Maturing operational security with an automation-first approach to IAM

Received (in revised form): 23rd July, 2021

Bryan Christ
IT Specialist, Texas, USA

Bryan Christ is an IT professional with almost three decades of industry experience. His fascination with technology started in the early 1980s with various models of the Commodore personal computer. He first published in 1991 and began his professional career a few years later. Along the way, he has worked for a number of high-profile companies including Compaq, Hewlett-Packard and MediaFire. Most of his career has been focused on open-source and software development opportunities with an emphasis on project management, team leadership and executive oversight. After serving two years in a full-time fractional CIO role in the Greater Houston area, Bryan carried his skills to Hitachi ID where he focuses on identity and access management. In addition to his work with Hitachi ID, he continues to serve as a fractional CIO as needed and frequently contributes to a number of SaaS-related endeavours.

34635 Wright Rd, 558, Pinehurst, TX 77362, USA
Tel: +1 832-257-7857; E-mail: bryanc@bkchrist.com

Abstract Over the last few decades, organisations have adhered to a number of security practices that are showing their age. With the explosion of remote work and software as a service (SaaS) adoption, this has become more pronounced. In pursuit of greater operational maturity, initiatives such as Zero Trust have placed these practices under scrutiny and the evidence suggests they are wanting. The rise of new technologies like adaptive authentication, enterprise federation and next-gen IAM offers new options and techniques — options that were once considered hypothetical. Among those worthy of consideration are an automation-first approach to identity and access management (IAM). In organisations where Zero Trust initiatives are being scoped, intelligent IAM can play a foundational role. Notwithstanding, IAM deployments should be regarded as multi-phase projects accompanied by unique obstacles that stakeholders would do well to avoid.

KEYWORDS: deperimeterisation, Zero Trust, identity and access management, operational maturity, identity and access management (IAM), identity governance, authentication, access requests, systems of record (SoR), joiner-mover-leaver (JML)

ALL DATA IS AT RISK: HOW WE APPROACH IDENTITY AND ACCESS MANAGEMENT MAY CHANGE THAT

From 2019 to 2020 the number of confirmed data breaches nearly doubled.[1] Forecasted trends show no signs of slowing and high-profile incidents such as SolarWinds, Microsoft Exchange and Colonial Pipeline serve to reinforce the same. With the average cost of a data breach nearing US$4m and long-tail impact exceeding 24 months,[2] the risk of inactivity is steep.

An automation-first approach to identity and access management (IAM) is a defining characteristic of an operationally mature organisation. It also plays a critical role in an enhanced identity governance-driven zero trust architecture (ZTA).[3] On the whole, 30 per cent of all breaches in 2020 were instigated by external actors, but the figure can be as high as 50 per cent depending on the vertical.[4] Moreover, when you consider that social engineering and phishing are the most common attack vectors, it becomes clear that in the 'hard-shell' model,[5] true vulnerability resides in the soft interior.

In the same way that overemphasising perimeter defence has led to a false sense of security, so has the governance-first approach to identity management. In part, the popularity of these refrains can be attributed to ease of implementation. It is relatively simple to deploy a firewall, configure some ingress/egress rules and call it a day. Likewise, setting up an access governance solution to ingest some data feeds and launching a few certification campaigns to satisfy an imminent audit is not terribly difficult. In fact, the motivation for doing so is often sadly reactive.

THE FUTURE OF IAM

In its most primitive form, IAM governs the relationship between identities and entitlements. This includes both human and non-human identities (users and devices) that request access to network resources, including those in the cloud and on-premises. Specifically, identities can include customers, partners and employees while network resources can include computers, smartphones, routers, servers, controllers and sensors. Conventional IAM efforts often involve routing new access requests through an IT service management (ITSM) system while periodically conducting attestation campaigns. For organisations that have minimal or no automation at all, this can be costly, time-consuming and error-prone. More often than not, these organisations generate a list of entitlements held by users, which is then circulated to managers, auditors and other stakeholders. In turn, these individuals manually validate the appropriateness of entitlements associated with each user.

