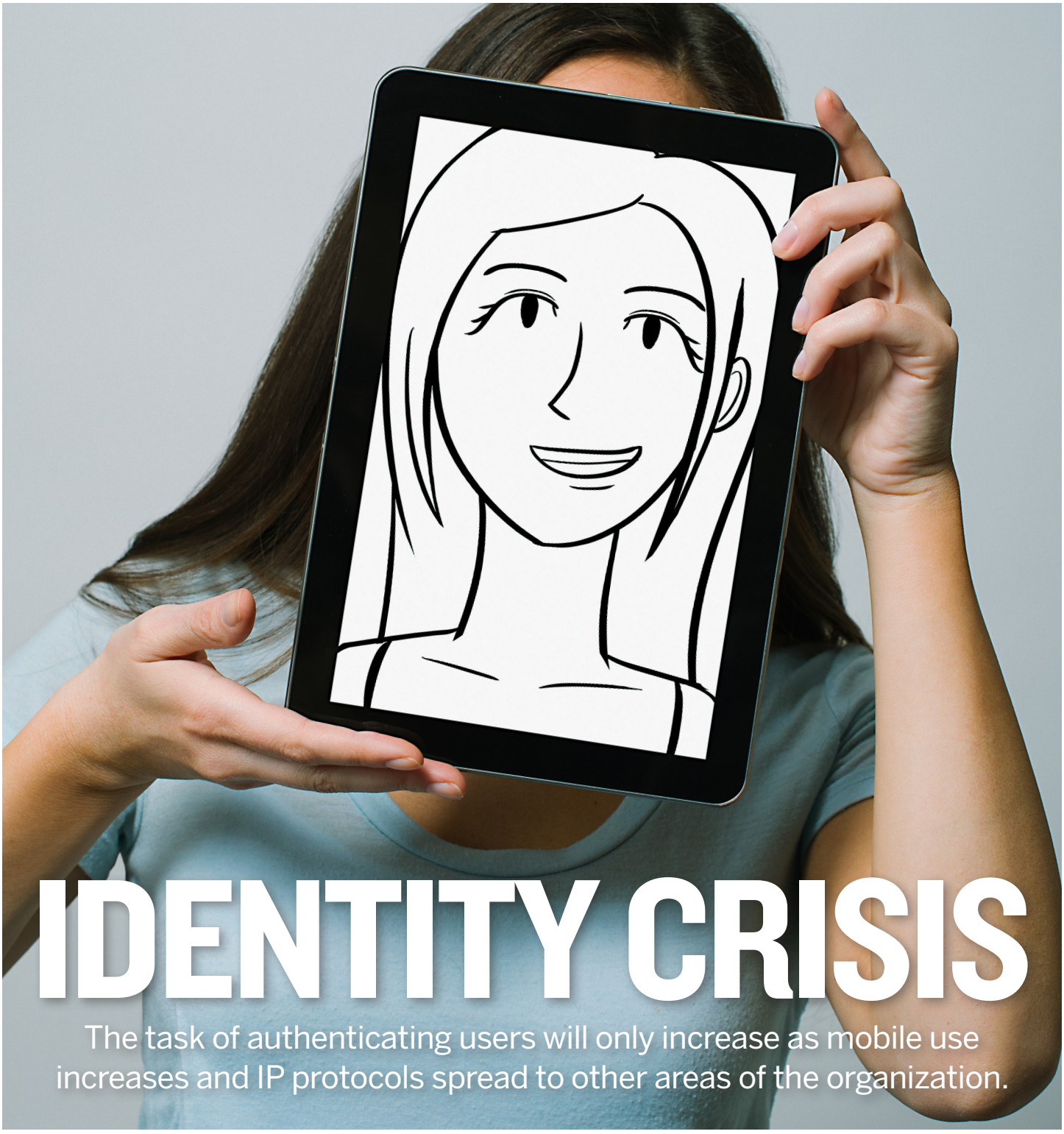

IDENTITY CRISIS

The task of authenticating users will only increase as mobile use increases and IP protocols spread to other areas of the organization.

ebook

An SC Media publication

Sponsored by

RSA®

Who are you?

Identity and access management tools and processes have come a long way, but enterprises face increasing challenges when it comes to authenticating users from both personal and corporate networks and devices. Karen Epper Hoffman reports.

Identity and access management is a mixed bag – not just among different sectors and industries, but even throughout individual organizations. Just ask Erik Avakian, chief information security officer for the Commonwealth of Pennsylvania.

