ISSN 2644-237X
MAY - 20 - 2020

# CIO Review

The Navigator for Enterprise Solutions

UK & EUROPE SPECIAL

CIOREVIEW.COM

IAM EDITION

Jiří Formáček,
Founder and CEO

## GreyCorbel Solutions

# TURN THE WEAKEST LINK INTO A SECURITY WEAPON

$ 15U S
22
0 74470 91626 0

Photo by Alev Takil

Is a hacker able to access priveleged accounts in the internal network and misuse your company data?

90% of cyber attacks are caused because of insufficiently secure accounts.

There is a way to prevent this.

The AdmPwd.E security solution will protect your data!

WE PROTECT YOUR DATA IN 17 COUNTRIES ON 4 CONTINENTS, AND KEEP MORE THAN 100 MILLION COMPUTERS SECURE

*greycorbel.com/admpwd-e* *office@greycorbel.com*

GreyCorbel

# Would you like to better monitor and manage regulations, standards and requirements?

compliance & risks

Since 2002, we've been helping companies mitigate risk, drive efficiencies and focus on growth opportunities via C2P, our compliance knowledge management platform and other solutions.

To find out more about how Compliance & Risks can help you to better manage your product compliance, visit **www.complianceandrisks.com**

**We help companies to:**

- Save time and reduce costs across your compliance functions
- Change the compliance mindset from being a cost center to a profit and growth center
- Preserve corporate memory through the use of a single platform

E: info@complianceandrisks.com www.complianceandrisks.com

# CONTENTS




## IN MY OPINION 08



## LAST WORD


## CXO INSIGHTS





## CIO INSIGHTS



CIOReview

Managing Editor
Justin Smith

Editorial Staff

Aaron Pierce Shirley Faith
Carolynn Walters Russell Thomas
Dean Winchester

Visualizers

Scott Juasy Issac George

Sales

Stephen Thomas
stephen.thomas@cioreview.com

Contact Us:

Phone:510-230-0395
Fax:510-894-8405

Email:
sales@cioreview.com
editor@cioreview.com
marketing@cioreview.com

CIOReview
May - 20, 2020, Vol 09, Issue - 22 (ISSN 2644-237X)
Published by ValleyMedia, Inc.

To subscribe to CIOReview
Visit www.cioreview.com



**Some of the Insights are based on the interviews with respective CIOs and CXOs to our editorial staff*

# Editorial

# The Future of Identity Management is Upon Us

Identity is the core building block of a robust 'Zero Trust' security ecosystem and infrastructure. However, the growing scope and complexity of modern identity environments is becoming too difficult to manage in the usual ways. This change in the status quo now requires IT leaders to evolve their identity and access management (IAM) environment. The move to the cloud, the adoption of microservices architectures, the digitalisation of the modern world, and the resulting growth in cyber threats continue to expand the use cases for IAM.

The future of innovation in IAM includes increased use of biometrics, the blockchain technology used in identity management systems, IAM for cloud services, and edge computing with IoT devices. It is, therefore, necessary for security and risk management technical professionals in the IAM landscape to focus on the trends of password-less authentication, value-driven IGA, increased consumer privacy mandates, and hybrid/multi-cloud environments.

In this edition of CIOReview, we bring you the story of some of the most successful IAM solution providers in Europe that deliver the best outcomes for their clients. This issue also offers a combination of thought leadership from subject-matter experts with real-life stories on fostering robust partnerships and exclusive insights from CIOs and CXOs. We hope this edition will provide you with the right assistance in choosing the best IAM solution providers according to your requirements.

Lets us know your thoughts!

Justin Smith
Managing Editor
editor@cioreview.com

MobiWeb
Making the world seem smaller!

Your ideal identity and authentication communication partner

Utilize two-factor authentication with one-time pins via SMS for user authentication and transaction authorization.
Secure your business operations and reduce fraud costs.

## SMS Messaging

Reach your customers globally via SMS, send notifications and one-time pins through one single API

## OTP SMS

End-to-end API solution for one-time pin generation, validation and delivery via SMS.

LE FONTI AWARDS
WINNER 2018

GSMA
Associate Member

www.solutions4mobiles.com

**Europe**
UK +44 203 318 3618
Greece +30 211 800 3325
Georgia +44 203 318 3618

**Asia**
Hong Kong +852 580 84070

**North America**
USA +1 702 608 8531

MobiWeb
Making the world seem smaller!

sales@solutions4mobiles.com

Ian Glazer

# PROFESSIONALIZATION OF IDENTITY MANAGEMENT

**By Ian Glazer,** Founder & President, IDPro

Within the enterprise, the relationship between privacy and security gets rightly deserved attention. But neither privacy nor security professionals can fully address the challenges presented to them, because their default toolbox is incomplete. The tools they are missing are the stock-in-trade of the identity and access management professional - the very peers that are frequently excluded from the conversation. Digital identity is the primary way that privacy professionals operationalize the controls they need ; in particular the governance of who has access to what information. Furthermore, identity provides indispensable context to security professionals to help understand who is doing what. Identity's voice is missing from the table and this is most unfortunate. I believe this is in part because, unlike the privacy and security industries, identity has fully not professionalized.

This is by no means to suggest that identity and access management practitioners are not professional in their approach: far from it! Consider, however, that privacy and security have professional organizations dedicated to the betterment of their industries and of those who work in them. These organizations provide a range of support, including professional development, shared good practices, certifications, forums for interaction, and provide a collective voice for their members

Where can the identity management practitioner turn for advice? Vendors and implementation partners certainly can educate us about their products and approaches - and many of them do a very good job. Analyst firms can inform us about the market and in some cases, system designs and architectures. Local user groups can help as well. But this is a piecemeal and often biased approach.

This lack of professionalization has real impacts on the identity industry - and, by extension, the business customers and consumers it serves. First, learning about digital identity is a long process. Most identity professionals I speak with share a similar origin story: they learned a specific product, then another, then another, and then had the experience and vision to generalize their knowledge. As a beginning identity professional, you often learn one vendor's user provisioning tool, another's a federation tool, and yet another's a privileged account management tool. And only with years of experience under your belt do you begin to fully understand identity management as a cohesive whole or even begin considering yourself as an identity professional.

One of the reasons why learning to become an identity professional is so time-consuming is because there is no vendor-neutral body of knowledge for the industry. Without such a body of knowledge, it is difficult and time-consuming to build a new identity professional -- a problem compounded by the fact that there are no identity management curricula at the undergraduate level. Unless your organization is a professional services company, the best you can do is very likely to hand a new hire a vendor manual, point her to a few blogs, and hope Stack Overflow and LinkedIn have some answers.

Second, to become a great identity professional requires interacting with your peers and, hopefully, finding a mentor. But that discovery process isn't straightforward. If you are lucky, there is an identity and access management meetup in your city. If you are not, you might find a helpful group online. But even then, your interactions will likely be infrequent, tactical rather than strategic, and so insufficient to accelerate the development of your own career.

In 2017, IDPro, the professional organization for identity, was formed to tackle these challenges and more. A non-profit, member-driven organization, IDPro provides a clearinghouse of identity meetups around the world so professionals can meet one another. It has a master calendar of identity-related events so that people can attend and learn. It offers an online forum where professionals can help one another. And IDPro publishes a monthly newsletter written by professionals for professionals with topics ranging from the identity of bots to the privacy implications of identity management.