The main objective of an IAM system, of course, is to govern identities and grant access to network resources in accordance with the principle of least privilege (PoLP). As more organisations embrace the philosophy of Zero Trust,[6] a fully automated IAM solution not only authenticates users and access requests, but it continually does so in response to business events that occur during the life cycle of an employee or other identity. This is in stark contrast to the conventional model, which provides only a snapshot in time and becomes largely obsolete with each passing day. This is one of many reasons why an automation-first approach to IAM is crucial to improving operational maturity and mitigating risk.

Speaking to this, one of the top industry analysts would say imperatively:

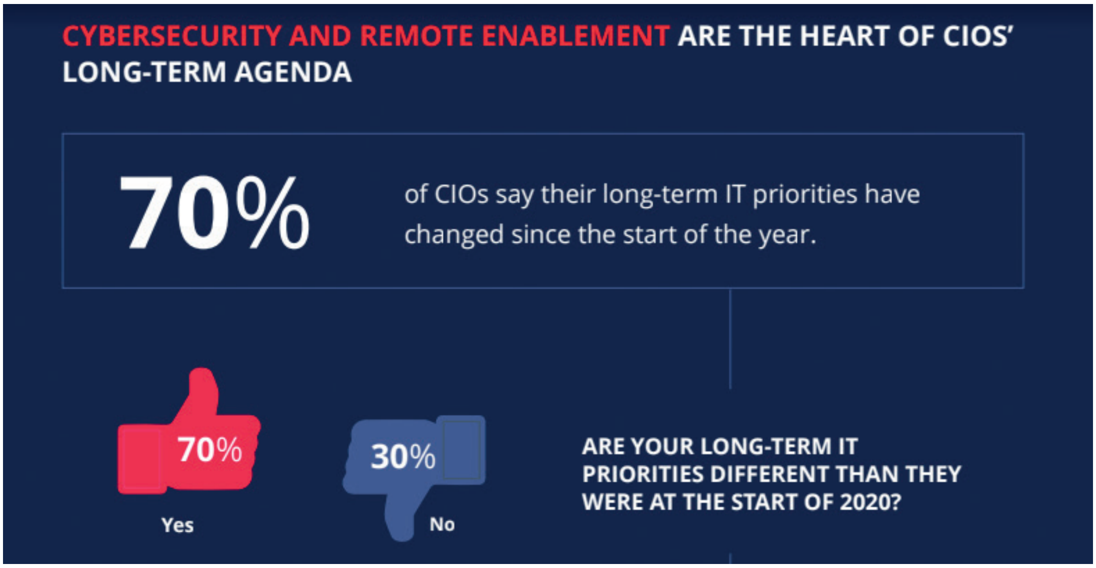
> 'You must fully automate access rights termination for joiners, movers, and leavers to ensure that they don't take sensitive data or continue to have valid accounts even after they've left the organisation.'[7]

On this point, they are not alone. Overwhelmingly, the market predictors agree:

> 'By 2022, more than 50% of IGA vendors will offer predictive, anticipatory and more autonomous governance engines leveraged by ML and AI identity analytics, up from less than 15% today.'[8]

A PROMISING SHIFT IN THOUGHT

A 2020 study of 131 chief information officers (CIOs) revealed that many IT leaders were forced to rethink their priorities and budget spend during the COVID-19 crisis (see Figure 1).[9] Now, as the economy slowly starts to regain speed, many are reconsidering their long-term strategies and which areas



CYBERSECURITY AND REMOTE ENABLEMENT ARE THE HEART OF CIOS' LONG-TERM AGENDA

70% of CIOs say their long-term IT priorities have changed since the start of the year.

ARE YOUR LONG-TERM IT PRIORITIES DIFFERENT THAN THEY WERE AT THE START OF 2020?

Figure 1: Cyber security and remote entitlement are the heart of CIO's long-term agenda

of cyber security they want to focus on as threats increase in frequency.