Identity and access management is fairly mature for the state's employee population, where Avakian's team works closely with human resources using automated processes to manage users' online identities throughout their employment lifecycle. Currently, the state Office of Administration's provisioning system automatically processes HR actions and creates or manages networking and email accounts for all employees.

"Since it went live a few years ago, we have realized significant efficiencies in account creation and management through the automated processing, a higher level of data integrity by the elimination of manual account creation, and an enhanced security posture by ensuring that user accounts are properly terminated when the user ends his employment with the commonwealth," he says.

On the other hand, Avakian admits that the IAM that Pennsylvania uses for its outside business partner populations (and its citizens) is decidedly "less mature." In an effort to extend the "pockets of security" here, his team is currently working on an initiative to allow citizens to conduct services with the commonwealth with a single, secure credential.

Avakian and his team in state government are far from the exception, and perhaps further ahead of the curve than many private enterprises or government agencies when it comes to beefing up their IAM processes and technology. According to Mark E.S. Bernard, principal for Secure Knowledge Management, while most of the more than two dozen critical infrastructure industries are obliged to follow compliance imperatives around IAM, "some industries still control access to classified information better than others."

Regulations help by imposing more structured requirements for access management, he adds, however regulations often miss basic layers, including role-based authorization to system resources and additional defense-in-depth techniques like the isolation of sensitive data and information assets based on a need-to-know.

However, even in more regulated and strictly controlled sectors, such as government, financial services and health care, information security teams have more recently stopped pushing back on their constituents' demands for access to work systems and documents through mobile or personal devices, or through their home or public networks, according to Terry Gold, founder of Boston-based D6 Research.

"Security executives have accepted that they can't have an argument that could inhibit business," Gold says. Instead, understanding that in many cases they still lack the "perfect" tools for the job, information security depart-

OUR EXPERTS: IAM

Erik Avakian, chief information security officer, Commonwealth of Pennsylvania.
Mark E.S. Bernard, principal, Secure Knowledge Management
Terry Gold, founder, D6 Research
Paul Hill, senior consultant, SystemExperts
Brett McDowell, executive director, The FIDO Alliance
Hugh Simpson-Wells, CEO, Oxford Computer Group

IAM

$18B

Estimated size of the IAM market in 2019.

– Covisint

ments are trying to assess how they can build better IAM systems to manage their increasingly expanding attack surface and find new ways to assert control and create defense-in-depth in these more open environments. In the meantime, unable to extend pre-existing controls, Gold says many organizations "essentially have more lax security."

Putting a positive spin on it, Brett McDowell, executive director of The FIDO Alliance, points out that it is a good time to work in enterprise IAM. On one hand, the problems are worse than ever as data breaches reach an all-time high, with more than 80 percent of these breaches attributed to compromised credentials. On the other hand, emerging innovations – such as biometrics and one-touch security devices that are based on open industry standards that are interoperable across most platforms, vetted by independent certification bodies and endorsed by some of the most trusted brands in technology who have already deployed the technology at scale – are becoming more readily available, McDowell says. "The stage is set for IAM managers to simply put these pieces together and look like heroes in the process," he adds.

Erik Avakian, CISO, Commonwealth of Pennsylvania.

Hugh Simpson-Wells, CEO of Oxford Computer Group, an IAM specialist, isn't so sure that it will be that easy. "There are still far too many companies [that] have more or less manual systems for managing [IAM]," he says, adding that a frequent comment he hears is "we have written a few scripts."

In particular, he finds that small companies in the throes of "becoming larger companies typically have not got a real plan, let alone implemented one. Of course, many larger companies have done a lot of work, but even these [larger companies] will typically not be managing permissions to any level of detail in their [line-of-business] systems, and many will have not have any kind of role structure, or even cross-platform support."

Ch-ch-ch-ch-changes

Other than the growing demands from users and an exponentially increasing access (and attack) surface, IAM professionals also need to weigh how high-profile ransomware and distributed denial-of-service attacks and other sensitive breaches – reported almost daily – are playing to these vulnerabilities in identity and access management. In short, it's not an easy nut to crack.

Case in point: McDowell's FIDO Alliance –members include the Alibaba Group, American Express, Bank of America, Google, Mastercard, Microsoft, PayPal, RSA and Visa – has been working since 2013 to deliver "open industry standards that address the problems," and are only now getting mainstream attention. While choices abound, finding an IAM solution to provide solid, reliable security across diverse front-ends is tough.

For example, McDowell points out that "biometrics offer great usability but can be spoofed; shared secrets, like passwords, aren't really secret anymore; one-time-passcodes over SMS are easily intercepted; and end-users are easily tricked by modern sophisticated social engineering."