> "Identity professionals are looking beyond current enterprise funding cycles and priorities to where the next challenges lay"


IDPro is in the process of building a body of knowledge. Identity professionals from around the world are volunteering to help shepherd and write sections of a vendor-neutral living document that, in the future, will serve as the basis for professional certifications. As the body of knowledge coalesces, the membership has built an annotated bibliography of works that the members feel have been useful to them as they have grown as identity professionals.

Lastly, IDPro has, since its inception, conducted an annual Skills and Programs Survey. Among the questions we asked were: 'what are the top priorities for your enterprise in the next 18 months' and 'what areas are you interested in learning about in the next 18 months'. The top 3 priorities for the enterprise were multi-factor and strong authentication, privileged access management, and user provisioning and lifecycle management. Interestingly, those three areas scored poorly in terms of individuals' priorities; at the same time, the IDPro survey data revealed that a majority of respondents had experience in all three areas.

When asked about their own areas of interest, respondents identified API protection, blockchain (or similar) identity, and identity for IoT and Connected Device as the top 3 areas they want to learn about in the next 18 months. Of those, only API protection was highlighted as an enterprise priority by more than 10% of the respondents. This indicates that identity professionals are looking beyond current enterprise funding cycles and priorities to where the next challenges lay.

The one area in which enterprise and individuals' priorities and interests were aligned was customer identity and access management (CIAM.) About 20% of respondents identified CIAM as a priority for their business and an area of individual interest in the next 18 months.

For a CIAM program to be successful in the long term requires that the enterprise puts the customer at the center of its thoughts, designs, and service. Perhaps more than any other business initiative, CIAM requires that identity, security, and privacy professionals work together in support of stakeholders from all parts of the business to deliver services which respect and delight the customer.

The professionalization of identity management won't guarantee your CIAM endeavor - or any other business objective - will be a success. But it will help to find, build and strengthen identity professionals who can be productive peers to your privacy and security teams. And that can only be a good thing. CR

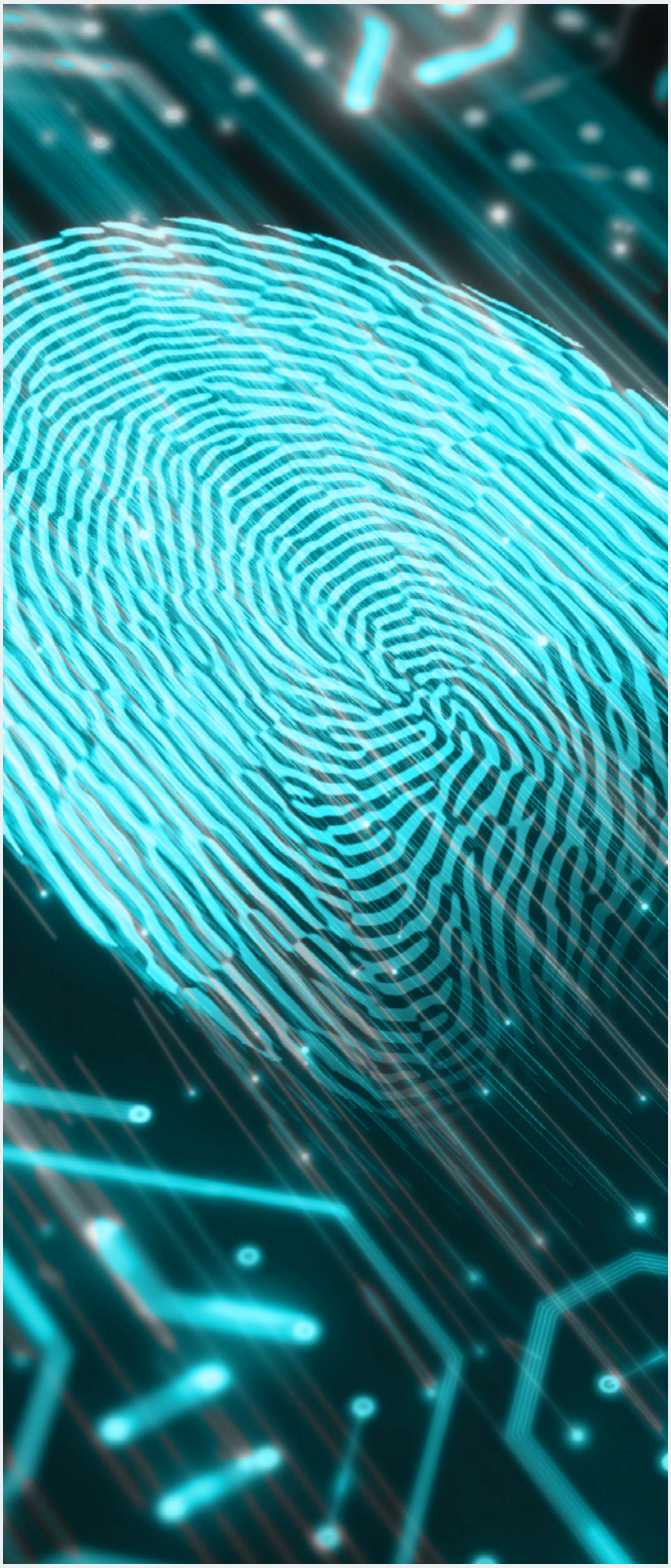
# TECHNOLOGIES TRANSFORMING THE IDENTITY AND ACCESS MANAGEMENT MARKET

With software organizations distributed worldwide irrespective of the boundaries, the end-users of their software products can possibly be from different geographical areas. This action of gaining access by various parties or users is not safe when some illegal users try to accomplish the same. So, organizations look forward to safeguarding their information assets against the threats of criminal hacking, phishing, and other malware attacks. In that regard, identity and access management (IAM) is fast emerging to help organizations set the precise mechanism while avoiding unwanted exposure of sensitive information. Identity and Access Management refers to the process employed by organizations and businesses to allow the right individuals to access their resources while deterring others from entering their environment, thereby securing their systems.

IAM is an IT security measure that comprises of policies, protocols, and procedures at various organizational levels, thus imposing strict monitoring and protection. Almost, all the sectors ranging from finance to healthcare use IAM to comply with best compliance standards to protect their business records. When IAM can protect enterprises, it can also enhance their productivity. IAM verifies user access requests and decides whether to grant or deny permission to authorized business data. Thus IAM systems provide organizations with technologies and tools including password-management tools, reporting, monitoring apps provisioning software, identity repositories, and security-policy enforcement applications to track user activities. With the rise in the end-user security threats, organizations should adopt the latest technologies in IAM to accommodate the complexities of the existing computing environment. Here are the current IAM trends in the market.

## MOVING IAM TO THE CLOUD

Almost 95 percent of organizations are already deploying their applications in the cloud and it is no wonder IAM is being migrated to the cloud as well. It is one of the most prominent trends because these tasks are usually handled in the backend, which gives the IT team time to manage other priorities. It helps to centrally manage the users who access the cloud resources while keeping the business under control. Nowadays, cloud providers provide their cloud solutions with integrated IAM tools, eliminating the need for migration and the associated cost. In any organization, this migration can enable critical administration, authentication, authorization, and audit responsibilities. Organizations that run most of their applications benefit from this cloud-based IAM tools provided by Google and others. The cloud identity provides free identity services for users by creating a free account for them and managing them from the Google Admin console.



## ADVANCED AUTHENTICATION METHODS

Utilizing one set of credentials to allow users to log in to applications is no longer acceptable to meet the growing security threat that the IT sectors should be aware of the new authentication technologies in the market. Organizations should consider integrating emerging technologies into their IAM strategies. Techniques such as smart card and biometric access take the organizations a step forward by incorporating the identity data for the individual.

