McKinsey&Company
Digital McKinsey

Article
August 2016

Is cybersecurity incompatible with digital convenience?

By Salim Hasham, Chris Rezek, Maxence Vancauwenberghe, and Josh Weiner

Not for successful companies, who tailor the digital experience to provide easy authentication while still valuing customer security. Here's how they do it.

Imagine this common scenario. Two customers log onto your site at the same time. The first one struggles to remember his log-in and password, goes through a password-reset process, and winds up feeling frustrated at what seems like a clunky process. He thinks "Why can't this site just remember my password for me?"

The second enters her password and gets right into her account—and then worries that, in an age of escalating cyberattacks, your site does not seem very secure. She would have appreciated a second challenge, or even the delivery of a secure one-time password giving her access to her account information.

These two customers have very different expectations about their digital security: One values convenience, the other security. How can you possibly make both of them happy? Our research and experience indicate that there is, in fact, a way.

The solution lies in changing the way companies think about both digital security and digital experience, moving away from a one-size-fits-all approach to a more granular understanding of how different customers think and feel about their security experiences. For decades, customer segmentation has been a crucial strategy for the disciplines of marketing and sales. It is time to put it to work for digital security. By focusing on the range of customer journeys, companies can deliver a superior digital

experience without compromising either customer perception of security or the underlying risk exposure for the enterprise.

What it's worth

In recent years, firms have responded to the increased frequency and complexity of cyber threats by putting higher security burdens on customers. The result is that the quality of the digital experience for customers has decreased dramatically. According to our research, customers have to remember more than 14 passwords on average and increasingly complain about the inefficiency and complexity of the authentication experience. Yet, ironically, consumer perceptions of security have worsened. Digital security and privacy are eroding consumer trust online.[1]

Improving the digital security experience for consumers is a high-value task for companies for several reasons. First, it drives digital adoption rates. The hassle of authentication is a key reason customers turn away from digital services. On the other hand, when consumers find the authentication process easy, they use digital services 10 to 20 percent more than customers who are frustrated by authentication.[2] This is important, because customers who use digital channels regularly spend roughly 45 percent more than customers who use digital channels sporadically. These customers also cost significantly less to serve since they are less reliant on customer-support calls or in-person servicing.

Secondly, delivering an experience that is both secure and convenient also has a direct material impact on customer-satisfaction scores. More than any other aspect of a customer's journey, "failing to authenticate" drives down customer satisfaction and overall brand perceptions. It is also the highest-volume customer journey by far and often the number-one pain point for customers. Companies that successfully deliver a remarkable digital experience while also keeping customers' data safe can see a potential 20 to 35 percent boost in customer-satisfaction scores.

Finally, there are cost implications. Authentication-related calls from customers are a significant resource drain. Password-reset inquiries can account for up to 6 percent of call-center activity, which could cost $5 million to $20 million per year for larger operations. Other call-in identity verification represents another 5 to 10 percent of agent handle time and an additional $5 million to $40 million in costs. A hassle for customers, most of these calls represent unnecessary costs, and the goal should be to

eliminate them with a convenient and secure experience.

