A Custom Technology Adoption Profile Commissioned By RSA

December 2013

Consumer Web Portals: Platforms At Significant Security Risk

Introduction

The increasing number of digital identities, prevalence and impact of data breaches, and loss of customer information are driving a heightened requirement for effective consumer-facing identity and access management (IAM) solutions. Many organizations with consumer portals, however, do not have effective protections in place.

This RSA-commissioned profile of business-to-consumer (B2C) security decision-makers in the financial services, healthcare, government, and online merchant sectors evaluates security around consumer portals based on Forrester's own market data and a custom study of the same audience.

Security Pros Are Standing Pat On Consumer-Facing Identity And Security Improvements

Forrester sees clear majorities of firms engaging in online consumer engagement in an identity-enabled way. In our Forrsights Security Survey, Q2 2013, 56% of IT security decision-makers reported that they either have implemented or plan to implement consumer identity theft/fraud management; 60% have implemented or plan to implement consumer IAM (see Figure 1).

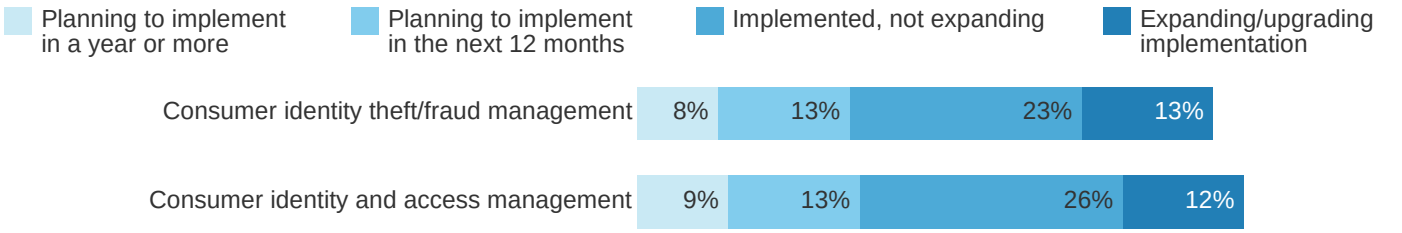
However, we have reason to doubt the security of all of these consumer portals. When asked what security solutions they use to protect their consumer-facing web portal, the top response of these security pros was standard single-factor authentication involving a user name and password (83%), with forgotten-password resets through either challenge questions (62%) or an emailed link (58%). A much smaller population of respondents reported using two-factor authentication or risk-based detection tactics (see Figure 2), both of which can increase the practical ability to authorize access by the right people to the right applications.

Often, the reason for such light security is the fear of a negative user experience, leading to lower rates of consumer conversion, such as shopping cart abandonment. We see security pros becoming more aware of stronger authentication options, however, as they attempt to battle security and fraud risks. Respondents showed significant interest in using hardware one-time password tokens, mobile-device-generated passwords for two-factor authentication, and certificates stored on a device for two-factor authentication (see Figure 3).

FIGURE 1

More Than Half Of Firms Have Already Adopted Identity-Related Technologies Focused On Consumers

"What are your firm's plans to adopt the following identity and access management technologies?"

