VERSION NEXT

# NOW

TEKSYSTEMS SECURITY ISSUE | DECEMBER 2019

# IDENTITY

## The critical shield to protecting the enterprise



# The Power of Identity

## If you do one thing, it should be this

**Information security is kind of like a referee. If a referee makes no mistakes, most fans won't even notice he's there.** Botch a call and suddenly the whole world is watching. Information security is a referee of sorts but most definitely a gatekeeper of the highest order. If a user or device passes muster, access granted. If they don't, access denied. Of course, like sports, the players of the digital world don't always play fair. Cybercriminals try to cloak their identities and run on the field. If they're successful, the whole world is practically watching as the victimized organization moves into breach recovery mode.

With a proliferation of devices and users trying to access systems, and a large army of hackers doing the same, companies need to focus attention on identity access management. This issue of *Version Next, Now* examines the importance of identity management in a digital game that has many losers. TEKsystems experts Steven Aleckson, Scott McCallum, Mike Mulligan and Kory Patrick, IDC security analyst Jay Bretzmann and SailPoint leaders Joseph Schramm and Steve Lewis, break down the why, what and how of IAM, hopefully providing a lens into the necessary steps to shore up data protection. If that's not enough, you can also learn a lesson from Chick-fil-A.

**Albert McKeon**
*Contributing Editor*

## FEATURES

### The Change Agent

As business continues transforming and adopting new technologies, the need for a strong IAM program has never been greater.

PAGE 6

### Market Perspective

A fireside chat with IDC analyst, Jay Bretzmann and SailPoint leaders, Joseph Schramm and Steven Lewis, who share their point of view on IAM's role in the business, best practices and common challenges, and evolving your identity strategy.

PAGE 12

### TEKsystems' Perspective

TEKsystems Risk & Security leaders, Steve Aleckson, Scott McCallum, Mike Mulligan and Kory Patrick, provide compelling insights and perspective on the critical importance of an IAM program.

PAGE 22

# THE CHANGE AGENT

**Every day, threat actors are working to penetrate your organization's perimeter and access unauthorized, sensitive and confidential information.**

# Protection Starts with Identity

Organizations are vulnerable to a range of threats: cyberattacks, malware, ransomware, theft and device loss, compromised passwords, phishing and even malicious attacks from the inside. Breaches are widespread. No organization is immune. Early detection is critical. With threats increasingly sophisticated, and as digital transformation and technology continue shaping how business gets done, many organizations have adopted a mindset of Zero Trust—a security discipline that holds nothing inside or outside the perimeter can be trusted, and everything must be first verified before getting access.

Information security is often the unsung hero in a business. If everything is performing up to expectations, the organization and its data remain protected another day—business as usual.

If any disruption to security or a significant data breach occurs, headlines are made and the potential damages are tremendous—from tarnished reputation and distrust to even lost revenue and customers. "In 2018 alone, 2.8 billion consumer data records were exposed at an estimated cost of more than $654 billion".[5] The stakes are incredibly high.

Identity is at the core of security. The need for a strong, well-thought-out and continuously implemented identity access management (IAM)* program has never been greater. Organizations that can seamlessly manage and maintain user access to business information and data will not only decrease the likelihood of a breach—and the financial, reputation and brand equity threats that accompany compromised data—but they will also eliminate service disruption, establishing a competitive advantage over their less-protected peers.

01

*Refer to Appendix for the acronym definitions.

## Why is IAM so important?

For as long as businesses have existed, identity has always been critical. But in today's digital revolution, identity has never been more relevant and necessary for a number of reasons.

### User Life Cycle

Every user is on a life cycle, from their first day at the company to their last. Users include full-time employees, vendors, consultants, contractors and even customers. It's critical to keep pace with the evolution and growth of the user, as they may assume new roles or take on different projects that require access to systems and applications they may need only temporarily. Effective IAM constantly adjusts and fluctuates permissions as the user and digital experience evolve over time. This ensures that users have authorized access to only the applications, systems and programs they need to do their jobs. It also ensures permissions are revoked when the user no longer needs access, thereby only sharing the minimum data and information that is required for business to keep moving.

*" Identity access management, or IAM is a program that manages identities of user populations typically in business through the identity life cycle and automates the process for granting access rights, changing those rights and, sometimes, auditing the appearance of inappropriate rights for a user's profile."* [8]

> ***7 out of 10*** *leaders have an IAM program in place at their organization.*[11]

## User Experience

IAM is happening behind the scenes, whether the user is aware of it or not. The three main systems used for IAM—SSO, MFA and PAM—have some level of automation built in. Products from companies such as Okta and Ping are designed to consolidate the number of passwords a single user has. Instead of requiring a manual sign-in when trying to access a program or application (e.g., logging into a laptop, checking paystubs, reviewing sales numbers), users have a frictionless, one-time sign-on user experience.

## Device Volume

Users are those who need some level of access to systems, applications, databases, physical locations or any other platform hosting information. With an increasing number of devices—including laptops/desktops, smartphones, tablets and wearables—at their fingertips, the reality is there are progressively more connected devices to protect.