A complementary study from a leading analyst seems to confirm the shift is real:

> 'Over half of our enterprise respondents expect to increase IAM spending by 5% or more over the next 12 months.'[10]

Additionally,

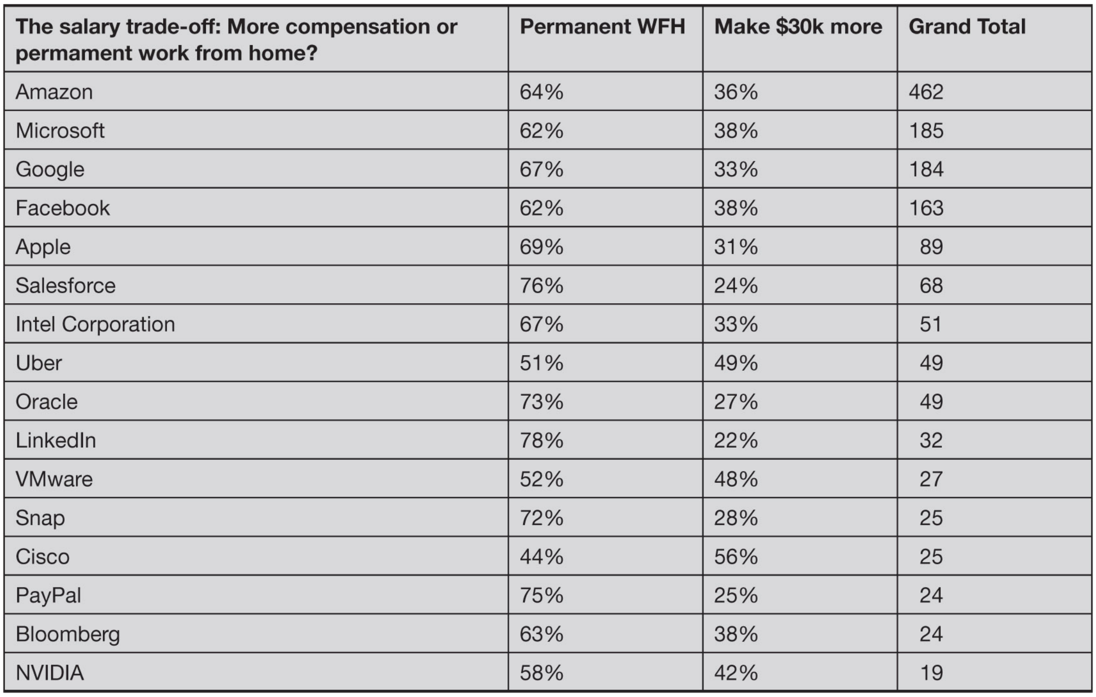
> 'Some 56% of respondents expect their organisation to increase IAM spending by 5% or more in 2020, up from 40% for 2019. High-profile breaches, an expanding list of global regulations, and increasingly sophisticated attacks, as well as the growing frequency of such attacks, are driving the need for ramping up security spend. While the COVID pandemic certainly harbors economic uncertainty, and likely lower budget expectations, it also highlights the criticality of IAM technologies as huge swaths of the workforce login from home.'[11]

Moreover, even when a sense of normalcy does begin to take shape, remote work and the risks associated with it are not going away anytime soon. A recent editorial on LinkedIn News showed that if people were given the choice of a US$30,000 raise or being able to permanently work from home, most people would choose to work from home. In fact, 64 per cent would rather stay home than take a pay raise (see Figure 2).[12]

While COVID-19, and all that came with it, was certainly the primary instigator, organisations have become increasingly introspective about maturing their operational security. For a significant number, that has placed IAM on the front burner.