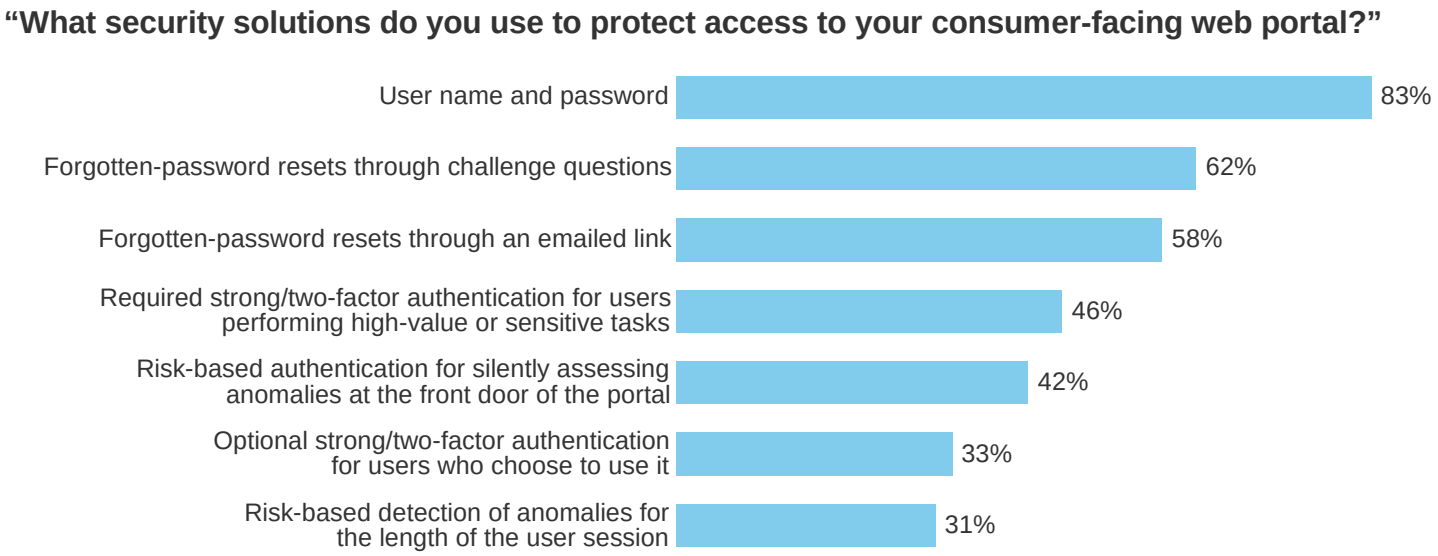


Base: 1,171 IT security decision-makers

Source: Forrsights Security Survey, Q2 2013, Forrester Research, Inc.

FIGURE 2

Organizations Typically Protect Consumer-Facing Web Portals Using Weak Password-Based Methods

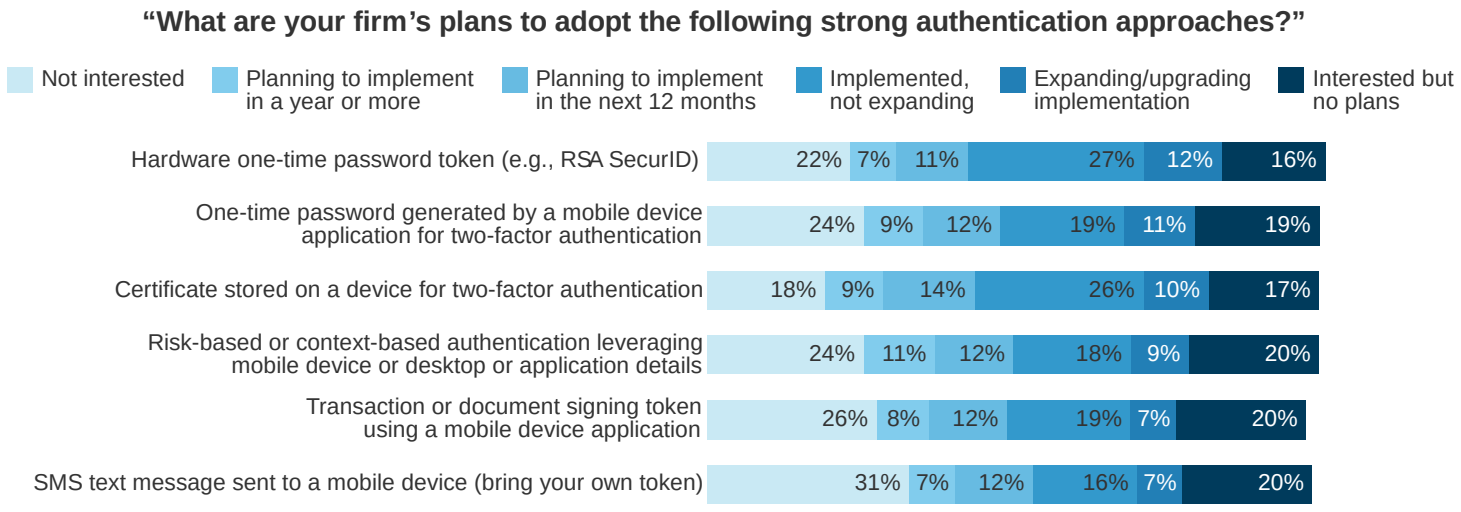


Base: 48 IT security decision-makers

Source: A commissioned study conducted by Forrester Consulting on behalf of RSA, October 2013

FIGURE 3

Security Pros Are Showing Interest In A Variety Of Stronger Authentication Techniques



Base: 1,171 IT security decision-makers ("Don't know" responses have been omitted)

Source: Forrsights Security Survey, Q2 2013, Forrester Research, Inc.