## Sophisticated Attacks

While innovative technologies give organizations the ability to deliver solutions to their customers better, faster and more efficiently, this revolution comes at a price. Security breaches and attacks that take advantage of technology vulnerabilities can be more sophisticated and occur more often, underscoring the demand for tight security measures. By reducing the chances of data being compromised with a mature IAM program, organizations have the potential to save 40% in technology costs and an average of $5 million annually in breach costs, according to Forrester.[4]

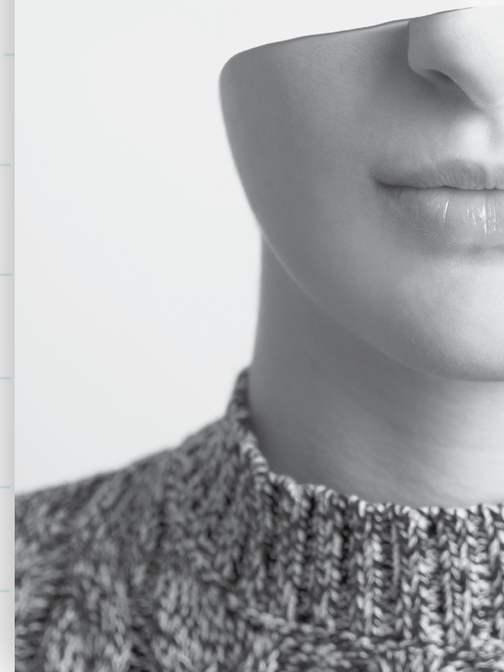
## Regulatory Landscape

GDPR and CCPA, two of the most recent data protection and privacy regulations enacted, have also changed the way companies manage data. Compliance is a lot easier with a solid IAM program.

> ***One-third*** *of leaders say lack of employee awareness poses the biggest cybersecurity threat to their business.*[11]

Digital transformation presents unique challenges for a security-minded organization. Companies strive to innovate and renovate, leveraging technology to improve the services they deliver and the speed at which they deliver them. While business-enabling technologies such as IoT, cloud enablement, mobility, analytics and AI present opportunities for organizations to reinvent the way they deliver value, these technologies need to be approached prudently in the business environment. An effective IAM program is a business necessity. Critical, sensitive and proprietary data is at risk. Protection isn't an option, rather a mandate.





# MARKET PERSPECTIVE

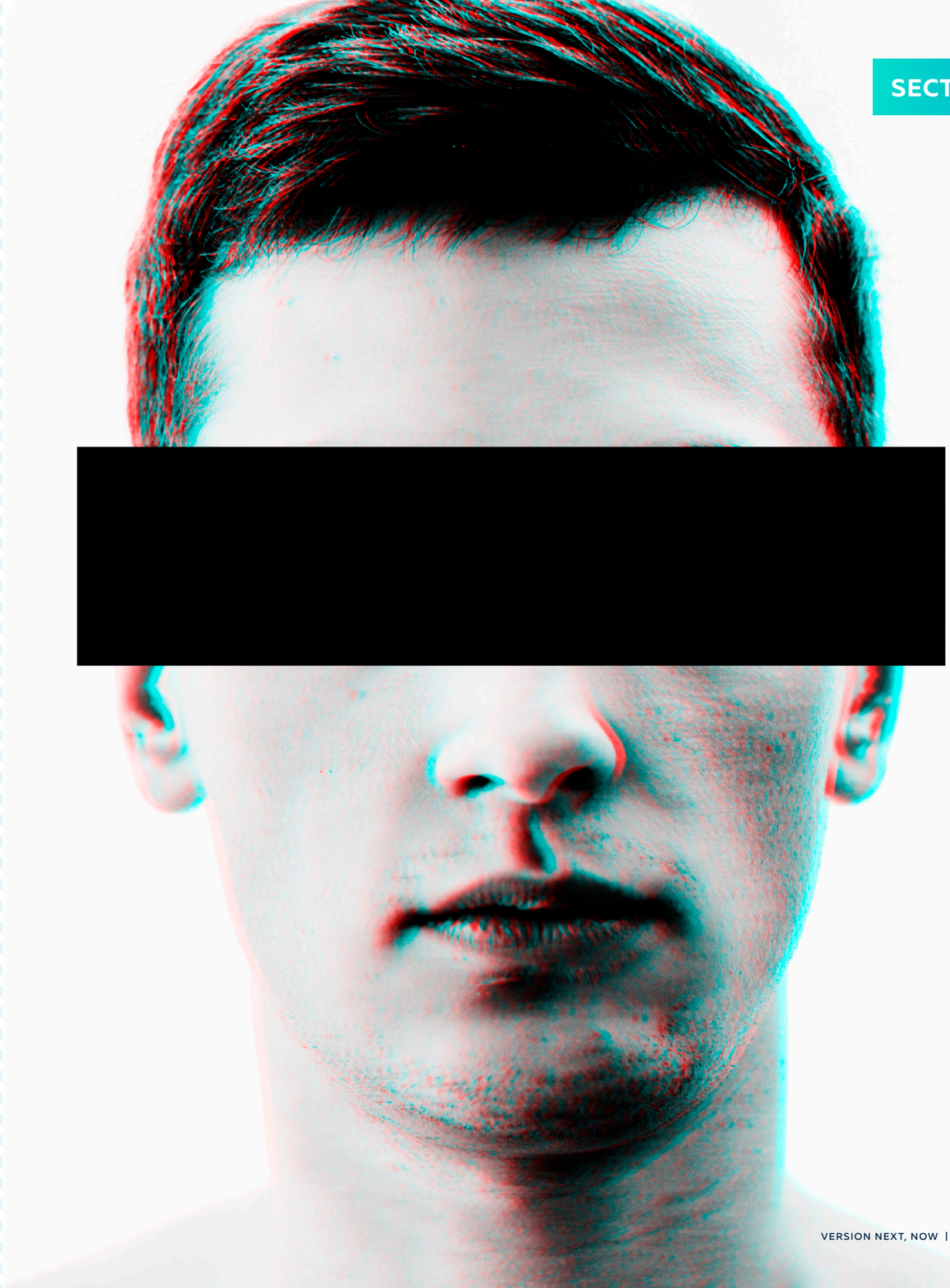
**Leaders from IDC and SailPoint share their point of view on IAM's role in the business, best practices and common challenges, and evolving your identity strategy.**