Multifactor authentication (MFA) authenticates users with more than one method. Authenticator app that can be deployed in organizations using Microsoft 365 provides multiple options like PIN, facial recognition, iris scanning, and others to sign in. Also, there are MFA apps that send notifications to the users' mobile enquiring the login attempt. Followed by the multifactor authentication is the next-generation successor, adaptive authentication that uses machine learning to calculate risk scores and determine an appropriate security response.

## GDPR IMPACTS IAM

General Data Protection Regulation (GDPR) came into effect in May this year. The European Union GDPR bolsters data protection, and it imposes a severe impact on organizations that fail to manage and secure their data. According to GDPR, individuals have ownership of their identities that businesses should understand and cater to the needs, especially when it comes to changing or deleting personal records. Also, GDPR can fine organizations for data breaches, and it can be avoided if the organizations have deployed the first line of defense 'IAM' to minimize damage.

## ADDING VALUE TO UEM

Another significant trend is the unification of unified endpoint management (UEM) and IAM platforms that enables administrators to manage a UEM console solely. Breaking the silos between the two independent platforms, organizations should focus on integrating them, thus helping accomplish the unified management. UEM vendors such as Citrix and Okta comes with features to integrate IAM with their platform. Successful implementation of identity and access management requires forethought, clear objectives, and defined business processes, because the old practices of IAM are no longer supported, organizations should readily embrace the above trends to ensure compliance. CR

# WHY BIOMETRIC AUTHENTICATION IS INDISPENSABLE FOR CYBERSECURITY SOLUTIONS

Biometric authentication is one of the branches of identity and access management (IAM) that is gaining popularity for amplifying security features. The biometric authentication process relies on the unique biological traits of an individual for authentication. Although the technology is still in its nascent stages, enterprises and users have started to trust the technology's efficient security solutions. Biometric authentication solution can solve many issues that pose security threats for the organization. Here are two of the most significant problems that traditional IAM solution faces and how Biometrics can eliminate those issues:

Passwords: Passwords have ruled the roost in identity security for many years. They were considered as a balanced tool for cybersecurity and convenience. However, with the emergence of smart technologies, hackers have been able to crack passwords of most users. These technologies offer various ways for hackers to breach the password protected identity security of a user as well as an organization. On top of that, users also have to memorize all the passwords of different websites that they use. Many users put the same password for all the sites with puts security at risk, as a security breach in any of the websites can put the safety of all the other websites in jeopardy. Biometrics, on the other hand, can be an ideal alternative for the cybersecurity solutions as hackers have not yet found answers to fake biological traits of an individual.

Endpoint Security: The proliferation of IoT devices has increased the number of endpoints, making endpoint security an essential component in supporting the digital perimeter. The hackers use more sophisticated attacks like phishing attacks to trick users into handing over their credentials to the bad actors. The phishing attacks allow cybercriminals to bypass the firewall of a system and steal a user's sensitive data. Biometric solutions can add an additional layer of security for the endpoint devices, strengthening the cybersecurity solutions. The biometric authentication tools provide a verification tool that prevents any phishing attacks on a network. CR

# IT WASN'T EASY, BUT WE DID IT.

We built out-of-the-box IAM service with proven technologies for you.


Secure Identity as a Service, powered by our SOC

Telia

Visit: www.unitedidentity.fi | Email us: sales@teliacygate.fi | Call us: +358 40 839 3985

# GreyCorbel Solutions

**GreyCorbel Solutions integrates services and solutions in the most valuable asset of companies to eliminate the risk of losing business data**

# TURN THE WEAKEST LINK INTO A SECURITY WEAPON

By Justin Smith

***"A chain is as strong as the weakest link."***

This quote rings true for every scenario in an organisation, particularly security. Enterprises seeking to strengthen their security around data and digital assets must face a bitter truth: the weakest link in the security chain is the people of an organisation. Hackers prey on the flaws of the people—the element that holds up the pyramid of People-Process-Technology. While the "people" aspect remains a fertile field for bad actors, most security administrators with access to servers, firewalls, network gear, business applications and databases continue to overlook password best practices, which can result in compromising of credentials and a threat to sensitive resources and data. In fact, according to a report from Microsoft, more than 90 percent of cyberattacks on enterprise data are carried out due to insufficiently secure passwords of corporate employees. In order to protect their organisations "inside out," they need to educate employees on the access component of enterprise security, prioritise, pick and implement solutions, while also maintaining thoughtful governance.

This is where GreyCorbel Solutions is in a league of its own.

With an aim to prevent sensitive data from falling into the wrong hands, GreyCorbel Solutions empowers enterprises with services and solutions for data protection. "GreyCorbel Solutions integrates services and solutions in the most valuable asset of companies to eliminate the risk of losing business data," says Jiří Formáček, Founder and CEO at GreyCorbel Solutions. Backed by years of rich experience in IT security, the experts at GreyCorbel Solutions can effectively capitalise on designing or implementing customised security solutions such as

CIO Review
TOP 10
IDENTITY AND ACCESS MANAGEMENT
SOLUTION PROVIDERS IN EUROPE - 2020

Jiří Formáček,
Founder and CEO


Identity management. In doing so, the company does not believe in forcing its clients into acquiring new infrastructure software components and aims at providing the optimal solution using existing resources.

GreyCorbel Solutions focuses on the delivery of quality IT services and the development of commercial and custom software solutions for the Windows platform. Touching upon the challenges in identity and access management space, Formáček cites an example of a company that was unaware of the fact that hackers walked unnoticed into the company as they had been able to log in as an admin all the time. They collected sensitive company data for three years and yet the company could not catch a whiff. Mitigating similar risks for enterprises, GreyCorbel Solutions focuses on defining the architecture of solutions, defining the scope and leading implementation teams towards delivery.

Specialising in security and identity services, the company brings in Admin Password Manager for Enterprise (AdmPwd.E) that effectively prevents the misuse of the administrator accounts and can save companies considerable money by mitigating possible cyberattacks. Based on the open-source AdmPwd Solution, AdmPwd.E covers everything from secure management of local administrator accounts passwords of domain-joined Windows machines, group policy integration and management. Passwords are stored in Active Directory (AD), and encrypted, so only eligible users can read it or request its reset. Besides password history management and password encryption, AdmPwd.E provides HSM support for storage of private keys and keeps simple and clear audit trail in a dedicated log detailing every operation performed. The solution comes with user-friendly auditing tools and security model, support for deleted computer objects, password management of domain user account, and much more. GreyCorbel Solutions enables seamless deployment of AdmPwd.E with Microsoft installer package, Windows Installer (MSI).

At the core, GreyCorbel Solutions solves the complex challenges around authentication and communication. As per the new European Directive, organisations need to publish their digital services through open APIs, which elevates the possibility of new threats. This is where GreyCorbel Solutions assists its clients by providing services which are secured by protocols like oAuth2, open ID connect, and more. The company also advocates implementation of communication security–typically secure E2E communication by encryption. "We help our client achieve the main goal of having the right architectural design, which can significantly increase the efficiency of safety. Furthermore, we follow a meticulous approach to identify and define what services inside the company are at risk and should be secured, before designing the appropriate discipline for them," adds Formáček.

He narrates a recent engagement with one of their clients looking for some changes within their current IDM. The client—one of the biggest banks in the Czech Republic—was facing issues with their identity and access management. GreyCorbel Solutions came on board fixed their issues and created a dynamic identity and access management solution for them. Instances as such highlight one of the many success stories the company has scripted for its clients. The company currently operates in more than 17 countries across four continents to protect more than 100Mn machines!

