RISING TO THE CHALLENGE OF IAM

Behavioral analytics is driving the arms race of determining "are you who you say you are"

ebook

An SC Media publication

Sponsored by

RSA®

The changing cultures of identity and authentication

"Are you who you say you are" is a question as old as the first computer login. The risk of getting identity wrong and enabling a breach is driving behavioral analytics and other technologies, taking IAM to new heights. Will that solve the problem? Evan Schuman explains.

Authentication systems historically involved a simple yes/no binary: Are users who they said they are when they presented their credentials? But those systems quickly are becoming obsolete. Today's authentication has evolved into an on-going process of behavioral challenge and response, essentially morphing into the next generation of identity and access management (IAM) that promises to reduce friction and increase reliability. How that promise is fulfilled is turning the IAM and cybersecurity markets upside down.

IAM comes with a plethora of technological, operational, financial, and legal challenges. First and foremost, according to Michael Wyatt, the cyber identity leader for consulting firm Deloitte Risk and Financial Advisory, and his colleague, Alex Bolante, managing director and a national leader for consumer identity management at Deloitte and Touche, enterprise CISOs, CSOs, and chief risk officers (CROs) sometimes struggle with IAM strategies in that they sometimes confuse identity and authentication.

From Deloitte's perspective, Wyatt and Bolante, both based in New York City, say that identity deals with identification data, such as metrics about end-users. This could include biometric and behavioral data, as well as permissions and privileges. Authentication refers primarily to analytics — the systems and software that crunch that identification data and make permit/reject recommendations or decisions.

Christopher Burgess, a Woodinville, Wash.-based independent security consultant, says that much of the data a company can access about customers, employees, contractors, and partners can change significantly depending on geography. "The level of detail that your employer can pull in the U.S. dwarfs what you can pull in Amsterdam," he says. "And you will know even less about your employees in India."

According to Deloitte's Bolante, security executives "keep missing the identity data challenge." Some who are unhappy with their existing IAM results try to fix the problem by purchasing expensive IAM software suites. However, they miss the mark because the sophisticated analytics software might be unable to produce better results when fed the

OUR EXPERTS: IAM

Conrad Agramont, CEO, Agile IT

Alex Bolante, national leader for consumer identity management, Deloitte Risk and Financial Advisory

Christopher Burgess, security consultant

Tim Callahan, senior VP and CSO, Aflac

Andras Cser, VP and principal analyst for security and risk, Forrester Research

Chris Duvall, senior director, The Chertoff Group

Dean Fantham, founder and chief technology officer, Edgile

Wesley McGrew, director of cyber operations, Horne Cyber

Steven Murdoch, principal research fellow, department of computer science, University College London

Daniel Portenlanger, CEO, Simprocity

Aubrey Turner, director of client services and identity, Optiv

Mike Wyatt, cyber identity leader, Deloitte Risk and Financial Advisory

11

Number of companies taken offline this month due to an expired Ericcson software certificate

– The Verge

same inaccurate or insufficient data as their original IAM products.

Multifactor authentication

Chris Duvall, senior director for The Chertoff Group, a Washington, D.C.-based consulting firm, says that having deficient data is only one in a long list of IAM headaches. "Authentication is really hard. CISOs from Fortune 5 to Fortune 5000 are struggling with it."

Chris Duvall, senior director, The Chertoff Group

There is also the issue of where to get the authentication data points, which leads to the in-band and out-of-band question. Andras Cser, a vice president and principal analyst for security and risk at Cambridge, Mass.-based Forrester Research, says there is not much to debate regarding multifactor authentication (MFA). "In-band is a bad idea but we see it all the time. Ideally, MFA has to be out-of-band," he says. "The best way today is push notification to a mobile app. If the original transaction is on a mobile app, then you'd want to use biometrics — face, voice, finger — for out-of-band MFA."