# Gatekeeper to Access

The International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services and events for the information technology, telecommunications and consumer technology markets. With a robust team of more than 1,100 analysts worldwide, IDC delivers informed analysis and insight to IT professionals, business executives and the investment community, enabling evidence-based technology decisions for their businesses.

SailPoint, the leader in enterprise identity governance, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies in a wide range of industries. IDC's Program Director of Security Products, Jay Bretzmann and SailPoint security leaders Joseph Schramm and Steven Lewis provide unique and informed perspective about IAM.

02



# Q + A

## How does IAM support the business's priorities?

Jay Bretzmann (IDC): You can think of IAM as one of the oldest IT controls ever developed. Anyone using a computer system was given an account and asked to create a login name and password. Most people were only allowed to process certain data collections using available programs. There were few concerns about system security.

Fast forward a few decades and IAM has become a cornerstone of any organization's digital information defenses. Glass houses and defined network perimeters no longer confine the data and processing resources used to conduct business. Those who can't control and monitor various types of users are exposing precious and private assets to anyone with the skills to access them. IAM systems should be the gatekeepers of access to both the back-office and front-office computer applications, including the ability to monitor and report *who did what* for internal accountability and external regulatory reporting requirements.

SailPoint: Business organizations are looking at a multitude of priorities. Those include, but are not limited to, transforming their digital infrastructure to a more cloud-oriented stance as opposed to on-premises, reducing risk in a more connected world and reducing operational expenses, especially those associated with governance and compliance. Mergers and acquisitions are important to execute correctly as well as spinning out subsidiaries into their own company. All these activities can benefit from a cybersecurity program based on an identity governance as the foundation.

Identity governance provides the secure foundation for all aspects of a cybersecurity program. An identity-aware approach to cybersecurity will help secure an organization as they work through one or more of the business priorities listed above. Organizations should be managing access for the people that employ their systems and data to do their job every day toward the "least privilege access" goal. This means ensuring that each person has only the access required to do their job—no more, no less.

# Q + A

## What common challenges do you see organizations trying to solve with IAM?

JB (IDC): The long and short of it is simply control of the business. Organizations can't effectively employ computers unless they limit access to defined user groups. The finance people don't need to be reading human resources materials and vice-versa. All of this just makes sense but defining an effective approach is a daunting task, and chances are that most organizations will impede user productivity along the way. It's generally easier to deny access than permit it when the goal is to protect the environment and easier to permit than deny when the goal is to maximize profits.

## With many products available in the marketplace, what best practices should organizations adopt in order to select the product that best suits their needs?

JB (IDC): Let's start with the idea that organizations are looking to upgrade or replace whatever they currently have because they must have something. Lots of smaller organizations start with something as simple as a spreadsheet of usernames and passwords. These simple solutions don't last long and end-up costing far more in terms of mis-spent IT staff time than they're worth.

Many other, larger organizations are using directory or domain controller services bundled-in with an operating system. Microsoft's Active Directory is the most prevalent example. This type of a solution works great as long as someone spends the time required to adequately configure it, but the reality is that most don't. Identity is hard, and most companies just don't allocate sufficient time and resources to correctly define it.

So, if there is an identity problem, it likely has to do with scale issues or documenting and reporting problems. If three out of five users request password resets every week because no one can remember what they invented, the IT or security staff is going to spend inordinate amounts of time just keeping people on-line. Three times ten is doable; three times a thousand isn't. Also, if the business needs to submit quarterly reports of who has access to private or sensitive data and when they processed what, it can become an arduous if not impossible task rather quickly.

Organizations need to clearly document what an IAM system must accomplish before they begin evaluating available options.