Moving ahead, as small companies and start-ups lack the funding to build infrastructure and services on-premise, GreyCorbel Solutions is planning to increase the cloud service development. The company will also expand its services in West Europe and Asia. "We want to educate our clients and help them acquire certain skill sets that they need for the future," concludes Formáček. CR

# JURA

## 1. Banknotes

Design Workstations for Banknote and High-Security Document Printers.


## 3. LetterScreen

High-Security Secondary Portrait for Passports with Personalised Line-Structure.




## 2. IQ-R

High-security version of QR codes for personal documents and brand protection.


## 4. IPI

Personal Data Hidden into the Primary Portrait of any Photo-Carrying Travel Documents.

## 5. ICI

Hidden image for security documents.

www.jura.hu

# CIO Review TOP 10 IDENTITY AND ACCESS MANAGEMENT COMPANIES IN EUROPE - 2020

In the modern IT environment, organizations have to know who is accessing what, when, where, why, and how. That's where a strong Identity and Access Management (IAM) solution comes into play. It is a necessity for businesses dealing with critical information and data which is not something to be overlooked. The IAM platforms are poised to not only dominate cybersecurity but to completely subsume it. Identity concerns have become top-of-mind for IT security professionals and personnel all over the world. Not only do they need to ensure the identity of the users, but they must also ensure that employees' entitlements are limited by their duties, that their privileged credentials are secure, and that their authentication methods can't be easily deceived. Hence, it is essential to adopt IAM systems for providing a superior level of healthcare services by meeting regulatory demands.

The implementation of IAM solutions across various industries including IT & telecom, BFSI, public utilities, and healthcare also leads to higher market demand. IAM companies in Europe and the UK are entering into strategic cooperative relationships, enabling customers to take advantage of the collaborative offerings. Bolstered by success, the IAM platforms are being positioned to help businesses thrive in an era of unprecedented change. To help the business decision-makers understand new technologies and market trends impacting IAM, and to guide overall strategy for investments in technology solutions, CIOReview presents "Top 10 Identity and Access Management Companies in Europe - 2020."

| COMPANY | DESCRIPTION |
| --- | --- |
| **ADUCID**<br>aducid.com<br>Solution | ADUCID provides the most innovative multi-factor authentication for eID solutions—in eGovernment, eHealth and private sector—that protects users from all types of authentication attacks known today |
| **GreyCorbel Solutions**<br>greycorbel.com<br>Solution | GreyCorbel Solutions focuses on the delivery of quality IT services and the development of commercial and custom software solutions for the Windows platform |
| **IDEMIA**<br>idemia.com<br>Services | IDEMIA, the global leader in Augmented Identity, provides a trusted environment enabling citizens and consumers alike to perform their daily critical activities (such as pay, connect and travel), in the physical as well as digital space |
| **Identity Maestro**<br>identitymaestro.com<br>Services | Identity Maestro is a leading provider of simplified Identity Orchestration and Management |
| **Indeed Identity**<br>indeed-id.com<br>Solution | Indeed Identity is a Software Vendor of Smart-card management system, Enterprise Authentication and Enterprise Single Sign-On systems |
| **ITSENSE**<br>itsense.ch<br>Services | Established in 2003, ITSENSE has been an established IT company specializing in the areas of Enterprise IAM (EIAM), Customer IAM (CIAM), Identity as a Service (IDaaS) and Single Sign-On (SSO) |
| **MobiWeb**<br>solutions4mobiles.com<br>Solution | Since its establishment in 1999, MobiWeb has been providing global SMS Messaging, Voice and Telecom Services for B2B, B2C and C2C mobile interaction |
| **QUANTO Solutions**<br>quanto-solutions.de<br>Services | QUANTO Solutions is a cybersecurity and authorizations technology specialist that offers exclusive advisory services as well as best-in-class IAM solutions to shield intricate business information from falling into the wrong hands |
| **SailPoint**<br>sailpoint.com<br>Solution | SailPoint, the leader in identity management, delivers an innovative approach to securing access across the enterprise with the SailPoint Predictive IdentityTM platform |
| **WiB Solutions**<br>wib.ch<br>Services | Offers unique two-factor authentication solutions that simplifies identity and authentication management and drive user experience in using online services |

KBC

A Yokogawa Company

# NOW IS THE TIME... WELCOME TO THE DIGITAL FUTURE OF THE ENERGY AND CHEMICAL INDUSTRY

Learn how 4 digitalization projects can help turn your organization into an agile machine that anticipates issues and organizes to prioritize and solve them before they escalate.

Find out more:
www.kbc.global/digital

*All about*
**EXCELLENCE**

# PUTTING THE "I" IN IDENTITY: HOW IDENTITY TECHNOLOGY FUELS THE UN-CARRIER REVOLUTION

**By Cody Sanford,** EVP & CIO, T-Mobile

What makes your business singular? What makes one customer, one device, one line of code different from the next? What makes you you?

The answer is identity. Identity is the key to modern life, and identity management—the means businesses use to distinguish one individual user from the next and to maintain and safeguard their proprietary information—is crucial to operating in the modern economy. However, in the digital era, establishing who or what we are is more challenging—and more critical—than ever before.

At T-Mobile, we view technology through the lens of customer obsession. As a result, we believe our customers and employees have an inherent right to data security and data access. It's a matter of trust that we've established with our customers, and a big part of our role as the Un-Carrier is listening to our customers and giving them what they ask for. And the core of that trust is identity management. We want to be sure that as we help drive the technology evolution of identity management, T-Mobile customers and employees will be among the first to benefit.

As T-Mobile's CIO, one of my main responsibilities is removing barriers to collaboration to encourage greater innovation, and that's led my team to develop some rather impressive solutions for identity management. When we began our journey of digital transformation in 2014, we sought to both learn from and contribute to the technology communities around us. We engaged with the open source software (OSS) community to explore the full depth of identity management and platform development. With millions of customers and thousands of employees, we understood that identity was at the center of our transformation. Our goal was security, and API-first software designs allowed us to realize the holy grail of identity management: giving our customers and employees the right access to the right resources at the right time.

By 2016, as blockchain technology became more widespread, we recognized an innovation that could change the way identity is accessed, managed, secured and audited. We also recognized real industry pain points: Standards were rare, even nonexistent, and throughput, key management, and oracles presented significant engineering challenges. To lead the way toward a future where blockchain dramatically improves the identity space, we had a lot of work to do. In the process of driving OSS efforts and industry-wide initiatives including the World Wide Web Consortium's Verifiable Claims work and the Token Taxonomy Initiative, T-Mobile became a thought leader, and we homed in on two primary identity-related use cases: identity governance and self-sovereign identity (SSI).

Identity governance, the centralized, policy-based management of identity and access, is critical to any company that manages identity at scale. Blockchain can play an important part. The three keys to this capability are tokenizing an identity entitlement that allows for precise tracking; leveraging smart contracts (which I like to think of as business processes defined and operated in code) to allow control definitions to be coded into the platform, and providing indisputable audit records of transactions. As T-Mobile continues to lead standards development in this space, we've implemented much of our research in theHyperledger Sawtooth NEXT Identity Platform. This OSS application combines the performance of a NoSQL database with the blockchain keys identified above. Layer a React UI over the Swagger-based APIs and you have a next-generation enterprise solution for controlling, operating and auditing identity. We developed this software in conjunction with Microsoft and Intel and we're sharing it freely with the sole intention of empowering businesses to better serve their customers.