SECURITY AND RISK MITIGATION

In today's world of digital transformation, accurate on-boarding and off-boarding of users plays a critical role in the modern enterprise, as it is inseparably linked to security and productivity. As more and more businesses store their sensitive data electronically, ensuring that data accessible to only authorised users is imperative. The rapid migration to the digital world has cut across all organisations and industries. It demands that companies shift their thought on workforce management and how they deliver



The salary trade-off: More compensation or permament work from home?	Permanent WFH	Make $30k more	Grand Total
Amazon	64%	36%	462
Microsoft	62%	38%	185
Google	67%	33%	184
Facebook	62%	38%	163
Apple	69%	31%	89
Salesforce	76%	24%	68
Intel Corporation	67%	33%	51
Uber	51%	49%	49
Oracle	73%	27%	49
LinkedIn	78%	22%	32
VMware	52%	48%	27
Snap	72%	28%	25
Cisco	44%	56%	25
PayPal	75%	25%	24
Bloomberg	63%	38%	24
NVIDIA	58%	42%	19

Figure 2: The salary trade-off

access to their applications and data. Over the last decade, the workforce has progressed from a relatively flat landscape to one that is far more complex and heterogeneous. In addition to providing access for employees, organisations must also concern themselves with contractors, vendors, partners and even consumers. Each of these user populations carry with them both direct and indirect ‘insider risk’, which is difficult to manage without moving away from legacy controls.

By contrast, a strong IAM programme, which emphasises automation, ensures that users have the right access privileges required for their job — no more, no less. Without it, bulk approvals for access requests, frequent changes in roles and departments and the lack of suitable processes for access reviews contributes to excessive access privileges, opening up the organisation to insider threats and magnifying risk throughout the business.

Supporting this statement, one study found that 50 per cent of respondents identified IAM as one of the most effective security tools to protect against insider threats.[13] Overseeing appropriate access through the right IAM security framework goes a long way toward bolstering an organisation’s risk management and security posture.

AUTOMATED ON-BOARDING MINIMISES RISK AND IMPROVES PRODUCTIVITY

From both a security and productivity standpoint, one of the biggest challenges is on-boarding and off-boarding users within an organisation. Deployed properly, an automation-first approach to access management can solve these challenges.

For most organisations, the on-boarding of a new employee, contractor, vendor or partner is often a labour-intensive manual process. Provisioning requests are often routed to the IT or helpdesk departments via an ITSM system. In turn, the staff are expected to predict which privileges and permissions to grant the user based on a limited set of information. For large-scale enterprises, this is highly complex and fraught with problems. Ultimately, this leads to protracted fulfilment times, loss of productivity and an introduction of risk.

To combat these problems, staff in these departments frequently resort to a strategy of cloning identities and their entitlements. It is the classic case of 'make Billy look like Bob'. If Billy and Bob are in the same department, there is a reasonable chance this strategy will work without any harmful side-effects; however, if Bob has significant tenure in the organisation and he has amassed some additional entitlements along the way, Billy is now grossly violating the PoLP on multiple fronts.

By contrast, an automation-first approach that leverages predictive intelligence can both expedite the joiner-mover-leaver (JML) processes and reduce the risk of human error. By monitoring multiple systems of record (SoRs), a robust IAM solution can consume identity attribute data and aggregate it in such a way that alleviates most of the guesswork. In other words, birthright access can vary from one class of user to another with minimal human engagement. For example, by evaluating the 'employee type' and 'department' attributes, a new contractor may be thinly provisioned with nothing more than an email account and an Active Directory login. Conversely, a new sales employee might be richly provisioned with access to a customer relationship management (CRM) application and memberships in a number of security groups.

Off-boarding employees manually can be equally challenging and costly. Without a canonical source of truth about what entitlements an identity holds (like an IAM system), it is difficult to determine what should be de-provisioned when an employee leaves. It must also be noted that even diligent IT staff are still prone to human error. An administrator might intend to de-provision an identity or entitlement, but distractions happen. This results in orphaned and dormant accounts which are attack vectors for hackers. Even when human actors follow through, they can be slow to respond, ultimately affecting the bottom line.

Furthermore, as data and applications spread across cloud, on-premises and hybrid infrastructures and are increasingly being accessed by a variety of mobile devices, including tablets, smartphones and laptops. These devices may be personally owned (bring your own device [BYOD]) and their security posture can vary wildly. An intelligent automation-driven IAM system can evaluate access requests based on the risk level of the request origin.