SailPoint: Organizations should look for vendors that lead their respective aspects of the cybersecurity program and work together both technically and in go-to-market motions. This reduces the risk associated with the whole program. If vendors work together and provide out-of-the-box integrations among each other's technologies, then an organization can focus on the business process that needs to be automated and not the technical bits and bytes of integration. Best-of-breed technologies that work together will go a long way to improving the program.

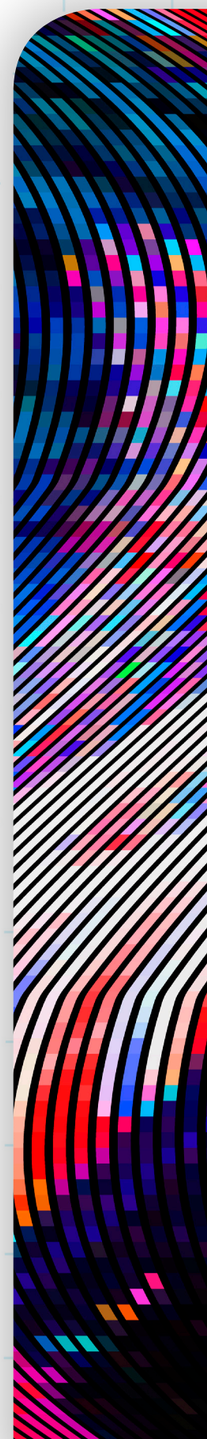
Q + A

## What are the main privacy considerations as organizations work toward their DX goals?

JB (IDC): Don't collect anything you don't need to collect and only store it for as long as it yields business value.

SailPoint: Identity information is just one aspect of the dataset that needs to be protected. Most regulation that concerns identity is common in its purpose. Protect the data that is involved with these sensitive processes. Nothing is perfect, but risks and costs can be reduced by taking a programmatic approach to any program. The alphabet soup of regulation exists because previous organizations were ignorant or willful in their disregard of data privacy. The result is a landscape of regulation that requires all organizations to take the proper steps to protect the data that is stored and used. Identity governance will help protect the identity aspect of organizational goals.