Identity governance is a compelling use case, but SSI marks a potential turning point in modern identity. The term describes the set of protocols, infrastructure, and standards that allows an individual to control their online identity, encrypted and decentralized. This truly revolutionary technology provides—for the first time—the ability to change the definition of online identity from "You are you" to "I am me." And its impact on business could be profound.

> **"Identity governance is a compelling use case, but SSI marks a potential turning point in modern identity"**

Cody Sanford

Whether in a B2B partnership, sales deal or employee hire, businesses traditionally trust claims without verifiable proof. SSI offers the opportunity for third party-verifiable claims—a potentially revolutionary and empowering advance across a wide spectrum of applications. This can, for instance, break down longstanding barriers around education and hiring. The personal anonymity of blockchain systems combined with the ability to verify individual claims could be a boon for diversity hiring, as applicants would present only the job-relevant aspects of their identities, eliminating potential bias against certain types of names, ethnicities or educational paths. In other words, any and all qualified applicants – whether or not they fit a specific socioeconomic profile – would suddenly find themselves in consideration for jobs they were previously denied. Opening the door to qualified candidates of all backgrounds could reveal a previously untapped talent pool and forever change how hiring decisions are made. Here at T-Mobile, where we're committed to expanding the diversity of our employees across all our teams, leading the way to that end is the kind of work we want to be doing.

From security that keeps private information safe to new models of blockchain audit and governance to fundamental changes in SSI and verifiable claims, identity management is at the heart of T-Mobile's technology transformation. It determines not only how our businesses interact, but how we interact as human beings. The tools are changing but T-Mobile's commitment to protecting and empowering our customers and employees is not. As this space continues to evolve, T-Mobile will continue pushing the boundaries, Un-carrier style. CR

# MobiWeb Ltd

## Smart Authentication for Enhanced Online Experience

Global business innovation has scaled greater heights, thanks to the advent of cutting-edge technology disruptions. With numerous business systems hosted in the cloud environment, the workforce of today is more confident about working remotely. However, on the flip side, these drastic changes in business operations are exposing the gaps in the current security practices. The archaic username and password mechanism for user authentication has time and again proven to fall short of meeting the expectations from the identity management and security perspectives. Moreover, bad actors are weaponizing the technology advancements to hurt businesses online. "Every year, businesses face fraud of $5 trillion in cost globally," says Alexander Spirotis, COO of MobiWeb. Adding to the woes is the inclination of most companies to use complex security tactics, which require considerable resources, complex administration, and high cost.

Headquartered in Hong Kong, MobiWeb is emerging as the ideal identity and authentication management partner for companies worldwide. Leveraging its direct connections with telecommunication carriers and operators in the largest cloud data centers across the globe, MobiWeb provides two-factor authentication (2FA) solution driven by high-quality SMS messaging services. Through the solution, companies can use a combination of username, password, and a one-time password (OTP) to secure their systems. "We bring an additional layer of security check for all modes of communications, thus enabling a protected environment in a simple way for our clients," says Spirotis. Regardless of their location and time-zone, clients can access their resources without any worry about the security breach.

With MobiWeb's SMS Messaging functionality, enterprises can utilize SMS to send OTP to their users globally, reaching subscribers of 2,000 mobile network operators through a single API connection. This is ideal for enterprises that aim to have full control and flexibility over OTP generation and validation. On the other hand, MobiWeb's OTP SMS is an end-to-end solution for OTP generation, delivery and validation. The company's API allows enterprises to easily generate OTP and deliver it via SMS for user validation. During login, a user receives an OTP via SMS with an expiry time, so fraudsters will not have sufficient time to tamper the systems. MobiWeb has adopted the highest standards in developing its solutions. The OTP SMS generation functionality is based on IETF standard RFC 6238, which is the industry-backed standard for two-factor authentication.

Alexander Spirotis

> **We bring an additional layer of security check for all modes of communications, thus enabling a protected environment in a simple way for our clients**

Besides user authentication, MobiWeb's solutions aid clients in authorizing financial transactions. Major financial institutions and banks based out of the Republic of Guinea and Chile are using MobiWeb's 2FA API for added security during the authorization of users and transactions. This has led to more secure and smooth business operations as fraudulent events are being checked in a fool-proof manner. Impressed by the enhanced security layer for accessing online services, the clients' customers welcomed the new measures taken by the service providers. Thus, MobiWeb's solutions are a shot in the arm for global firms, enabling them to drive customer experience and loyalty.

For the future, MobiWeb is focused on developing a new platform and capability. MobiWeb Omni-Channel Platform eliminates SIM swapping by supporting OTP via multiple channels like Google RCS Messaging, Viber and WhatsApp. On the other hand, MobiWeb Anti-Sim Swap feature will allow businesses to check if a mobile number is SIM swapped before sending OTP SMS to the user. These new offerings will further enhance the security provided by two-factor authentication. CR

# Secure Data to Avoid Misuse of Identity

**By David Pollington,** Head of Services, GSMA

Digital identity is becoming core to the future growth of the Internet, be that through reducing the friction of onboarding users to new online services, or providing trust within the sharing economy, or enabling Internet players to understand individuals better and curate personalized services and experiences for them.

David Pollington

But digital identity is brittle, the majority of the public not truly understanding the role their identity plays online, and the thirst for data fuelled by the surveillance economy, creating honeypots of identity information. These pieces of information are targeted by cybercriminals and results in irreparable reputational, financial and legal damage for the businesses and are devastating for the individuals whose identities are stolen. With credential misuse being the leading threat metric behind most data breaches and associated identity fraud, it's imperative that the next generation authentication mechanisms increase in robustness, but in a way that doesn't present a barrier to user experience.

A move away from passwords to authentication methods utilizing multiple factors, and most importantly authentication factors such as possession (of a mobile phone) and inherence (biometrics) that are immune to scalable attacks, will help to build robustness. Similarly, a migration to a more passive, continuous means of authentication using behavioural biometrics or cleverly inserting physiological biometrics (such as facial recognition) within the user flow has the added benefit or not only improving security but also delivering on the holy grail of reducing user friction. It is perhaps ironic that one of the most promising methods, behavioural biometrics, has a dependency on passively monitoring and collating data on the user. This is unfortunately the mouse trap that is the surveillance economy - on the one hand it can be beneficial in keeping us safe, but if abused can be used to manipulate us in the process.

GDPR is helping to create awareness and provide a set of guard-rails to encourage good behaviour amongst online players. Whilst not as progressive and effective as some believed or feared, GDPR has been instrumental in raising awareness around privacy and data protection and encouraging companies to reposition themselves more favorably within the privacy debate, thereby currying favor with the regulators and winning back confidence from the public. Arguably though, the Internet is sorely missing an identity layer that delivers trust intrinsically.

Decentralized identity is seen by many as a potential way forward, giving back control of identity to users and creating an open framework that can foster an ecosystem for identity without reliance on any dominant players. Work to define and standardize on the critical building blocks is progressing well in W3C and DIF with strong backing from the community. Still, there remain many commercial and operational challenges that need to be worked through before such decentralized identity solutions will be able to achieve mass market adoption.