IDENTITY AND ACCESS AUTOMATION IS CRITICAL TO ZERO TRUST

For the unacquainted, Zero Trust is a security model based on a set of design principles that assumes a breach is inevitable or has likely already occurred. By considering all access requests and their origin inherently risky, the Zero Trust philosophy attempts to tame the Wild West of identities. It is a paradigm shift in perspective. At the heart of the ZTA model described by the National Institute Standards and Technology (NIST) is the policy decision point (PDP). The PDP is composed of the policy engine (PE) and the policy administrator (PA). A cursory examination of the PDP and its sub-components is sufficient to realise that it presupposes a high degree of automation. A fully automated IAM solution will contextually authenticate users and evaluate access requests. This can serve as a critical component of the PDP. In fact, an intelligence-driven IAM solution that delivers a frictionless experience is foundational for a Zero Trust strategy.

PLANNING FOR A SUCCESSFUL AUTOMATION-FIRST IAM PROGRAMME

IAM, like any large programme or technology initiative, can fail for a variety of reasons. As with any major project, there are usually several factors that, when present, make real and meaningful success nearly impossible to achieve. For IAM, the lack of stakeholder support, misguided beliefs about data integrity and roles, and a heavy reliance on existing systems are a few common pitfalls.

Planting the seeds for success

IAM has an impact on every department. For this reason, it is imperative to build and garner stakeholder support across the organisation as soon as possible. It cannot be overstated how important it is to build cross-department support, including human resources (HR), change management and those who deal with regulatory compliance. The ideal outcome would be a fully commissioned working group tasked with automating IAM.

In some cases, it might be helpful to bring in a consultant that specialises in IAM deployments. As subject matter experts, they bring a wealth of knowledge and experience to the table. Having worked with other organisations and their IAM projects, they are in a unique position to recognise common problems and help navigate solutions. Moreover, good ideas, especially those that demand cross-department collaboration, can become easily politicised. As an independent party, a consultant can help mediate and deflect these issues.

As with any technology implementation, it is critical to put a competent project manager at the helm who can ensure that milestones are met and budgets managed. In all but the rarest of circumstances, a ‘boil the ocean’ approach to deployment is destined to fail. In fact, a successful IAM deployment is really a programme — a set of iterative projects intended to be executed in several phases. This is especially true if the IAM deployment is part of a Zero Trust initiative. A seasoned project manager will understand this.

Common pitfalls to avoid

In finer detail, an automation-first approach to IAM means continually monitoring one or more SoR, intelligently consuming identity and resource attributes, aggregating it in meaningful ways and ultimately affecting change to various entitlements based on business processes and policies. When these attributes change as a result of a business event, the expectation is that entitlements and user access change accordingly — and automatically. Excluding budgetary reasons, most attempts to deliver an automation-first approach to IAM become snakebit by issues related to planning and business policy.

Paralysis by analysis

In an automation-first approach to IAM, a robust solution will respond to business events. This means that the entire identity life cycle is managed from cradle to grave. This is commonly called JML processes whereby various create, read, update and delete (CRUD) operations are applied to identities and their entitlements in response to business events. Many IAM projects exceed both their project milestones and budgets because they fall victim to two common misconceptions. These misconceptions take root when project planners over-analyse JML and CRUD in an overly fine-grained manner. The first is the belief that SoR data must be pristine and free from defects — a red herring of sorts. The second is the belief that roles must be defined before deployment. Neither of these are true and seem to reflect a ‘boil the ocean’ approach to deployment rather than one that is agile and data-driven.

The red herring of imperfect data

Almost every organisation has at least one SoR. Even when the data contained therein is flawed, it generally rises to the threshold of ‘good enough’. If an organisation ever falls below this threshold, it seldom lingers in such a state. A crippled organisation, which cannot perform primitive operations such as on-boarding and off-boarding employees and paying their staff and vendors, will certainly face outcry sufficient enough to evoke corrective action.