> "The wave of the future is incorporating concepts of machine learning or intelligence to say we know this is the user because of their key stroke, the way they hold their phone or other very discrete mannerisms users don't even realize."
>
> *– Tim Callahan, senior VP and CSO, Aflac*

Daniel Portenlanger, the CEO of Chicago-based security consulting firm Simprocity, thinks in-band/out-of-band is not that cut-and-dry. "I don't think they are mutually exclusive," he says. "Many out-of-band MFA systems authenticate and provide in-band authentication. [The] key is to have as many separate validations as possible. If they all are successful, authenticate. The industry is pushing out-of-band MFA because the keys to the locks on the door are stored in different places. If a [cyberthief] breaches one authenticator and not the others, things are still locked down."

Tim Callahan, senior vice president and CSO for Aflac of Columbus, Ga., the $23 billion insurance giant, argues that both forms of verification data have their uses.

"There are pros and cons for each. Out-of-band MFA requires separate actions that could be seen as inconvenient, but this offers much better security from the standpoint of something [from] the internet," Callahan says. "Analysts are correct regarding [the problems with] in-band MFA. However, if I am protecting an application within my environment, in-band MFA is probably good enough and user convenience, which is always important in any protocol, outweighs the risk in my opinion."

But "in a different scenario over the internet like consumers using ecommerce sites, then out-of-band is more important because you don't have visibility into the user environment or on the user's machine," Callahan says. "In this case, where you can't know with certainty, out-of-band MFA is more of a necessity."

The central concern for an enterprise identity strategy today, though, involves behavioral analytics. In theory, it is the approach that will improve security, eliminate passwords, and do it all while delivering close to zero friction. Potentially it also could be a threat to the user.

$7.1B

Projected size of the IAM market in 2018

– Statista

www.scmagazine.com | © 2018 Haymarket Media, Inc.

Early and late adoption

Forrester's Cser sees global enterprise adoption of behavioral analytics somewhere between 15-25 percent, with the U.S. much more aggressive with adoption approaching 40-50 percent. "But that is imbalanced toward larger organizations," he says, projecting that some 60-70 percent of Fortune 100 companies already adopted some level of behavioral analytics. When that group is expanded to the Fortune 1000, adoption rate drops to the same 15-25 percent.

Steven Murdoch, principal research fellow, department of computer science, University College London

Cser says that he sees enterprise CISOs making "two big mistakes: thinking it's too easy and thinking it's too complicated." Some, for example, rely on social logins, letting customers gain access by piggybacking on their Facebook or Twitter credentials "to give [customers] a warm and fuzzy feeling around the veracity of the identity." The problem is that this approach fails if the social media partner is breached.

Also, social media authentication has verification issues. "If you're taking information from Twitter or Facebook, there's no reason to believe that is going to be accurate," says Steven Murdoch, the principal research fellow in the department of computer science at the University College London. Consumers "may not tell the truth to Facebook and Twitter."

Forrester's Cser adds, "Machine learning is the only cure for reducing customer friction." AI's machine learning is the basis of almost all behavioral analytics efforts.

Aflac's Callahan agrees. "This is the direction where we have to go, where we are combining authentication with behavioral analytics. In this scenario, aspects of the user, the session, the client, or machine that are outside the individual's view or conscience are [used to] validate that a person really is who they say [they] are.

"For the consumers now, there is knowledge-based authentication — such as call centers or Equifax — where they are asked questions that are discrete enough that the criminal shouldn't know but the consumer should," Callahan continues. "We knew that this method would only be effective for so long because the criminals are building databases of consumers. The Equifax breach accelerated the demise of this type of authentication as a reliable method."

This problem logically builds into behavioral analytics. Callahan notes, "Other points of authentication are now preferred like repeat customer environments where you can authenticate by building a logical user profile, increasing recognition of [the user] over time, and forcing them into another authentication method if necessary. The wave of the future is incorporating concepts of machine learning or intelligence to say we know this is the user because of their key stroke, the way they hold their phone or other very discrete mannerisms users don't even realize."

