Right way to establish critical pro-active defences against emerging cyber threats

Andrew J Clarke

Director, One Identity

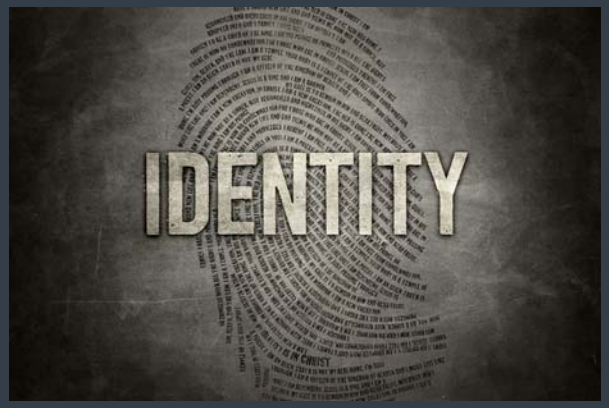
ONE IDENTITY

A fast changing world

Digital Transformation

Internet of Things (IoT)

The new attack vector



…network credentials that were stolen from a third party vendor

The group apparently compromised a VEVO employee account for the single-sign-on (SSO) workplace app Okta.

Equifax's website in Argentina allegedly were protected by the same generic username and password: "admin."

Identity and Access Management (IAM)

- Identity and access management (IAM) is a security, risk management and business discipline, and it is a set of processes and technologies that manage the identities and entitlements of people, services and things, and the relationships and trust among them. It provides the right access for the right reasons, enabling the right interactions at the right time, to help drive business outcomes.

- IAM highlights a continued overall trend toward technology maturity, as several technologies have broadly penetrated the market to enhance operational efficiency, enhance security effectiveness and enable business

Survey : Goals and Methodology

Research Goal

The primary research goal was to understand current experiences and challenges around Identity Access Management (IAM) and privileged accounts.

Methodology

An online survey was fielded to independent databases of IT professionals with responsibility for security. A wide variety of questions were asked about experiences and challenges with IAM.

Participants

A total of 913 individuals completed the survey. All had responsibility for IT security as a major part of their job and were very knowledgeable about IAM and privileged accounts.

Survey reveals old fashioned IAM processes still widely used, leaving organisations ripe for breaches and disruptions

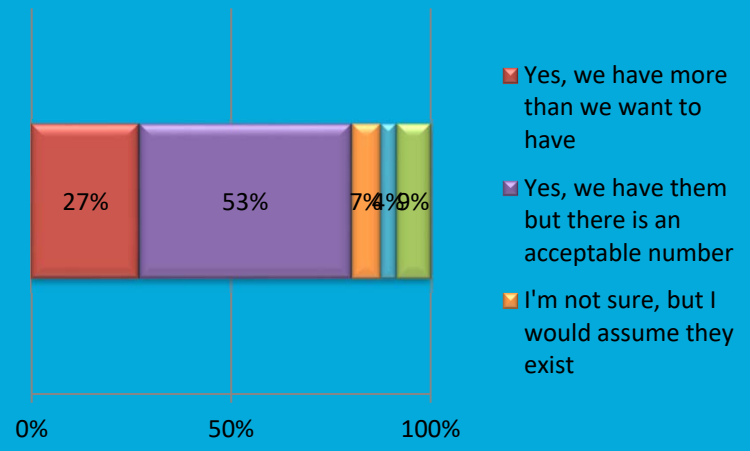
- Despite years of high-profile breaches, it turns out that a significant number of organisations still aren't close to applying best practices to their IAM processes, which leaves them and their users vulnerable to attacks and data breaches

- The survey shows that:
  - 71% of survey respondents have concerns about risk from dormant accounts
  - Just one in four (25%) are "very confident" that user rights and permissions are correct
  - Despite concerns, nearly a quarter of respondents audit accounts annually or less frequently - including two-percent that never audit!
  - Most respondents have some sort of process to identify dormant accounts, but less than 20% have tools to find and monitor them

To access the full survey results: https://www.oneidentity.com/whitepaper/survey-reveals-that-old-fashion-iam-processes-are-still-widely-used-wh8129464/

