers expect today. Or, if they don't, they are running into the risk of becoming seen as a dinosaur.

Leaders and Laggards

FIELD: As you look across sectors, where do you see leaders and laggards in providing digital security and trust? And what are some of the factors behind what makes a leader or what makes a laggard?

DEFAZIO: Financial institutions typically are leaders in the space, as they tend to have the most stringent compliance and regulatory guidelines. They've experienced exponential fraud risks more recently, especially with the rollout of EMV. And it's forced them to constantly be one step ahead of their fraudsters. They don't have a choice.

At the same time, they're trying to assure their customers that their investments are safe, all while trying to offer a seamless customer experience.

I wouldn't say they were laggards. However, retail faces significant challenges as the customer omnichannel journey is really quite complex. It requires a great deal of multifactor security and step-up authentication, but still enabling digital growth and adoption. So unlike the leaders – the financial institutions who are typically having returning customers who come back and they're building up this profile – retailers have customers who are quite unique. They can be one-time customers; they can make guest purchases. And therefore it presents a whole new set of challenges when really trying to establish digital identity trust.

In addition, a new user is more likely to give a bank more PII, especially since they're holding investments, whereas if retailers' customers can't easily and quickly make a purchase, then they'll just go on to the next competitor who can.

So it's quite interesting to watch the space evolve. And I would just, in closing, say that all organizations are going to continue to be under pressure to find this balance. And as the fraud landscape continues to evolve, so must our efforts with regard to establishing digital identity trust. It'll just remain an ongoing opportunity to continuously improve.

2019 Investments

FIELD: Christine, one of the things that stood out to me is that more than half of our respondents say that they have budgeted specifically to improve digital trust in 2019. Knowing that, where would you counsel them to prioritize their investments?

DEFAZIO: Every organization is different, and I can't provide unique recommendations. However, generally speaking, with a priority of establishing digital identity trust in this demanding digital transformation environment, I would say a few things are key.

The omnichannel journey is tricky to navigate, so you must be constantly understanding their behaviors across every stage of the journey; that's a challenge. Investments in digital identity trust tools that encompass things like the ability to identify new and existing users – including their attributes, device, activity environment and behavior – are essential.

Customers want to know that you're securing their interactions, but they don't want to be hindered with their experience, either. So the balance is visible security, as well as continual transparent security.

Behavioral biometrics, machine learning and AI are just a few of those tools – also, the security intelligence to back it up. Digital trust requires continuous improvements and optimizations; it's not a "set it and forget it" type of solution.

So if you start to get comfortable, fraudsters are definitely going to know and they're going to prey on your weakness. Things like single-factor authentication and one-time passwords rely on PII that's readily available on the dark web. And sometimes it's even available with a simple internet search or something you could easily find on social media.

So multifactor authentication, risk-based authentication, step-up authentication – all of these are must haves. And again, every organization is unique as to the challenges they face, so it's crucial to find the right vendor who can really build a custom solution to help you meet those challenges.

Metrics

FIELD: What would you say are the key metrics organizations should be paying some attention to?

DEFAZIO: You want to take a look at abandonment into other more costly channels – for example, the call center. You're going to want to look at fluctuations in fraud loss and churn. And you're also going to want to consider adoption and growth of the digital channel products and services.

Putting Survey to Use

FIELD: If you take a look at our survey results overall, how do you recommend that our audience use them? What's the case that they can frame for their organizations based on what we've discovered?

DEFAZIO: The survey tells a fantastic story, and it's full of opportunity. Almost everyone wants to improve the customer experience and digital trust while meeting the growing customer expectations for more digital services – that we know. So many are working toward this 2019 goal. And we've identified these gaps, therefore enabling you to build a business case. You don't have to favor security over customer experience or vice versa; you can actually have both, and I know that's crazy sounding.

If we break it down and look at it from a challenge/opportunity/solution perspective, the challenge is for organizations to revisit their current single-factor authentication methods that are leaving them susceptible to breaches and fraud loss, among other types of financial loss. Be smarter than the fraudsters. That requires establishing a key team to help drive change management, and then identifying your true fraud loss, identifying your abandonment rates, churn, and other factors that are negatively impacting your business. And from there, it's a matter of really investigating what opportunities you have for reducing fraud and churn, as well as improved customer satisfaction, adoption and digital growth.

And lastly, it's a matter of interviewing best-in-class providers that can help you meet those needs. Make sure that they have a strong cloud solution; it needs to be backed by the intelligence and services to help you through your digital journey. Ensure that they're the ones who could help you provide the next-generation customer experience with the right mix of visible, transparent security customers expect.

IBM's Offerings

FIELD: How is IBM helping organizations across sectors improve their means of ensuring digital trust?

DEFAZIO: IBM Trusteer helps organizations seamlessly establish digital identity trust across the omnichannel journey. Again, it's really critical to make sure that you're following their behaviors, their devices and interactions from start to finish, and continually improving upon what you're trying to build, as far as a profile.

Through cloud-based intelligence, backed by AI and machine learning, Trusteer provides a holistic platform that's really designed to help organizations welcome in new and existing customers while keeping the bad actors out. This allows organizations to leverage Trusteer solutions to help them really establish a trusted and frictionless digital relationship quickly as well as transparently. ■

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io