By implementing an automation-first approach to IAM, organisations can realise immediate gains by focusing on automated on-boarding with birthright access in the first iteration of the project. When dirty SoR data becomes a barrier to an on-boarding event, the same corrective action can be taken. This provides an opportunistic way of cleaning up the SoR while simultaneously benefiting from automation.

Death by a thousand roles

From an enterprise point of view, roles should be used sparingly to define communities of users who hold the same entitlements. Roles should be determined by letting analytics identify these communities and their related entitlements. Most attempts to guesstimate role definitions in the planning stage are counterproductive and often lead to an excessive number of roles. In fact, trying to define too many roles could be the kiss of death …

> ‘Companies that try and establish roles for an entire enterprise, as opposed to one application or department, could end up with as many roles as there are employees’ … It’s hard to maintain because the business is always changing. So you must start small and look at all of this identity management as evolutionary.’[14]

In other words, IAM does not depend on role-based access control (RBAC) and RBAC does not strictly require IAM, but RBAC is much easier to deploy once an IAM system is in place.

USING THE WRONG TOOL FOR THE JOB

Many organisations have invested heavily in their ITSM tools. At first glance, they appear to share some similarities with IAM products but using them in such a manner is misguided. While it is possible to route access requests through a service catalogue or a ticket request portal, ITSM tools often lack the privacy and automation controls that are found in a modern IAM solution. To be clear, IAM and ITSM products are not mutually exclusive; rather, they are complementary. Just as IAM products would be wholly unsuitable for general help desk operations, ITSM is not well suited for automating JML processes. Without heavy scripting and supplemental customisation, they cannot consume and aggregate identity from HR or other SoR systems, nor do they have awareness of existing entitlements already provisioned. When operating alongside IAM automation, however, they are an excellent mechanism for providing input and output feeds, such as a secondary audit trail. In fact, if an automated IAM deployment is part of your Zero Trust strategy, then a well-integrated ITSM becomes symbiotic with the components of your PDP. Beyond that, trying to push your ITSM into operations it was never designed for can be both costly and failure prone.

WHAT ABOUT GOVERNANCE?

Identity and access governance (IAG) is largely concerned with the audit and certification of entitlements. In most implementations, data is ingested from multiple feeds, and in response stakeholders at various levels are invited to act. These campaigns are designed to verify that the entitlements held by users in the organisation are assigned appropriately. By going through this process, it often reveals other types of risk (such as orphaned and dormant accounts) that may put the organisation in regulatory jeopardy. In fact, many organisations adopt a IAG programme as a hasty reaction to an imminent audit — or even worse, a failed audit. The problem with a governance-first approach to IAM is that it is not sustainable. In other words, when automation is not constantly reacting to and managing the JML processes on a consistent and perpetual basis, the audit campaign quickly becomes outdated. In a fluid organisation where users are constantly being on-boarded, transferred and off-boarded, certification becomes but a mere snapshot in time. This is not to say that IAG has no value — quite the contrary. IAG is complementary to an automation-first approach to IAM because it supplies stakeholders with an opportunity to validate the fidelity of automation. In this way it provides assurance for an imminent audit and an opportunity to fine-tune automation where necessary.

IAM: WHERE DO WE GO NEXT?

Achieving a higher level of mature operational security is critical, even in a post-COVID world, and the gold standard for security is Zero Trust. With no shortage of signals, the evidence is clear: a larger remote workforce is here to stay.[15] Just as relying heavily on the perimeter fosters a false sense of security,[16] the same is true for a governance-first approach to IAM.

Getting started with an automation-first approach to IAM does not have to be difficult, especially when efforts are properly scoped and treated as a programme. In other words, a multi-phased approach to deployment that delivers IAM as a series of iterative projects will greatly increase the potential for success. In planning these projects, the key is carving the phases into manageable chunks, setting realistic expectations, and avoiding the deceptive pitfalls that cause an initiative to stall or fail to launch. Lastly, make certain to evaluate the initiatives on a periodic basis against industry standards to ensure lessons learned are incorporated and to keep the security posture of the organisation strong by adopting continually improved IAM practices.