Q + A



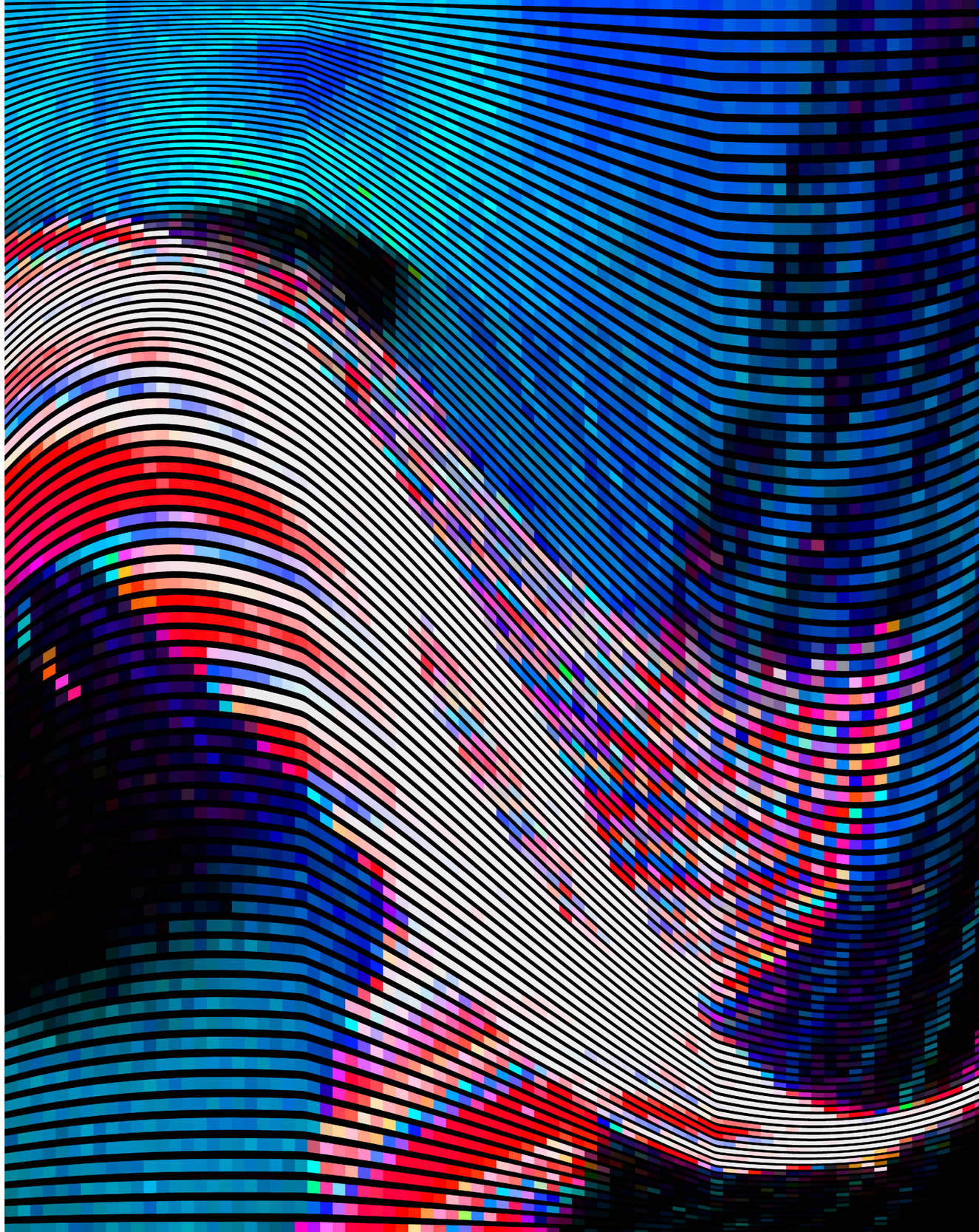
# Q + A

## What do you recommend to organizations who are trying to evolve or expand their IAM programs?

JB (IDC): Firstly, plan for the future and figure on dealing with one or more millions of users. If the business doesn't currently sell directly, chances are it will someday down the line. We all want to know our customers better and tracking their behaviors is important. Few legacy solutions were designed for B2C capabilities and rip-n-replace due to scale issues is not only costly, but disruptive and simply aggravating to all parties.

Secondly, acquire a technology that will permit user data collection and monitoring. The days of username, password, IP and MAC addresses as the only required criteria are gone. People access the network using multiple devices and your ability to assess risk is directly proportional to what you know about someone's behaviors, locations, and job responsibilities. Authentication should not be a binary activity, but something done continuously depending upon their activities and the severity of any network or data breach.

SailPoint: The constant evolution of a cybersecurity program is important to acknowledge and manage. These programs are complicated yet yield value that is greater than the overall cost. Working with a trusted advisor that can help steer and update the program throughout its life will go a long way to improving the success of the program. Some organizations think that they can manage the program on their own. It is our experience and opinion that organizations need to focus on their business and work with a partner that specializes in these programs. Technologies mature, regulations change, businesses grow and priorities shift. Being able to manage this landscape will help an organization evolve the program and the technologies associated with the program. Priorities may shift, which may impact the order in which the technologies get implemented. Merger and acquisition activity can materially affect the program as personnel and technologies may change as a result. Having a consistent hand guiding a program will reduce the risk of program failure as these things change.



# OUR PERSPECTIVE

**TEKsystems Risk & Security leaders, Steve Aleckson, Scott McCallum, Mike Mulligan and Kory Patrick, provide compelling insights and perspective on the critical importance of an IAM program.**

# Identity: The Holy Grail

Privacy and security are achievable with an IAM program that keeps people from getting access to the wrong data, systems and applications. "IAM programs help organizations streamline manual identity workflows and processes, ultimately helping them be more efficient with their security," explains TEKsystems Risk & Security Executive Director Steve Aleckson. "And it's not just protecting information. It's also about enabling employees from day one. Getting them access to what they need in a new role so they can be up and running right away," says TEKsystems IAM Product Line Lead Scott McCallum.

One of the most common challenges organizations face is underestimating the complexity and scope of IAM. It needs to be thought of as a never-ending program—not a one-time project or task. "The reason you see challenges in this space is because people don't have a program; they buy a product and then they try to build a program around the product. They don't think of it programmatically," says TEKsystems Risk & Security Practice Manager Kory Patrick. IAM consistently strives to secure the organization.

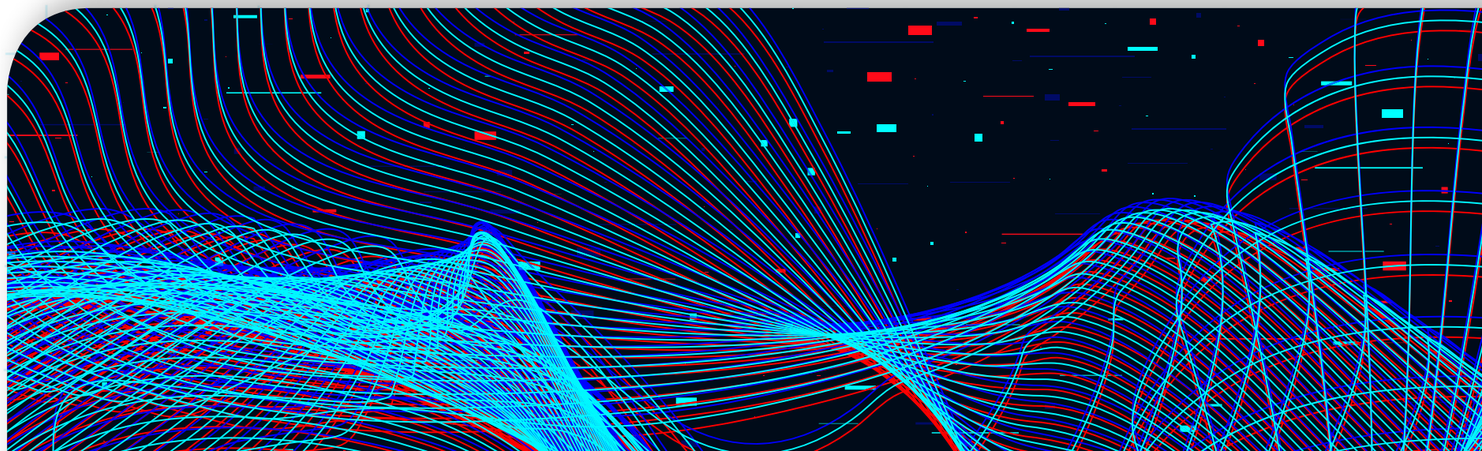
It's worth noting the IAM landscape continues to evolve, and the cloud drives a lot of that change. As customers search for solutions that reduce hardware spend, an increasing number of cloud-based tools and technologies are emerging in the marketplace. "Cloud isn't necessarily changing the way we do IAM; cloud is *forcing* us to do IAM—because identity is really one of the last things that an organization still remains in control of as they move their infrastructure or platforms or even software-as-a-service to the cloud," says Patrick. In a strictly on-prem environment, organizations could make less of an investment in identity. But once the cloud became a factor, identity became the one thing you can—and must—tightly control.