Indeed, since hackers recently demonstrated that they could crack two-factor authentication, IAM teams have been unsure of the most effective approach, according to Bernard. "For several years, organizations have been instructing both operational and development teams to integrate two-factor, but now that it is broken they will look at other means of authentication such as biometrics," Bernard says.

$20B

Estimated size of the global IoT IAM market in 2022.

– Market Research Futur

Nothing is 100 percent secure and this extends to any countermeasures that have been chosen to protect classified information, Bernard says. The integration of biometrics will bring on new risks that put humans directly in harm's way due to emerging global privacy regulations and personally identifiable information, he continues.

In the past year, Avakian's team in Pennsylvania implemented technologies, such as multifactor authentication, for employees to access enterprise applications, such as email and Microsoft Office 365. The shift to using multifactor authentication on such a scale was primarily driven by the challenges "we have all witnessed related to the cybersecurity threat landscape as well as from the increased use of cloud, [software as a service], and services as email and file storage," Avakian says. In the near future, Avakian plans to use multifactor authentication to validate Pennsylvania's citizens and business partners too.

Mark E.S. Bernard, principal, Secure Knowledge Management

"The use of third-party identities (such as Google) or social media sites (such as Facebook) for access to applications has also been increasing," Avakian says, adding that this trend offers the advantage of offloading routine account management to a third party. "The user is less likely to forget their credentials as they use this identity on a daily basis," he adds. "We've seen the private sector, including retail, take advantage of this approach."

For his part, Paul Hill, senior consultant with SystemExperts, sees what he calls "a bifurcation in the identity management market." On one hand, there are a large number of traditional companies that are using familiar tools, such as Microsoft's Active Directory, expanding its use to their cloud deployments on both Amazon Web Services and Azure, he says.

"On the other hand, there are also a number of companies that are more distributed, the network perimeter is blurrier," Hill continues. This latter group tends to have no on-premise servers, infrastructure is in the cloud, large portions of the staff may never visit the corporate offices, and many of these organizations may use dozens of SaaS platforms for different business functions, he explains. In these companies, identity management is often outsourced or the companies use a centralized repository for at least some of their IAM services.

Seeing the demand and opportunity in the market, Gold says that mobile products vendors are starting to look at supporting more challenging security models that, until recently, they were resistant to tackle due to the lack of alignment, understanding and complexity in the market. "One such area is supporting actual public key infrastructure for much stronger authentication, authenticity and protection measures that enterprises increasingly desire as protecting the data and communication becomes more of a priority," Gold says, adding that this is "a logical next step for organizations that have already hardened access to start implementing kill chain layers to address the realization that keeping the bad guys out all the time isn't realistic and [enterprises] need to have measures in place assuming they may already be in."

Herding cats (with credentials)

Fighting the rising tide of attacks, especially those executed with misappropriated credentials, IAM professionals are waging wars on multiple fronts to both stem the flow of losses and also improve their methods for authenticating users, third parties, partners and customers long term. It does not help the

62%

Percentage of users who changed a password after a data breach.

– Gigya

situation that no matter how wily and sophisticated enterprises are becoming, cybercriminals are finding new ways to get around these safeguards and protections. Case in point: McDowell says many people he knows in enterprise IAM are concerned over scalable malware attacks and phishing attacks that harvest credentials. "But even more innovative firms are seeing how voices, fingerprints and even iris patterns can be spoofed by diligent attackers."

Further, Hill says that he is rarely seeing improvements in asset management, device authentication and knowledge-based authentication, especially in companies that operate in a more distributed environment. Many companies that have adopted bring-your-own-device, he says, do not even have a formal registration process or a method to associate a personally owned device with an employee or customer, which further complicates and confounds secure authentication. Products aimed at solving these issues have yet to be widely adopted, he says.

Terry Gold, founder, D6 Research

"More traditional, heavily regulated market sectors that are slowly moving into the cloud are the ones most likely to adopt new controls to tackle these problems," Hill says. "But I fear that in many cases, companies are adopting newer architectures, but not adopting the additional controls necessary to properly identify compromised accounts or devices, which will result in more undetected breaches."

In Pennsylvania, the executive branch consists of more than 40 agencies, departments and offices, many of which have an online presence to interact with the public via custom created applications, Avakian explains. "Over the years, these separate agencies have developed their own IAM systems with private user stores and inconsistent implementations," he says. "A citizen attempting to interact with different agencies or different aspects of government needs to register and maintain multiple accounts and may only interact with that agency infrequently."