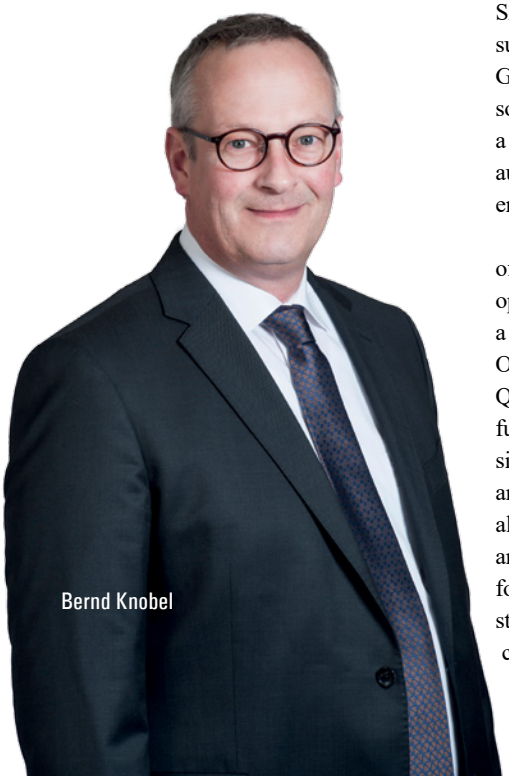
Whilst the large Internet companies are likely to continue their relentless pursuit of user data, combining it with advanced machine learning to further generate insights and influence user behaviour, the future belongs to those brands who can be trusted to manage their customers' data with integrity, security and transparency; although many believe that such a halcyon view will not be achieved without an evolution in the regulation built on a more thorough understanding of how the surveillance economy operates today and may evolve in the future. CR

# QUANTO Solutions

## 21st Century User-Authorization Management

Identity and access management (IAM), in summary, translates to the authorizations provided to users within an enterprise setting. When faced with a change within the business infrastructure, some of these critical authorizations remain assigned to employees that have transitioned into different roles, causing discrepancies within the workflow. This problem gets magnified when authorizations are assigned in multiple combinations, shedding light on the importance of efficient IAM solutions in the enterprise landscape.

"Technology continues to grow with time, and if a company does not have the right tools to oversee authorizations, they will inevitably come to a standstill in terms of growth," says Bernd Knobel, Managing Director of QUANTO Solutions. To keep firms up-to-date on the best data protection strategies, QUANTO Solutions—a cybersecurity and authorizations technology specialist—offers clients exclusive advisory services as well as best-in-class IAM solutions to shield their most delicate information from falling into the wrong hands. QUANTO Solutions' IAM offerings include QUANTO-SEC, QUANTO-GO, and QUANTO-Connect, all of which stand tall as a collective force to reckon with against cyber-fraudsters trying to find vulnerabilities and gain access into an enterprise system infrastructure. "It is vital to reduce the existing critical combination of authorizations, and we have some great tools to analyze user-credentials to determine whether they require particular permission or not before reorganizing their data access approval," explains Bernd Knobel, Managing Director at QUANTO Solutions.



Bernd Knobel

Sebastian Winkelhofer

> **we have some great tools to analyze user-credentials to determine whether they require particular permission or not before reorganizing their data access approval**

QUANTO-SEC, the company's flagship product in the IAM space, is an SAP security application that features tools such as QUANTO-SEC/SoD, TGL (Trusted Go Live), and CleanUP. The complete software program allows clients to perform a risk analysis to identify and reduce critical authorizations that can be harmful to an enterprise.

Upon engaging with a client, a segregation of duty (SoD) analysis is performed on their operational systems architecture to initiate a screen-test for user authorization issues. Once the nature of the problems is gauged, QUANTO uses the Trusted Go Live (TGL) function to reduce the test effort on a customer side during the authorization reassessment and reallocation process. The tool can analyze all of the required user authorizations, and then define a new protection strategy for clients without affecting a project stakeholder's everyday workflow. In the off-chance that a user is facing a problem with new access credentials, they can revert to an image of their old user data until all known hindrances are addressed adequately. Once all the aforementioned procedures are complete, QUANTO Solutions, utilizing its CleanUP tool, removes any unwarranted authorizations that are assigned to a role within an SAP system, enabling the users which are no longer needed to avoid future system access mishaps.

Besides, the deployment of QUANTO-Connect allows clients to gain a full overview of their IT infrastructure and create data lakes. This can help to check employee authorizations with complete adherence to GDPR but also all other kind of data which are today an important good. This adherent structure is achieved owing to the addition of the data protection compliance regulatory guidelines followed within the QUANTO-GO program algorithm. Finally, the QUANTO-Go tool can categorize data by predefined statistics, delete unwarranted files, and store only essential information while allowing customers to uphold the regional and international regulatory laws. QUANTO-GO is the solution for data migration.

With the release of QUANTO-GO/DS, QUANTO Solutions now allows the intelligent integration of SAP systems within data lakes. The company has also upgraded the program to provide S/4HANA compatibility, and in turn, further enhancing its IAM range of services and solutions. CR

# WHO'S IN YOUR ELECTRONIC WALLET?

**By Scott D. Ramsey,** Managing Principal Cybersecurity, CAPCO

Originally, identity and access management (IAM) started out requiring username and password for authentication and authorization. As the technology footprint began to expand providing users with continuous access through remote connectivity via laptops, hand-held devices, and now the Internet of Things (IoT); this simple combination had to evolve into more complex techniques and technologies to ensure proper validation of the user. Complex algorithms using multi-factor authentication (MFA), biometrics (fingerprints, retina scan), vocal patterns, and facial recognition have and are being developed and used. However, many people continue to ignore the risks and liabilities of not protecting their identities. Companies trade off on security and confidentiality for the convenience and ease of use of non-invasive immediate access. For the 'convenience' of their employee's many organizations institute bring your own device (BYOD) policies that allow personnel to access corporate email and networks utilizing their personal devices, which now combines both personal and corporate information. Breaching these devices puts both the end user and company at risk. Today, you can unlock a mobile phone by simply placing your thumbprint on the 'home button' or unlock a laptop or tablet with your face, granting access to all the devices' contents. Both access methods are easily 'fooled' putting all of the information and data on these devices at risk. On your next visit to a restaurant, see if you can determine if the mobile device that has been given to a toddler to 'amuse them' is a personal or corporate device. Can you guess how that device was activated and do you suppose any restrictions are limiting what the toddler can access?

Today, 'smart devices' have invaded our homes, including TVs, appliances, thermostats, security cameras, digital assistants (i.e., Alexa, Google, Echo, etc.), sound systems and more. People connect all of these devices to their home wireless networks that desktop systems, printers, laptops, tablets, mobile phones, and IP phones are using. By doing this, they increase their exposure to identity

theft and the compromising of information (i.e., photos, videos, contact lists, shopping patterns, conversations, health information, etc.) on these devices. To make matters worse, the vast majority of homes where these devices have been installed, the default passwords/passcodes from the manufacturer have not been changed by the homeowner.

Intelligent vending machines are cropping up in employee breakrooms and public areas across the globe. These machines not only accept good old fashion cash but also accept payment from electronic wallets on mobile phones and credit cards, which require the machines to be connected to the internet through either wired or wireless networking. How are these devices being secured, or are they? Have they been placed on a segmented network or just added to the corporate backbone or hot spot as another device? What information are they providing back to the distribution center other than their inventory and who else might they be providing information too?