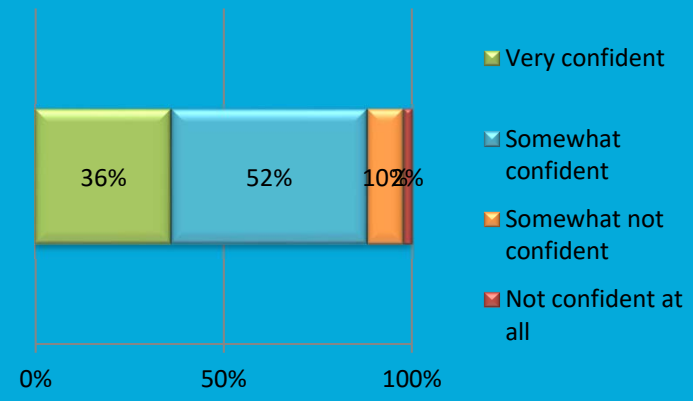
87% have dormant users

Does your enterprise have dormant users, where the accounts associated with the identities are not being used?



Only a third are very confident they know which dormant users accounts exist

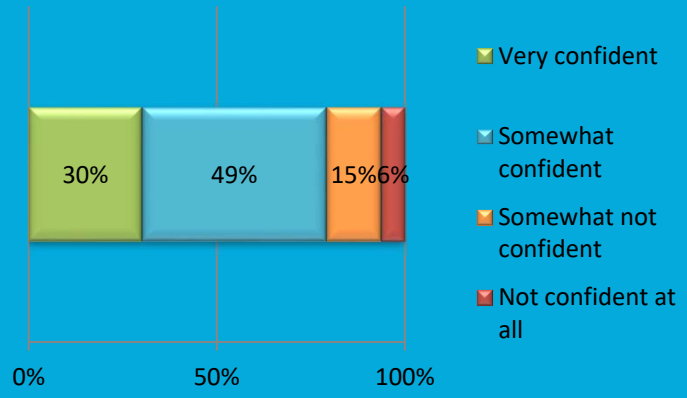
How confident are you in knowing which dormant user accounts currently exist?



ONE IDENTITY

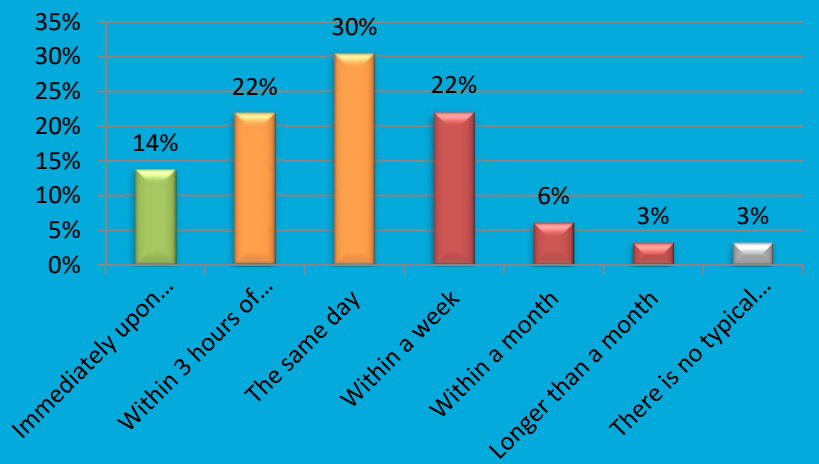
Less than a third are very confident that their users are deprovisioned properly

How confident are you that all former users are fully de-provisioned in a timely manner (i.e. before retained access becomes an unacceptable risk)?



Only 14% de-provision a user immediately upon change in status

How long does it typically take to de-provision a user?



Inadequate IT Processes for Managing User Accounts and Access Continue to Create Major Security and Compliance Risks

- Disgruntled former employees or other threat actors still have widespread opportunity to cause harm because their IT accounts remain active
  - 70% of respondents lack confidence that accounts of former employees are fully deactivated in a timely manner
  - 84% percent of respondents say it takes a month or longer to discover forgotten dormant accounts

- Results show that common IT security best practices continue to be a challenge for organisations worldwide

Notable finding : Internal threats as well!