> "Machine learning is the only cure for reducing customer friction"
>
> *– Andras Cser, VP and principal analyst for security and risk, Forrester Research*

But it is not a magic bullet. "Traditionally, criminals rely on phishing, spoof calls, and other tricks to get info from people because they know it and are subject to revealing it," Callahan adds. "However, using these

72%

Percentage of European IT executives who said IAM should be a platform to secure digital services

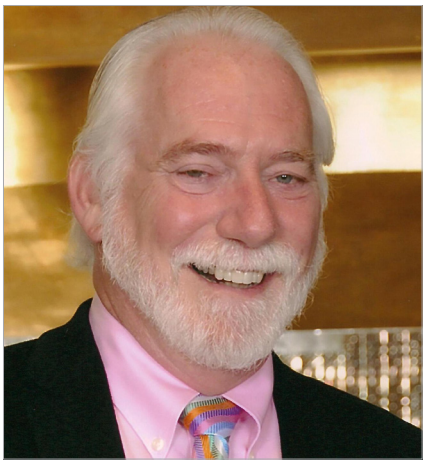
– Teknology Group

new intelligence methods that users don't even realize means users can't be tricked into revealing it. These authentication methods will have a limited time just like everything else."

Aflac is still using a call center query approach for its current customer authentication, but Callahan says that he knows this tactic likely is just a stopgap measure while awaiting the next authentication security option.

> "When you are buried in false positives, it's like swimming in manure. You're not getting anywhere and it stinks"
>
> – *Christopher Burgess, security consultant*

"Today, we are doing client validation through [a credit reporting company], for instance, which is a very effective, third-party method with a rich database to authenticate that an individual is who they say there are. This option is still effective in the vast majority of cases," Callahan says.



Christopher Burgess, security consultant

"However, companies need to up their game quickly to get to the next level. For example," he continues, "we need to be able to prevent a man-in-the-middle event attack where a user is accessing a site that's been compromised and criminals are using robotics and machine learning to essentially turn into the consumer and commit fraudulent acts."

MFA is not the only answer. "Everything in MFA is time-limited, like encryption algorithms," he notes. "It's our job as security professionals to figure out the next best thing to stay ahead of criminals, especially state-sponsored criminals with deep pockets and resources. We need to continue building the strongest possible partnership between industry, vendors and the government."

But behavioral analytics is new enough that much will depend on administrator choices regarding analytics strictness. Which is worse: Having the system be too lenient and let cyberthieves in (false positives) or having the system be too strict and blocking legitimate users (false negatives)?

"When you are buried in false positives, it's like swimming in manure. You're not getting anywhere and it stinks," Burgess says. "If you can't support [the false positive decision rationale], one false positive can make you dead in the water."

In case of emergency, break glass

Another consideration is what happens during an emergency. Is there a contingent break-glass plan to override the system if — or more precisely, when — the need arises?

Conrad Agramont, CEO of the San Diego-based consulting firm Agile IT, argues that such a contingency plan is vital and that relatively few enterprises have them in place. And the few that do have such plans rarely test them.

Agramont says that there is an "importance of having break-glass procedures in place for when identity and authentication systems fail, due to outage or natural disaster. [A recent] MFA outage by Microsoft saw hundreds of businesses shut down because when MFA fails, and users can't log in, global admins are in turn unable to access the controls needed to turn it off. This [problem] can occur for many reasons, from DDoS attacks or loss of devices to loss of the cellular network.

"In life or death critical systems, such as ePHI in health care," Agramont adds, "this is doubly important, as disaster scenarios often

80%

By 2022, identity and access management as a service (IDaaS) will be the chosen delivery model for more than 80% of new access management purchases globally

– Gartner

require deviance from HIPAA compliance that must be reported and logged."

Yet, according to Agramont, CISOs are "definitely not thinking about" break-glass protocols. "They simply haven't thought about that scenario."