Finding the right balance between convenience and security for customer segments

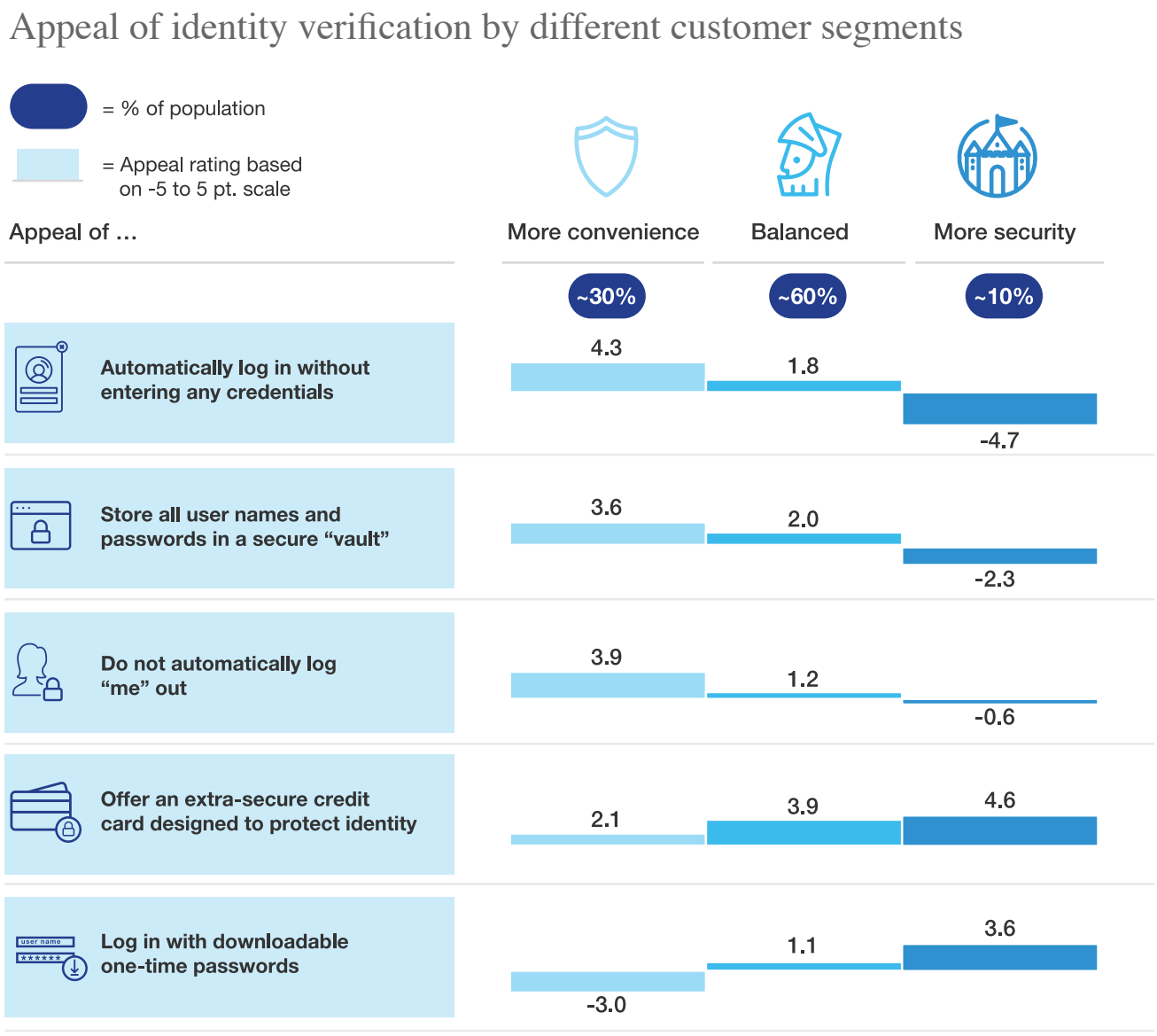
Our research shows that companies should consider three buckets of customers—those who prefer convenience, those who prefer security, and those who are comfortable with a blended model. Although all customers, if you ask them, will say they want both security and convenience, a deeper analysis reveals that a growing minority cares more deeply about one than about the other.

In our research, we find that roughly 30 percent of the population prioritizes ease and convenience over security. These consumers do still want a basic level of security operating behind the scenes, but they say that having access to account information without the need to enter a password (e.g., with automatic device recognition) is attractive or very attractive. They also reject the idea of having a one-time password sent to them for every log-in.

On the other side of the divide are the 10 percent of people who place a higher value on security. These consumers like the idea of a one-time password and feel that not having a password at all is unsafe. The remaining 60 percent are willing to make reasonable tradeoffs in both convenience and security.

So how do you address such a diverse customer base? Our model is two-pronged (Exhibit 1).

Exhibit 1



McKinsey&Company

1. Tailor the digital experience

With the help of data analytics, insights into customer preferences should be applied systematically across the four main elements of authentication:

A. Identification. Different customer segments want different ways to identify themselves. People who value convenience, for instance, might be most comfortable

using their email for an ID and social security number for a password, at least online. Security-aligned customers might want a user ID and eight-character alphanumeric text.

Biometric verification technology, which allows consumers to be identified by their face or fingerprint, can be used for the minority of customers who like this option, but due to the permanent consequences of fingerprint hacks or theft, it is not the across-the-board security panacea many once hoped it would be.

B. Identity Management. Give customers clear and concise options for how they can tailor their security preferences. In consolidated "security centers" or pop-ups that ask customers if they want to "remember this device," lay out the options and let them opt in either for security (send one-time passwords for each access) or for convenience (save their user name and password or allow unmasking of passwords on mobile to solve the "fat finger" problem, i.e., mistakenly clicking a key).

C. Segment access based on risk. Not all transactions are equally prone to fraud and losses. Predictive analytics and transaction segregation can help align authentication with fraud exposure. Companies could, for instance, allow for basic account access without any specific authentication (e.g., view account balances), but require a password for monetary transactions and a one-time SMS password for high-value or unusual actions (e.g., changing mailing address). This could be further segmented based on customer desire, tolerance, and expectations. For convenience seekers, low-risk transactions could require only that they be using an already registered device, whereas high-risk transactions would require a password.