> **The value of the information stored, processed, and transmitted by the technology should be the driving factor in how users are authenticated and authorized for use**

Now, what has all of this got to do with IAM? In my opinion, everything! We have become a society of on-demand and convenience. We shop online and have purchases delivered to our front doors; we expect our house to be at the perfect temperature before we return from work; we rely on our appliances to tell us we need more eggs and milk and that we need to set the dishes to wash. As a society, we focus more on the ease of access than the protection and securing of our identities and information. The weakest link in the security chain is the end user. By not being vigilant in protecting our identifies and data in the use of technologies, we are exposing ourselves to fraud, theft, misuse, and misrepresentation. Convenience cannot be the primary requirement for accessing technology. The value of the information stored, processed, and transmitted by the technology should be the driving factor in how users


Scott D. Ramsey

are authenticated and authorized for use. It's true for both corporate and personal devices. If you are storing credit card, frequent flyer, access codes, personal information on your devices, you need to take appropriate measures to secure it. Ask yourself this question, "If my device is compromised, what are my potential impacts and liabilities?" Then look at how you are securing and protecting the information on those devices and see if you are comfortable with the access measures in place.

IAM alone will not secure the data on your devices, whether personal or corporate. IAM should be combined with additional security measures to obscure sensitive information. Incorporate MFA, requiring you to have something and know something. The 'have something' is your finger and the 'know something' is the passcode or passphrase (i.e., on your mobile phone, use the biometric feature on the home button in combination with a passcode or passphrase). Also, it never hurts to consider encrypting the hard drive of your mobile computing devices in conjunction with your access method.

Remember, your devices and data are only as secure as you make them. CR

NO SALES GUYS.COM

# WE'VE REVOLUTIONIZED THE COPIER LEASING EXPERIENCE.


Finally! Leasing a Copier is as easy as shopping for anything else online — quick, easy, and convenient.

Drop the salesperson. NoSalesGuys.com the future of the copier industry is now!

Don't be left out! Find out how you can become part of the revolution!

**3 Executive Campus, Suite 260B**
**Cherry Hill, NJ 08002**
**Email: Support @ NoSalesGuys.com**

NO SALES GUYS.COM

# CIO Review TOP 5 IDENTITY AND ACCESS MANAGEMENT SOLUTION PROVIDERS IN UK - 2020

As the intricacy and scope of modern identity environments are becoming challenging to manage using traditional methods, there is an imperative need to bring innovation and new technologies for creating a secure, flexible and adaptive IT infrastructure. Identity and access management (IAM) has advanced to become a vital segment of the IT infrastructure. IAM has become an essential asset as it encompasses processes and information technologies that are correlated and mutually reliant on all business areas. Amidst escalating security threats and ever-increasing data breaches, protecting customers from identity theft, account takeover and privacy abuses requires sophisticated identity and access management capabilities. However, lack of effective identity and access management poses significant risks to compliance and to an organization's overall security, which limits the growth of the market.

It is imperative for organizations to understand that security definitions are evolving at a disruptive speed. If IAM solution is planned and implemented well, it eventually helps strengthen regulatory compliance, facilitate secure operations, and enhance operational agility within an organization. IAM tools installed across an organization's critical functions needs to be updated and must be compatible with upcoming advanced technologies and functionalities.

Organizations must prioritize identity management tools that can provide highly automated workflows to simplify IAM administration, and that can integrate well with other systems and security technologies. The idea is the more seamless a tool fits within an environment and with other security tools, the more likely organizations are to close security gaps and improve business operations.

To gear up for the IAM era, we suggest our readers have a look at how new technologies, practices, and trends are redefining innovation in the cybersecurity space. Offering a nexus of innovative technological capabilities, these IAM service providers are upping the business security by several notches. Navigating through these best-of-breed consulting and services, CIOReview aims to help you build the partnership and make prudent decisions your organisation needs to foster a technology-driven environment.

We present you CIOReview's Top 5 Identity and Access Management Solution Providers in UK - 2020.

| COMPANY | DESCRIPTION |
|---|---|
| **Centrify**<br>centrify.com | Centrify is redefining the legacy approach to Privileged Access Management by delivering multi-cloud-architected Identity-Centric PAM to enable digital transformation at scale |
| **GBG [LON: GBG]**<br>gbgplc.com | GBG offers a series of solutions that help organisations quickly validate and verify the identity and location of their customers |
| **My1Login**<br>my1login.com | My1Login's multi-award-winning IAM solution solves the problem of weak passwords and practices, enabling organisations to control user access and centralise identity through Single Sign-On and Privileged Password Management |
| **Securience**<br>securience.co.uk | Securience is an organisation specialising in Identity Management, Access and Governance solutions |
| **ThirdSpace**<br>thirdspace.net | Award-winning Microsoft gold partner, ThirdSpace specializes in identity management, enterprise mobility and cyber security solutions |

NEXIS

The leading Identity and Role Analytics Solution for Business and IT.

# Go ahead with your **Identity and Access Governance.**

- Identity & Analytics
- Role Optimization
- Role Modeling
- Workflows
- Entitlement Visualization
- Access Governance
- Business Communication
- Risk & Quality Controls

Nexis GmbH | Franz-Mayer-Str. 1 | 93053 Regensburg - Germany | www.nexis-secure.com

# Securience Limited

## A Trusted Partner for Identity and Access Management

Companies want to be in complete control when it comes to managing the access rights to their systems. To that end, they adopt identity and access management (IAM) solutions but still struggle to achieve the desired outcomes. There can be several reasons to this. Primarily, most organizations lack knowledgeable leaders who can lead the IAM project from the front and encourage every stakeholder in the project to be fully committed to following the best practices. The lack of consistent data quality and skilled resources add pain to the misery. As a result, legitimate end-users are denied of the seamless authentication experience.

Founded in 2014, Securience Limited is a company on a mission to finding an optimum balance between security and user experience. Led by seasoned IT security professionals, Securience practices a customer-first culture and advises IAM solutions and strategies that are best for their unique business needs. The technology-agnostic company offers RSA Security's IAM solution, RSA Identity Governance and Lifecycle, which is acclaimed for its unmatched IAM functionalities. In fact, Securience's Technical Director and Product Owner is an RSA veteran who earlier worked as Senior Solutions Architect in Identity Governance at RSA.

Doug Chin

> **Unlike other service providers, we build a strong and stable technology foundation upon which we can add new capabilities as part of our continuous development efforts, every month**

Securience has the proven capability to complete projects of any size quickly and efficiently and enable clients to achieve ROI as soon as possible. Such an impressive track record has helped the company achieve a year-on-year growth of 80 percent and emerge as the trusted IAM partner for public and private sector organizations from across industries. "Unlike other service providers, we build a strong and stable technology foundation upon which we can add new capabilities as part of our continuous development efforts, every month," says Doug Chin, Managing Director of Securience. "Our continuous delivery approach enables clients to respond to the dynamic business demands in an agile manner. Moreover, by turning to Securience's IAM managed services, clients can leverage expert resources to managing their IAM tasks, saving themselves from having to hire skilled individuals and retain them.

"Our solutions, services, and client engagement strategy are all tailored based on our experiences," says Chin. So they are primed to support faster solution implementation while keeping the cost in check. To elaborate, Securience initiates client engagement with a well-defined governance structure. The agenda is to take onboard the right stakeholder–client teams, vendor partner, or systems integrator—and make them aware of the accountability aspects.

It has been found that IAM project execution consumes unnecessary cost and time when there are issues with data quality. To address this challenge, the company has developed Securience Data Manager (SDM) that automates data integration and accelerates application onboarding during the IAM project execution. The company uses SDM to analyze the quality of the data coming from various applications and identity sources. The insights help the client understand the problems before executing the IAM program.