He estimates that fewer than five percent of Fortune 1000 companies have a break-glass protocol, which typically empowers two system administrators to jointly use their passwords to break the rules and restore direct access. "It's just not a normal practice. It should be."

Aubrey Turner, director of client services and identity, Optiv

This requirement is a critical reason for repeated testing as well, given the issue of personnel changes. "What if one of the people who has the other half of that password left six months ago?" he asks.

Aubrey Turner, the director of client services and identity for security consulting firm Optiv in Denver, says another hurdle for many IAM deployments is budget and corporate ownership. He compares the handling of enterprise resource planning (ERP) to that of IAM. "From a technical deployment perspective, […] it is similar to ERP and other large enterprise deployments, and yet enterprises often do not treat it this way, with nobody holding clear ownership over IAM.

> "The struggle right now is that we are all living in a very hybridized world."
>
> – Dean Fantham, founder and chief technology officer, Edgile

"Imagine deploying ERP with no clear ownership?" he continues. "As a result, these deployments often fail. IAM is often treated as a one-off project rather than an ongoing ERP-caliber deployment ongoing management initiative. When enterprises treat it as such, they are always disappointed with the outcome."

For many companies, ERP projects have their own line in the enterprise budget. But IAM projects are typically owned by multiple business units, and as such, there is no clear ownership nor a clear path to a meaningful budget. "Nobody wants to own it because, if you don't do it right, you have a bad reputation," Turner says.

And IAM can also suffer from the inevitable cloud complications.

"As more and more cloud services use third party services, it is impossible to know how secure your company's systems are," Simprocity's Portenlanger says. "What audit methodology does IT staff use to validate and certify cloud services are secure?"

Dean Fantham, the founder and chief technology officer for Edgile, a security and compliance consulting firm based in Austin, also points to the cloud as a key challenge for IAM.

"The struggle right now is that we are all living in a very hybridized world," he says, referring to systems that exist to varying degrees both on-premises and in the cloud. "How do I mold these things together? What is the right spot to have my primary authentication? Is it Active Directory now?"

There is also the question of intervention rates. In other words, how much friction is too much and how much is not enough?

With all of the talk of behavioral analytics reducing friction, it is easy to forget that friction is not always a bad thing. In banking and healthcare companies, for example, customers value privacy and security much more highly than they typically do in retail or hotels. A bank or hospital that appears

65%

Respondents who identified Shadow IT as a challenging development to the consistent implementation of IAM controls

– KPMG Identity and Access Management in the Digital Age

to offer no friction might make customers nervous that their money and medical test results are not being sufficiently protected.

Agramont notes that there are other factors in choosing the level of friction as well, such as competitiveness. He points out that Amazon, for example, has dozens of rivals one click away, so it is careful to keep friction low. But how much authentication friction would have to happen before someone would change doctors or move their money to a different bank?

"With healthcare, they don't have that pressure of consumers leaving," Agramont adds.

Security and compliance at a crossroads?

Another authentication technology that is popular is self-learning, where a system updates its identity database over time based on end-user interactions. One popular consumer device company has deployed facial recognition and says that if the system declines to authenticate a user, it defaults to the phone's PIN. If the person then authenticates with the PIN, the system examines the new picture and updates its profile database.

In other words, if the user is growing a beard or changing how makeup is applied, the phone would add that information to its database so that, eventually, the phone can authenticate the user's new look.

Wesley McGrew, director of cyber operations, Horne Cyber

Murdoch points out, however, that a well-designed self-learning system still has serious limits on how far the initial profile can be altered. "If something is continually learning, it can cause the system to drift away" from its initial information, Murdoch says. "It looks at what it expects and if it's relatively close, [the system] will accept the update. But if it's very far away, [the system] will just ignore it."

Then there is the opposite security hole: Could attackers use the data enterprises collect to pose as legitimate users? This tactic is the judo strategy of using an enterprise's strengths against them.