D. Exception management. When something goes wrong—passwords or usernames are forgotten or unusual activity occurs on the account—only the security-seeking minority will appreciate having to jump through hoops to identify themselves. For them, this offers reassurance that hackers cannot easily gain access. But most customers will want a quick resolution to the problem. Slack, a messaging and communication start-up, has pioneered an innovative system that sends users who have forgotten passwords an email with a "magic link" to automatically log them in. Capital One prompts users to call for forgotten passwords and uses communication to help minimize frustration, putting the blame on itself ("We are having trouble signing you in") (Exhibit 2).

Exhibit 2

For the authentication journey, the customer experience is grounded on four primary elements.

McKinsey&Company

We have found that the exception verification method—having customers use their phone to take a picture of their driver's license or passport next to their face—appeals to 80 percent of people who have smartphones. They prefer it to answering security questions (which they may have forgotten) and view it as both secure and convenient. The remaining 20 percent prefer a verification phone call.

2. Make the experience clear, simple and consistent for all customers

In addition to delivering different experiences for distinct customer segments, there are ways to improve the authentication experience for everyone. This includes existing options such as device or number recognition and omnichannel authentication (customers do not want to be treated like strangers just because they are on a different device). Log-in credentials should be the same across all channels and should allow for customers to log in on one channel in order to use another, eliminating duplicative authentications. At Capital One, for instance, customers on the site can request a secure and convenient push notification to be sent to their registered mobile device. Additionally, customers who are logged in online and call the customer-service number are not asked by the automated voice prompts to reauthenticate.

Another simple yet powerful improvement is better visual and functional design of the digital experience. The perception of security drops significantly with inconsistent designs, poor error messaging, clunky communication, and site slowness or unavailability. Fixing this improves the overall perception of security with no trade-offs in actual underlying security. When consumers rate companies as having a "visually appealing digital experience," they give them a 15 to 20 percent higher customer-journey satisfaction score.

Finally, communication about security initiatives is often underappreciated. On its own, without changing any back-end system functionality, improved messaging on how a company is approaching security can lift the customer-satisfaction score by 5 percent. Sophisticated cyberattackers and high-profile breaches have made security a top concern for consumers. Targeted marketing can help educate customers about the hows and whys of the authentication journey—and let them know about the firm's real-time fraud monitoring and under what circumstances the company will tell them about unusual activity in their account. Proactively reaching out to customers via text when there are transactions in two cities on the same day, for instance, and giving them a chance to confirm or deny the transactions, is a simple way to boost customer loyalty.

The right capabilities

Making different types of customers happy at the same time requires a suite of elegant and subtle solutions across many interactions and thus presents organizations with no small challenge. Rising to meet these challenges entails the merger of several capabilities. Laying a strong foundation of customer-journey analytics is critical for developing a segmentation algorithm to rapidly identify patterns and opportunities that need to be addressed. This can include looking at interaction history, such as people who viewed fingerprint ID options but chose not to use them vs. those who did, or those who opt to have a password reset by email vs. a phone call. This data can be augmented by carefully worded customer surveys to further identify preferences and pain points.

The second capability is customer-centered design. This means that every initiative is framed by the question, "How will this affect or be received by customers?" Part of delivering on this approach entails empowering customers with various simple but noninvasive options. One simple example is to accept all passwords but provide a red, yellow, or green indicator for password strength, letting customers calibrate based on their preferences.

Lastly, it is critical for companies to have sophisticated security and technology expertise. In order for changes and innovations to have a net positive impact and not create genuine security risks, companies must understand the latest fraud and hacking threats and exposures from both a legal and technical point of view. This way they can distinguish between cases where risk exposure is minimal and thus the allowance of customer preferences is acceptable, and instances where additional monitoring or controls may be necessary. Creating a successful customer-authentication team requires directly engaging with the security and fraud teams early on in the customer-experience design process—instead of seeking their review after the fact.

The new era of the customer requires that companies think of security and ease of use as compatible goals. Instead of focusing exclusively on how to enhance protections in the back office, companies need to reimagine security from the customer's point of view. Organizations that do this will not only become more adept at digital security; they'll build trust with their customers and develop a crucial competitive advantage.

1. "New survey highlights startling erosion of online trust," May 15, 2016, *Forbes*.

2. Unless otherwise noted, all data is sourced from McKinsey's ClickFox database and unique market research.

About the author(s)

Salim Hasham is a partner in McKinsey's New York office, where **Maxence Vancauwenberghe** is head of ClickFox partnership and **Josh Weiner** is a client service manager. **Chris Rezek** is a senior expert in the Boston office.