In a case study, an asset and pension management company handling 400 billion pounds in assets management across 4.5 million people wanted to meet and exceed compliance requirements while driving the UX and adoption of their strict identity governance processes. Securience was engaged to design and implement an apt solution to that end. The company understood the client's needs and optimized IAM processes through role-based access strategy for improved compliance. It implemented its SDM to enable a two-way feed between the service desk application and the cloud, and provisioned various endpoints. Rapid implementation of the IAM solution and seamless monitoring enabled the client to reduce the risks.

Securience is currently working on Securience Access Anywhere, a new product that brings IAM capability to mobile devices, allowing end-users to perform IAM tasks more easily. This will streamline processes such as reducing the time for the manager to approve access requests. CR

# NOT YOUR FATHER'S IDENTITY *AND ACCESS MANAGEMENT*

**By Martin Ingram,** Product Owner, Identity and Access management, Royal Bank of Scotland (RBS)


Martin Ingram

It used to be easy to define the boundaries of Identity and Access Management (IAM)–its purpose was to prevent anyone getting to anything that they weren't supposed to. While that is still true it fails to recognize the world that is unfolding for IAM going forward, even in industries that are more cautious such as Finance.

You can trace the roots of IAM to at least two separate roots: Controlling access to early computer systems and authenticating customers face to face in branch.

• In the first case, computer users, at first access were controlled by physical security–if you could not touch the computer then you could not use it. As access broadened and progressively, controls that are more complex were brought in: Accounts, Passwords, Role Based Access Control, etc.

• On the customer facing side, we progressed through passbooks and cards to the introduction of call centers, which brought with it a need to introduce customer to account name and password, and subsequently, we progressed into the Internet world.

> **"Financial organizations that take advantage of the opportunities provided by federation will be able to maintain their value for the customer"**

And from that point, the two strands joined and we have moved forward, recognizing the weaknesses, while fundamentally seeing IAM as a way to constrain access and isolate systems. For financial services, isolation has been the watchword ever since–IAM has been about restricting access.

In common with other industries, financial services are now shifting to a digital approach to customer interactions. This is now well established and improving the customer's experience. The key to digital is that it works from a focus on the user's journey through a web site or service. Businesses are aware that these efforts frequently hit a roadblock at the boundary of the organization and that there are opportunities beyond them. These opportunities may be to simply reduce user friction but in many cases, they involve opening up additional streams of revenue or cost reduction that would benefit the business.

• A customer may use their good standing at one Bank or service provider to open accounts or services at another bank or service provider.

• A customer may use information that is held in one organisation to seamlessly conduct business with another. For instance, filling in the common data that businesses often require.

• A customer's continued use of the new service would be via the original service, improving stickiness.

Consequently, there is a drive to break down the historical isolation that has existed, and allow more complex customer journeys that may span multiple companies. This flow can be enabled by IAM using the Open Standard protocols that have become popular in recent years. Originally established for use with social media protocols such as Oauth and OpenIDconnect, Open Standard protocols can be used to create journeys that both federate and meet the security requirements all the way up to the financial service industry. Also, by being open rather than proprietary it is reasonable to expect that others can and will interoperate.

Financial organizations that take advantage of the opportunities provided by federation will be able to maintain their value for the customer. They will be the route through which the customer accesses existing services and signs up to new ones. Companiess with strong and reusable data that can be federated will be in the strongest position. Such enterprises include financial institutions, mobile phone networks and governmental organizations. The value that a company can charge on data will depend on the dependability and breadth of that data and the consent that the user has provided for its use.

The conclusion is that, while we must still protect that which we see as valuable, the way forward for IAM is not so much in the isolation but in federation. From the perspective of us practitioners, the move from being an obstruction to an enabler will be very welcome. CR

# Why Security Is More Pivotal *than Ever in the Office of the Future*

**By Hiro Imamura,** Senior Vice President and General Manager, Business Imaging Solutions Group, Canon U.S.A.


Hiro Imamura

When you think of security in an office setting, what comes to mind? Now picture that same office five years from now. Does the security landscape look the same? As the enterprises of today advance into the "Office of the Future," businesses nationwide will start to be even more connected. And while connected office solutions bring convenience that will help fuel collaboration and productivity, they also bring the potential for new vulnerabilities.

Confidential information is no longer confined to the walls of an office. We are working remotely – conducting business meetings from our self-driving cars, sending high priority emails from 30,000 feet up in the air, and maybe even using AR and VR to virtually meet and communicate with team members from around the globe. We are using AI to break down barriers and create a new document workflow process, but is this new level of transparency introducing new flaws?

In a sense, it almost seems like every employee in today's workforce needs to be an IT expert. Without the fundamental knowledge of how a data breach can happen, how can it be avoided? Yet, the reality we face is that everybody cannot be an IT expert. Acknowledging that the role of a future enterprise executive extends beyond traditional definitions of business technology can be fundamental to adapting your security framework for the office of the future.

> **"As businesses continue to evolve and embrace the digital transformation, they too must evolve their outlook on security"**

According to a study of 500 CIOs and IT decision-makers, conducted by IDC and sponsored by Canon U.S.A., 84% of business leaders surveyed say that network security is critical to digital transformation in the workplace, making it one of the first steps for organizations tackling enterprise security. And as such, future office leaders will need to emphasize the importance of utilizing network and device security protocols to help ensure their workers the freedom to work and collaborate remotely.

As more connected devices and virtual assistants enter the office, there will be a requirement for more sophisticated security measures in order to manage the enterprise network. Neglecting device security within an organization, for example, can create openings in workflow processes for employees and other outside members to share confidential business information – either intentionally or by accident.

And to take it a step further, the trend toward bring your own device (BYOD) policies plays its own role in the overall increase in work mobility. In fact, the introduction of personal mobile devices to the workplace led 77% of IT decision-makers and CIOs surveyed to consider mobile device management to be a priority for organizational information security and compliance, according to the same survey.

It will be important for enterprises to implement a robust security software suite across all in-office and mobile devices to help organizations manage document sharing in the cloud from employees' personal devices or to and from remotely connected office technology. In the immediate future, this may mean that companies looking to partner with digital solutions providers that can support remote accessibility and expansion of an organization's traditional document sharing network while keeping content security in mind.

84% of decision-makers surveyed said that they believe that content security in the cloud is a top security concern for 2018. User authentication schemas and encryption processes can help organizations provide a layer of protection surrounding the private data it shares across different regions and devices within its network.

Now when you think of security in an office setting, what comes to mind? The "Office of the Future" will be collaborative; it just too needs to be protected. As businesses continue to evolve and embrace the digital transformation, they too must evolve their outlook on security. CR

OFFICESPACE

# The leading standard in workplace management

OfficeSpace is the best platform for managing workplaces of every size. We give forward thinking companies the tools and insights they need to engage employees and create the workplace they've always wanted.


## ROOM BOOKING

Find and book the meeting rooms you need with ease from any device

## DESK BOOKING

Create bookable desks for hot desking or free addressing

## VISUAL DIRECTORY®

Give your employees interactive floorplans to find anything they need

## MOVE MANAGEMENT

Simplify your moves from single relocations to complex shuffles

## SPACE MANAGEMENT

Understand your real estate portfolio and make informed decisions

## REPORTS + ANALYTICS

Gain insight into your workplace with intuitive reports and real-time data

## REQUEST MANAGEMENT

Simplified work orders and service requests mean happy employees

officespacesoftware.com

# Treating vendors like employees can come back to bite you.

Easily identify, audit, and control third-party network access with SecureLink.

SECURELINK
VENDOR PRIVILEGED ACCESS

SECURELINK.COM 888.897.4498