Technologies are driving transformation and innovation across the enterprise. It's not limited to the cloud. "Digital transformation has made the security professional's world a lot more difficult because there are more surfaces to protect," says TEKsystems Risk & Security Practice Executive Mike Mulligan. "In theory, that's better for the consumer, better for the customer and better for the user of said technology, but it creates a tremendous amount of technology and security challenges because that means more things need to be accessed and provisioned, more things need to be protected with IAM."

> *IAM programs help organizations streamline manual identity workflows and processes, ultimately helping them be more efficient with their security.*
> *– Steve Aleckson, Risk & Security, TEKsystems*

It's essential for organizations to create a strategy built around the security products purchased. Otherwise, organizations run the risk of an out-of-the-box technology solution that ultimately doesn't meet the needs of their business. "One of the biggest mistakes companies make is choosing a tool without knowing all the business requirements of the organization," says McCallum. This could also result in stitching disparate products together—which creates a separate set of challenges. Without the right people with product-specific expertise, organizations don't know how to support the tool they just purchased. "I've also seen customers trying to make the wrong tool work," Patrick adds. "It boils down to perception. They were sold this tool that's going to solve all their problems, but that's just not the case. Tools are tactical, not strategic."

03



# TEKsystems' Tips: A Programmatic Approach to IAM Confidence

Align IAM goals with business outcomes. IAM deployments should be based on business priorities.

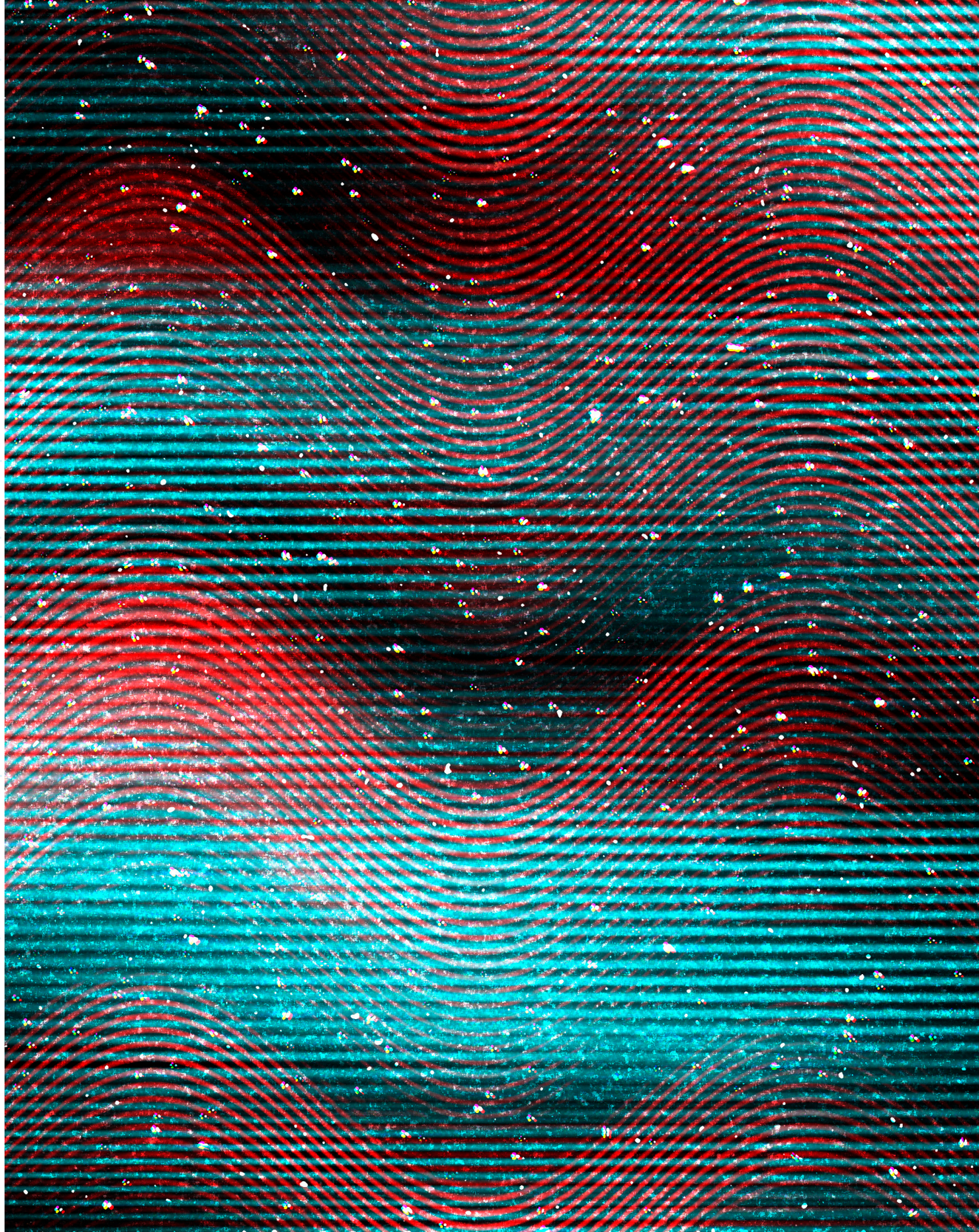
IAM is complex and requires planning and preparation. Don't overlook the importance of data cleansing, business process reengineering and building the right team.