Businesses around the globe have a major employee snooping problem

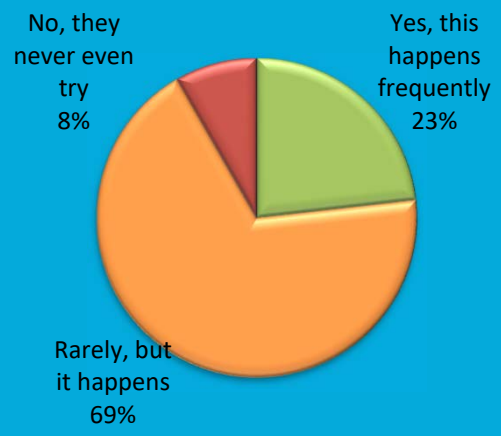
- 92% of respondents report that employees attempt to access information they do not need for their day-to-day work.
- Nearly one in four (23%) of respondents report employees frequently attempt to access information that is irrelevant to their daily job functions.

IT security professionals are among the worst snoopers – and get worse with seniority

- More than one in three (36%) of IT pros admit to looking for or accessing sensitive information about their company's performance, apart from what is required to do for their job.
- Nearly two in three (66%) IT security professionals admit they have specifically sought out or accessed company information they didn't need.
- 71% of IT security executives admit to seeking out extraneous information, compared to 56% of non-manager-level IT security team members.
- 40% of executives admit to snooping for or accessing sensitive company performance information specifically, compared to just 17% of non-manager team members.

92% say employees attempt to access information they don't need

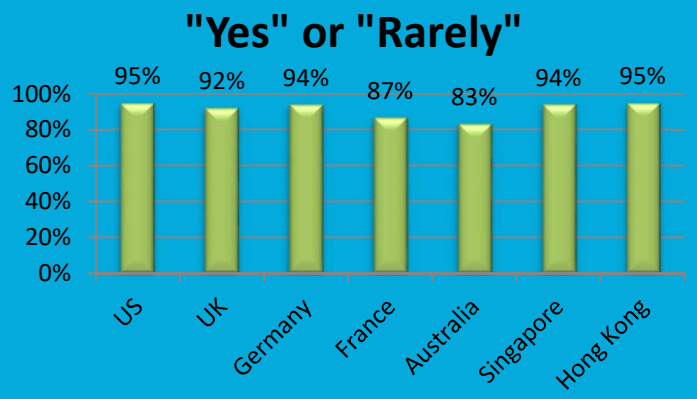
In your experience, do EMPLOYEES ever attempt to access information that is not necessary for their day-to-day work?



Employees from every country attempt to access information they don't need

In your experience, do EMPLOYEES ever attempt to access information that is not necessary for their day-to-day work?

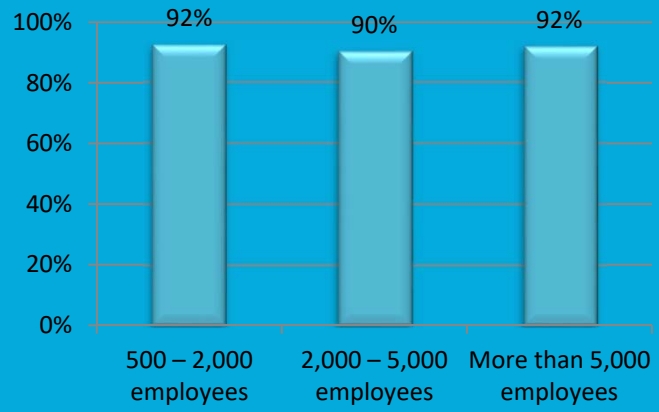
(by region)



Employees at every size company try to access information they don't need

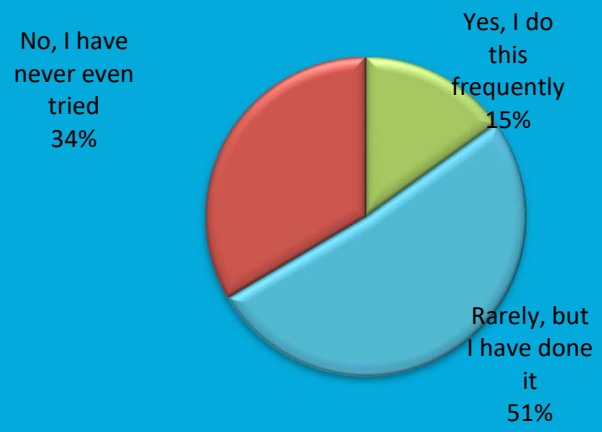
In your experience, do EMPLOYEES ever attempt to access information that is not necessary for their day-to-day work?