If an attacker is able to obtain a user's PIN, then any device protected by that PIN is vulnerable. A phone that uses facial recognition to authenticate the user might reject an attacker's visage, but if that attacker has the appropriate PIN the phone might well accept that new facial image as the base image since it was effectively authenticated. Despite advanced technologies and biometrics, in some cases devices revert back to the user's PIN, which might be one of the least secure technologies in the user's arsenal.

> "The infrastructure required to sustain ongoing [behavioural analytics] monitoring will require additional compute capacity."
>
> *– Mike Wyatt, cyber identity leader, Deloitte Risk and Financial Advisory*

Wesley McGrew, director of cyber operations at Horne Cyber, a security consulting firm based in Washington, D.C., poses this query: "Can an attacker with access to another system — such as an app, ecommerce site, etc. — learn the characteristics of a user in a way that can be reproduced?"

McGrew also wonders if "a user's mood/stress-level/other factors could [prompt] behavior changes that will cause them to be denied access."

Finally, are enterprises prepared to fund

48%

Percentage of respondents who said threat and breach mitigation is a pre-requisite for digital transformation

– KPMG Identity and Access Management in the Digital Age

the additional resources they need for this managing behavioural analytics in the long term? One staffing concern is the need for larger call centers to deal with employees and customers who are abruptly knocked off the system when a behavior does not match system expectations.

"The infrastructure required to sustain ongoing [behavioural analytics] monitoring will require additional compute capacity," says Deloitte's Wyatt. "It's a pretty heavy lift. A lot of IT environments are not developed and equipped for this."

As noted earlier, behavioral analytics can be a serious threat to user and consumer privacy. These new, deep pools of knowledge collected for authentication also have value beyond security and IT. Data captured to note how users are typing, what locations they frequent, and the times they typically shop is also data that many marketing departments would love to access. Although privacy compliance efforts such as the European Union's *General Data Protection Rules* (GDPR) or the *California Consumer Privacy Act* could permit using such behavioral data for strict security reasons — it makes little sense to let thieves opt-out of more stringent authentication. Passing such data to departments beyond security and IT easily could generate compliance problems.

Ultimately, companies that commit to anticipating problems caused by deficient data; meeting technological, operational, and financial challenges head-on; assigning someone clear ownership over their IAM implementation; investing in the proper resources for staff, equipment, and ongoing adjustments; and carefully considering how such data will be used will find themselves well-prepared into the future. Those that put their heads in the sand and ignore these issues risk paying a steep price. ■

For more information about eBooks from SC Media, *please contact Stephen Lawton, special projects editorial director, at stephen.lawton@haymarketmedia.com.*

If your company is interested in sponsoring an eBook, please contact David Steifman, VP, publisher, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.

65%

Percentage of organizations that were aware that their employees are using unsanctioned file sharing tools

– AIIM

Sponsor

RSA

RSA offers Business-Driven Security™ solutions that uniquely link business context with security incidents to help organizations manage risk and protect what matters most. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and, reduce business risk, fraud, and cybercrime. RSA protects millions of users around the world, and helps 90% of the Fortune 500 companies thrive in an uncertain, high risk world.

For more information, go to rsa.com.

Masthead

EDITORIAL
VP, EDITORIAL Illena Armstrong
illena.armstrong@haymarketmedia.com
SPECIAL PROJECTS EDITORIAL DIRECTOR
Stephen Lawton
stephen.lawton@haymarketmedia.com
SPECIAL PROJECTS MANAGER
Samantha Lubey
samantha.lubey@haymarketmedia.com

DESIGN AND PRODUCTION
ART DIRECTOR Michael Strong
michael.strong@haymarketmedia.com

SALES
VP, PUBLISHER David Steifman
(646) 638-6008 *david.steifman@haymarketmedia.com*
VP, SALES Matthew Allington
(707) 651-9367 *matthew.allington@haymarketmedia.com*