As a result, Avakian says the state's constituents or partners often forget their individual identity credentials and they are forced to reset their account or even recreate it, which has "led to a less than seamless end-user experience when a citizen does business with the commonwealth."

In particular, the issues of cloud computing, increasing third-party access and controls, and key management are really changing the game in IAM, according to Gold. "Key management really comes down to those organizations that believe that they need to protect their data and communications, not just the access to them," he says. "As legal experts in health care say, 'the only way to ensure that data is completely protected is to either delete or encrypt it'."

"After all, implementing encryption is easy, doing it well is very difficult," Gold adds.

While implementing encryption is becoming more accessible, organizations still must fully understand their industry and internal policies and regulations to make sure that the product that proposes to make it simple can do just that, Gold says. "Many solutions will skip steps to get to simplicity, which can compromise the strength and integrity," he points out. The challenge specifically in mobile is that sound encryption requires storage of key material, and mobile handset vendors and operating system developers generally place many restrictions from storing this key material in a manner that most key management experts would agree is the most secure or manageable and scalable, according to Gold.

10%

Percentage of cybersecurity professionals who believe username/password is still adequate authentication.

– Enterprise Strategy Group

The need to support legacy systems, another prominent issue in many heavily regulated and distributed industries (like financial services, government and health care) poses a huge obstacle to better IAM development because, as Simpson-Wells puts it, "these systems are not necessarily built to make use of best practices here." For example, many legacy systems use shared accounts, have only basic logging, and do not support modern protocols that increase security and allow for integration with enterprise and federated identity systems.

Hugh Simpson-Wells, CEO, Oxford Computer Group

"Even when the systems involved do support modern approaches, the management is too often distributed across the organization – identity and access for SAP by the SAP team, and for Oracle by the Oracle team, for Microsoft by the Microsoft team," according to Simpson-Wells. "This approach does not protect well against security and compliance problems arising from cross-platform segregation of duty failures. Especially with the increasing use of cloud apps and cloud-centric identity, this separation makes no technical sense either."

While Bernard points out that security architecture should play an important role with in-application development, the majority of enterprise applications are usually chosen for other reasons than their security capabilities. "IAM systems are bolted on after the fact as opposed to fully integrated from the operating system outward," he adds.

An explosion of endpoints

Building better, more secure access will be increasingly complicated by the exponential growth of endpoints and systems that need to be accessed, as well as the number of internal users and third parties that need to have ready access. For any IAM professional looking for things to ease up before they commit to implementing better controls, experts warn they better not hold their breath.

"BYOD is not a passing fad," McDowell says. "Personal devices accessing corporate assets will continue to grow in volume and importance, underscoring the needs for open industry standards as the basis for next-generation authentication so the enterprise can insulate itself from the choices their employees and customers make when acquiring those devices."

In addition, the widespread adoption of IP-enabled Internet of Things devices for mission-critical data collection will only exacerbate access concerns too. "In recent years, we have seen the source of so many credit card breaches traced back to the point-of-sale devices," says Hill. "I expect that in the future we will see many more breaches traced back to the use of IoT devices instead of web servers on fully fledged managed platforms."

For IT security professionals like Avakian, "business identity management has moved to the forefront." Seeing the dramatic increase in the use of BYOD, he believes most organizations have started embracing a remote workforce to one degree or another. And, with the absence of a defined perimeter, he adds "it's all about identity, which surely becomes the driving force behind secure transactions and interaction." ■

For more information about ebooks from SC Media, *please contact Stephen Lawton, special projects editor, 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.

93%

of organizations surveyed are running applications or experimenting with infrastructure-as-a-service.

– RightScale, "2015 State of the Cloud Report"

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 more than 90% of 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 EDITOR Stephen Lawton
stephen.lawton@haymarketmedia.com
MANAGING EDITOR Greg Masters
greg.masters@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*

RSA

BUSINESS-DRIVEN SECURITY™ SOLUTIONS

SECURE ACCESS IN A WORLD WITHOUT BOUNDARIES

PREPARE YOUR BUSINESS FOR TAKEOFF WITH RSA SECURID® SUITE.

Imagination. Ambition. Fearlessness. They're the jet fuel that launches businesses to new heights. Your identity management strategy should be the engine that keeps your business—and your users—soaring.

Reimagine your identity strategy with RSA SecurID Suite, the industry's most advanced identity and access management solution including multi-factor authentication that helps minimize risks and accelerate business. With RSA SecurID Suite, you're free to explore a world of limitless possibility.

rsa.com/reimagine