(by company size)



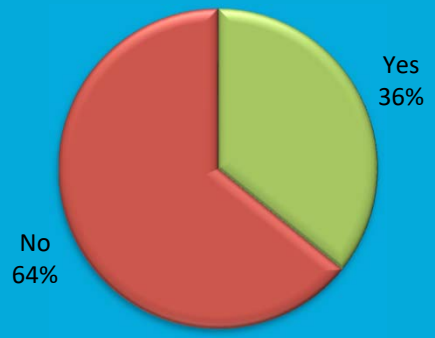
2 in 3 (66%) have tried to access information they didn't need

Have YOU ever attempted to access information that is not necessary for your day-to-day work?



More than 1 in 3 have accessed sensitive information about company performance

Have you ever looked for or accessed sensitive information about your company's performance, apart from what you are required to do as part of your job?



Credential-Based Attack Vectors

- One of the easiest ways for malicious outsiders, or even insiders, to gain access into an organisation's IT network is by stealing user credentials such as user names and passwords.
- Once access is secured, a series of lateral movements and privilege escalation activities can procure access to the type of information and systems that are most coveted by bad actors, such as a CEO's email, customer or citizen personally identifiable information, or financial records.
- The more time inactive accounts are available to bad actors, the more damage can potentially be done, including data loss, theft and leakage, which could end up in irreparable damage to reputations, compliance violations, as well as possibly large fines and a significant drop in stock valuation.
- Exploitation of excessive or inappropriate entitlements remains a goldmine for threat actors who will then capitalise on access to gain a foothold in an organisation to steal data or inject malware.
- Accelerate the deprovisioning of access, proactively discover dormant accounts, and help ensure appropriate access rights across the entire organisation and user population

Lessons learned from the survey

- The survey results expose that most companies are not adhering to best practices regarding user access control and governance, enabling employees to snoop and gain access to unpermitted information on the corporate network, potentially putting organisations at risk
- By not putting basic identity and access management (IAM) processes into practice, organisations allow employees to move through the enterprise to access -- and even share -- sensitive information. Financial performance data, confidential customer documentation, or a CEO's personal files are just a few examples of information that could result in major reputational or financial damage if accessed and exposed by the wrong person or group
- Best practices such as role-based access control and strict governance of rights and permissions can help prevent employees from accessing confidential or sensitive information
- With regard to snooping done by IT security team members and other employees with elevated rights, organisations can leverage identity intelligence and effective privileged access management to identify who has those elevated rights and easily put controls around unauthorised access behaviour

What happens if you don’t get it right?

- It becomes difficult to achieve objectives
- You lose your competitive edge
- Your organisation may suffer irreparable harm
- People lose their jobs, reputations, suffer possible fines and legal penalties

Every high-profile breach is due, at least in part, to the misuse or abuse of legitimate user credentials.
In other words, these breaches could have been avoided with better **identity and access management.**

Translation: “ To hold the line on security and compliance, you must Get IAM Right

What does right looks like?

The **right** people are in control

You achieve the outcomes that drove the program in the first place

Security is considered an ally, not an enemy, to organisational success

Your IAM program covers all of your needs today, and paves the way for future **success**

IAM has transitioned from a barrier or obstruction into an enabler

Your IAM program is a top-line revenue generator

Your vendors, service providers, and partners focus on **your** success, not just theirs

What does right look like?

The right people

Employees, administrators, partners, customers, whomever

In all the ways they want

On-prem, remote, mobile, company-controlled devices, BYOX, and over any connection

With the right governance

The line-of-business decides what is right and is able to attest to it

The right access

Precisely what they need to do their jobs… no more, no less

To the right resources

Applications, on-prem, in the cloud, SaaS and privileged accounts

At the right time

During regular work hours, but also anytime anyone wants or needs access as well

And you can prove it

To whatever regulation or framework you need to adhere to whenever it is requested

Summary

- IAM technologies are predominantly infrastructure technologies
- They are implemented to support one or more business process improvements or compliance initiatives
- Many of the business benefits from IAM adoption are indirect and are not easily made visible to the business
- The ability to deliver accountability and transparency of access to the business remains important
- IAM has a significant opportunity to deliver direct business value by enabling easy, lower cost, risk-managed interactions with partners and customers
- **IAM is the right way to establish critical pro-active defences against emerging cyber threats**

www.oneidentity.com