References

1. Verizon 2019 DBIR (see https://www.nist.gov/system/files/documents/2019/10/16/1-2-dbir-widup.pdf) versus 2020 DBIR (see https://www.verizon.com/business/resources/reports/dbir/) (both accessed 23rd September, 2021).
2. IBM, 'How Much Does a Data Breach Cost?', pp. 5, 58, available at https://www.ibm.com/uk-en/security/data-breach (accessed 23rd September, 2021).
3. NIST, 'SP 800-207 Zero Trust Architecture', pp. 11, 12, available at https://csrc.nist.gov/publications/detail/sp/800-207/final (accessed 23rd September, 2021).
4. Langlois, P. (2020) '2020 Data Breach Investigations Report', p. 54, Verizon, available at https://www.cisecurity.org/wp-content/uploads/2020/07/The-2020-Verizon-Data-Breach-Investigations-Report-DBIR.pdf (accessed 23rd September, 2021).
5. Cleeff, A. van and Wieringa, R., 'Rethinking De-Perimeterisation: Problem Analysis And Solutions', Drienerlolaan 5 7522 NB Enschede, University of Twente, The Netherlands, available at https://ris.utwente.nl/ws/portalfiles/portal/5414132/IADIS2009_RETHINKING_DE-PERIMETERISATION.pdf (accessed 17th October, 2021).
6. Mahon, D. (June 2021), 'Is Security An Illusion? How A Zero-Trust Approach Can Make It A Reality', Forbes Technology Council, *Forbes*, available at https://www.forbes.com/sites/forbestechcouncil/2021/06/28/is-security-an-illusion-how-a-zero-trust-approach-can-make-it-a-reality/ (accessed 23rd September, 2021).
7. Cser, A. and Ryan, S. (September 2020), 'Transform Your IAM Strategy To Succeed In The Post-Pandemic World', Forrester, available at https://www.forrester.com/report/Transform-Your-IAM-Strategy-To-Succeed-In-The-PostPandemic-Era/RES161297 (accessed 23rd September, 2021).
8. SCRIBD, '100 Data and Analytics Predications Through 2024', available at https://www.scribd.com/document/499666296/721868-100-data-and-analytics-predictions-through-2024 (accessed 17th September, 2021.
9. Hitachi HD (August 2020), 'Half of CIOs Are Increasing IT Budgets, 43% Focused on Identity and Access Management, Hitachi ID and Pulse Survey Shows', available at https://www.hitachi-id.com/aboutus/news/press-releases/2020-08-11 (accessed 23rd September, 2021).
10. Ryan, S. and Cser, A. (April 2020), 'Understand the State of Identity and Access Management, p. 5, Forrester, available at https://www.forrester.com/report/

Understand-The-State-Of-Identity-And-Access-Management-2020/RES159981 (accessed 23rd September, 2021).

11. *Ibid*., ref. 10.
12. Prudente, G., '$30K raise or work from home?', LinkedIn, available at https://www.linkedin.com/news/story/30k-raise-or-work-from-home-5059540/ (accessed 23rd September, 2021).
13. Schulze, H. (2019), '2019 Mid-Year Insider Threat Report', p. 17, Cybersecurity Insiders, available at https://www.cybersecurity-insiders.com/wp-content/uploads/2019/11/2020-Insider-Threat-Report-Gurucul.pdf (accessed 23rd September, 2021).
14. Radcliff, D. (November 2004), 'Identity Management int the Real World', CSO, available at https://www.csoonline.com/article/2117567/identity-management-in-the-real-world.html (accessed 23rd September, 2021).
15. Castrillon, C. (December 2020), 'This is the Future of Remote Work In 2021', *Forbes*, available at https://www.forbes.com/sites/carolinecastrillon/2021/12/27/this-is-the-future-of-remote-work-in-2021/ (accessed 23rd September, 2021).
16. Security Boulevard (May 2021), '10 Exploits Cybersecurity Professionals are Concerned About', available at https://securityboulevard.com/2021/05/10-exploits-cybersecurity-professionals-are-concerned-about/ (accessed 23rd September, 2021).