IAM is a program—align your business strategy to your tactical execution. Don't purchase a tool without understanding the full business requirements and needs of the organization.

Tools are tactical, not strategic. Don't try to force a product to fit your business needs.

Secure buy-in from the appropriate stakeholders. Think holistically and consider the impact of your IAM program across the enterprise—including how it impacts HR, help desk, compliance, IT and security.

> ***Only about half*** *of leaders believe that their company's security strategy and business strategy are fully aligned.*[11]



# Real-World Application: Chick-fil-A

The multibillion dollar fast-food restaurant chain Chick-fil-A has grown to more than 2,000 locations across North America.[6,7] They required a scalable and secure identity solution that would reduce their footprint and dependencies on legacy systems, like Active Directory (AD).

In 2000, Chick-fil-A installed AD, which provides services and use cases—including access management of users/credentials, workstation authentication, control of file access and group permissions, group policy objects and email. From humble beginnings of just a single domain and eight domain controllers, the AD became too expensive as its user population expanded to 50K+ users—significantly increasing in complexity.

While using AD, the company introduced a web portal into its environment in 2004, creating a .NET sync engine to move identities from the HR system into AD. The restaurant chain was using the web portal and web application security for authorization while still maintaining AD for authentication.

Three years later, Chick-fil-A invested in Oracle Identity Manager (OIM) to replace its sync engine, which had become difficult to manage. Realizing the value and need for a cloud-based identity solution, Chick-fil-A engaged with Okta—the leading independent provider of identity for the enterprise. Since 2017, Chick-fil-A has integrated Okta's authentication, SSO and MFA capabilities across its applications, which has enabled them to reduce their footprint with legacy authentication apps.

"Now that we've moved authentication over to Okta, we've got really good visibility into the attacks we're getting from a global perspective against our Office 365 tenet, and by turning off that legacy protocol, we've eliminated a lot of those attacks," says Ryan Walker, senior principal team leader, identity & access management, Chick-fil-A Inc.[7]

# Meet Our Contributors

### Steve Aleckson, Executive Director – Risk & Security Practice, TEKsystems

Steve Aleckson has more than 24 years of business development and resource management experience at TEKsystems. He's focused on developing executive relationships while increasing revenue and profitability at local branches, as well as national programs. Steve leads TEKsystems Risk & Security, partnering with customers to maintain the right balance between managing risks, complying with regulation and maintaining security through resource, outcome and advisory services.

### Scott McCallum, Solutions Architect & IAM Product Line Lead, TEKsystems

Scott McCallum is a seasoned IT security professional specializing in enterprise IAM solutions with a focus on customer-facing roles. Scott has an extensive background in identity, access management and privileged account risk mitigation while working for companies such as BeyondTrust, Dell, Novell, Oracle, Quest Software and One Identity. He currently holds the CISSP and Security+ certifications.

### Mike Mulligan, Practice Executive for Risk & Security Services, TEKsystems

Security executive Mike Mulligan has been in the tech industry for nearly 25 years and has experience overseeing sales and delivery strategies. He helps customers solve technology and workforce challenges related to data center, network infrastructure and security. Prior to his current role, Mike worked in a variety of capacities at TEKsystems, starting as a technical recruiter, then growing into roles including senior account executive and director of network services and regional director of divisional sales.

### Kory Patrick, Risk & Security Practice Leader, TEKsystems

Kory Patrick is an information security professional offering more than 19 years of experience in designing, developing and managing cybersecurity projects in both public and private sectors. Kory possesses a strong background in threat analysis, vulnerability assessment, crisis management, implementing effective security controls, digital forensics and incident response (DFIR), and technical operations with a deep understanding of information security from multiple perspectives.