FORRESTER®

Breaches Pose A Heavy Risk To Businesses

Security pros are, of course, greatly concerned with the multitude of security threats to their consumer-facing web portals, and with good reason: Weak authentication, authorization, and fraud detection capabilities present a known and growing risk. Adobe recently disclosed a breach of credentials and credit card data for more than *38 million* consumers, requiring all of them to go through a password reset experience — and enabling hackers to learn passwords commonly shared by users across sites.[1] Users reuse passwords in this way to simulate single sign-on (SSO); unfortunately, this faux method is much more vulnerable to attacks than true SSO, particularly when real SSO is combined with strong and risk-based authentication.

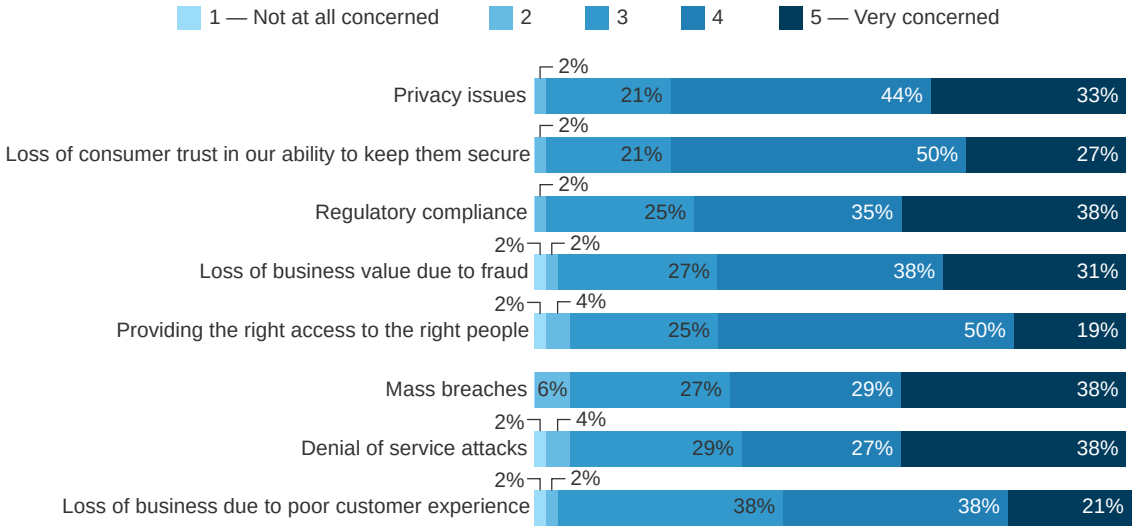
Survey respondents told us that privacy issues, loss of consumer trust, and regulatory compliance are the top three threats they see from consumer portals, with at least 70% of respondents ranking their level of concern for each of these as a "4" or "5" on a 5-point scale (see Figure 4). And loss of business due to a poor customer experience resulted in well over half (59%) of respondents expressing this level of concern.

Breaches put many types of data at risk. Forrsights data shows that two of the three most common types of data to be compromised among companies that had been breached were personally identifiable information (32%) — frequently used as the basis for security challenge questions — and authentication credentials (25%). Both of these, when used without compensating controls in the form of stronger authentication, authorization, and contextual fraud detection techniques, can give attackers the means to gain full access to consumer accounts and inflict the most damage (see Figure 5).

Further, these breaches can result in many different types of business value walking out the door. Even a "soft" risk like loss of consumer trust in a portal can have significant revenue implications. Nearly all of our respondents (92%) were using their consumer web portals for direct monetary transactions — with the majority being used for transactions higher than $1,000 (see Figure 6).

FIGURE 4
Security Pros Report Great Concern About Both "Hard" And "Soft" Business Risks Related To Security

"How concerned are you about the following security-related aspects of your consumer-facing web portal?"