### Jay Bretzmann, Program Director of Security Products, IDC

Jay Bretzmann is Program Director for IDC Security Products responsible for Identity & Digital Trust and Cloud Security. Jay focuses on identity management, privileged access management, identity governance, B2C identity management and a multitude of other identity and cloud security topics. Previously, Jay was director of marketing for a data protection startup (SecurityFirst) and the long-time worldwide product marketing lead for IBM Security QRadar. Joining the team after IBM's acquisition of Q1 Labs, he was there through the rapid expansion of the security solutions portfolio, managing launch activities for add-on products including vulnerability management, Network Insights, UEBA, App marketplace and QRadar as a Service.

### Joseph Schramm, Head of Americas Partner Sales, SailPoint

Joseph Schramm brings over 25 years of experience in a variety of alliances and business development roles. In his current role at SailPoint, Joseph heads partner sales for all channel & alliance partners in the Americas. Prior to joining SailPoint, he was Vice President of Global Alliances and Channels for BeyondTrust. In addition, Joseph has developed and led partner programs for various high-growth security and technology companies including Core Security, Endeca, BusinessObjects / Crystal Decisions and SAP.

### Steven Lewis, Senior Sales Engineer, SailPoint

Steven Lewis has been with SailPoint for seven years and currently serves as the senior sales engineer, overseeing pre-sales and channel related activities.

## TEKsystems Risk & Security Portfolio

**Core team with expertise** from critical venues including the FBI, top OEMs, top financial institutions and top audit and compliance entities

**2,800 consultants** in the Risk & Security Services group

**Process-driven approach** enhanced by certified partnerships with major OEMs

**Community-centric** approach in each of our 120+ offices in North America

**In good company**

Transformational technologies demand equally transformative partnerships. TEKsystems has strategic partnerships with major OEMs and is proud to deliver product-agnostic security solutions that meet the unique needs of our customers.

*The views and opinions expressed in this publication are those of the authors and do not necessarily reflect the views of TEKsystems, Inc. or its related entities.*

# Appendix

*Acronyms organized alphabetically*

**IAM (identity and access management, identity access management or identity management):** A program that manages identities of user populations "typically in business through the identity life cycle and automates the process for granting access rights, changing those rights and, sometimes, auditing the appearance of inappropriate rights for a user's profile."[8]

**CCPA (California Consumer Privacy Act):** Enacted in 2018, CCPA "creates new consumer rights relating to the access to, deletion of, and sharing of personal information that is collected by businesses."[9]

**GDPR (General Data Protection Regulation):** Approved by the European Union Parliament in 2016, GDPR is a regulation focused on data privacy and protection of all citizens in the EU. It took effect in 2018.[10]

**MFA (multifactor authentication):** "An authentication methodology that involves three categories of factors—something the user knows (e.g., password), something the user has (e.g., ATM card or token), and something the user is (e.g., biometric characteristic such as a fingerprint)."[8]

**PAM (privileged access management):** A segment of the Identity market that "focuses on user accounts not assigned to a normal user—superusers, shared accounts, service accounts, and so forth."[8]

**SSO (single sign-on):** A streamlined approach and capability to authenticate and log in to multiple systems, programs and applications through a one-time login.

## About TEKsystems

We're partners in transformation. We help clients activate ideas and solutions to take advantage of a new world of opportunity. We are a team of 80,000 strong, working with over 6,000 clients, including 80% of the Fortune 500 across North America, Europe and Asia. As an industry leader in Full-Stack Technology Services, Talent Services and real-world application, we work with progressive leaders to drive change. That's the power of true partnership.

TEKsystems is an Allegis Group company.
TEKsystems.com

## Albert McKeon, Contributing Editor

Albert McKeon has written an estimated 5,000 articles and has received leading journalism industry recognition, including the New England Press Association's Journalist of the Year honor. He writes for magazines and news services and creates content for organizations.

## Listen Now

Don't miss Kory Patrick's appearance on The Agile World podcast. Host, author and industry expert Greg Kihlström asks Kory about the evolution of the IAM market, IAM best practices and privacy considerations as organizations work toward their digital transformation goals.

## Be in the Know

Check out previous issues and what's next: Version Next, Now

## Follow Us

## Sources


1. Market Analysis Perspective: Worldwide Identity and Access Management, 2018 – The State of Identity, **IDC**
2. What is Identity and Access Management and Why is it a Vital IT Security Layer?, **BeyondTrust**
3. Security Intelligence Podcast: Zero Trust and the Evolving Role of Identity and Access Management, **IBM Security**
4. Stop The Breach: Reduce The Likelihood Of An Attack Through An IAM Maturity Model, Forrester
5. U.S. Consumer Data Breach Report 2019, **ForgeRock**
6. Increase Business Agility by Reducing Your AD Footprint, **Okta**
7. Minimize AD Dependency As You Move to the Cloud, Okta – **Oktane19**
8. IDC Market Glance: Identity & Trust 2019, **IDC**
9. California Consumer Privacy Act (CCPA), **Office of the Attorney General of California**
10. EU GDPR Portal, **EUGDPR.org**
11. TEKsystems Risk & Security Survey, November 2019, **TEKsystems**



TEKsystems
Own change