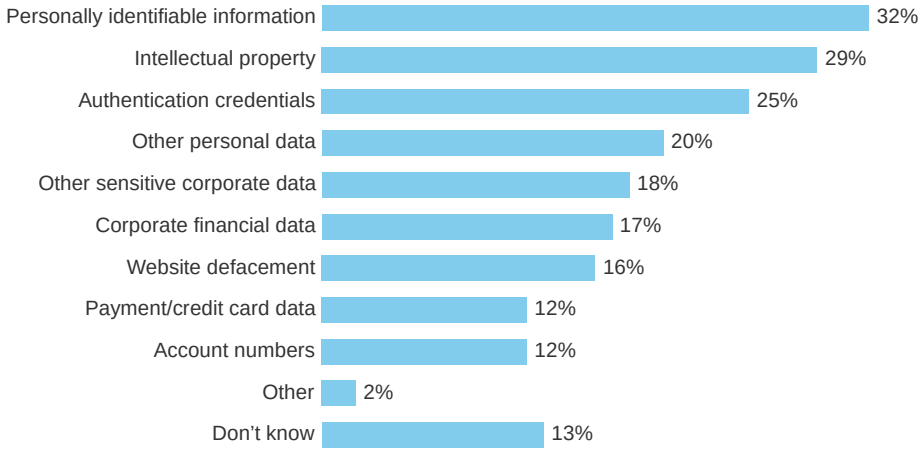


Base: 48 IT security decision-makers (percentages may not total 100 because of rounding)

Source: A commissioned study conducted by Forrester Consulting on behalf of RSA, October 2013

FIGURE 5
Authentication Credentials Of Various Types Are A Frequent Data Breach Target

"What types of data were potentially compromised or breached in the past 12 months?"

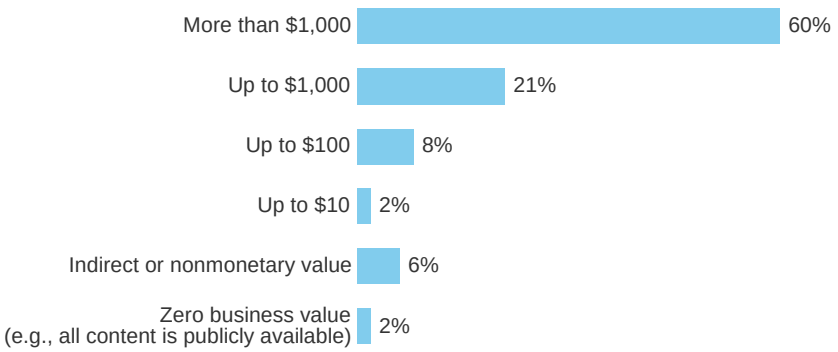


Base: 578 IT security decision-makers who had a data breach in the past 12 months

Source: Forrsights Security Survey, Q2 2013, Forrester Research, Inc.

FIGURE 6
Financial, Healthcare, Government, And Merchant Consumer Portals Support Significant Transaction Value

"What is the highest-value transaction that consumers can perform through your web portal?"



Base: 48 IT security decision-makers (percentages do not total 100 because of rounding)
Source: A commissioned study conducted by Forrester Consulting on behalf of RSA, October 2013

Key Findings And Conclusions: Desire And Reality Are Badly Mismatched When It Comes To Consumer Web Portal Security

Security pros can see that poor security in consumer web portals leads to significant direct risks, such as loss of transaction value through fraud. But they may not yet be connecting poor authentication, authorization, and fraud detection strategies with the resulting business risks, such as the loss of trust in the business by consumers forced to perform password resets in the case of a breach or even simple loss of business value due to a poor consumer experience that gets in the way of a transaction.

While these professionals recognize that there's a wide world of stronger controls out there, most of them have yet to make the leap to recognizing the dramatic impact such controls could have: They can avoid a great deal of password reset pain, consumer dissatisfaction, and a cascade of other negative impacts to the business simply by catching fraudsters ahead of time.

Methodology

This Technology Adoption Profile was commissioned by RSA. To create this profile, Forrester leveraged its Forrsights Security Survey, Q2 2013. Forrester Consulting supplemented this data with custom survey questions asked of US enterprise security leaders (managers and above in title) directly involved in decisions regarding security for their consumer-facing web portals. The auxiliary custom survey was conducted in October 2013. For more information on Forrester's data panel and Tech Industry Consulting services, visit www.forrester.com.

Related Forrester Research

“Introducing The Customer Authentication Assessment Framework,” Forrester Research, Inc., June 12, 2013

“Inquiry Spotlight: Consumer-Facing Identity, Q4 2012 To Q1 2013,” Forrester Research, Inc., March 22, 2013

“Navigate The Future Of Identity And Access Management,” Forrester Research, Inc., March 22, 2012

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester’s Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

Endnotes

[1] Source: Nick Bilton, “Adobe Breach Inadvertently Tied to Other Accounts,” The New York Times, November 12, 2013 (http://bits.blogs.nytimes.com/2013/11/12/adobe-breach-inadvertently-tied-to-other-accounts/).