IDENTITY AND ACCESS MANAGEMENT: A GUIDE TO BEST PRACTICES

www.dig8ital.com

dig8ital

Contents

The problem of credentials theft cannot be overstated. Organizations around the world are suffering serious data breaches because cyber espionage groups have been able to get a hold of sensitive passwords and, thus, gained access to their systems.

In fact, personal credentials is the most sought-after data type by hacker groups, and it was found that credentials are also the fastest to compromise compared to other data types (Verizon).

Best practice identity and access management (IAM), therefore, is essential to protecting your business from cyber threats. This guide will discuss six elements of best practice IAM, what they are, and offer practical tips for implementing them.

1

Identity and Access Management

Access management, also known as identity and access management, is the umbrella term for the process of assigning digital rights to IT systems to users and apps. Used in conjunction with an access control system, it covers the allocation, renewal and revocation of permissions in line with key policies, i.e. JML (see page 11).

On this page we will discuss IAM broadly, but each following chapter in this guide forms another core piece of the IAM puzzle. You wouldn't generally choose one or the other best practice, but rather try to adopt most or all of them.

WHY IS IAM SO IMPORTANT?

We know that credential theft is such a huge issue. IAM tries to prevent unauthorized personnel from accessing certain resources and information even if credentials are stolen, and it can help contain a breach from spreading to multiple systems.

Additionally, it can be used to keep third-party apps in line, able to access only what they require to function properly – so you can't be compromised through your vendors, either.

Overall, IAM is critical to the security, efficiency and regulatory compliance of a modern organization.

PRACTICAL TIPS FOR IMPLEMENTING IAM

Stop using traditional security approaches such as role-based or attribute-based authentication and start thinking about a mixture of both.

- Here we're creating a policy based on access controls.
- Consider the business role of the user in combination with your strategic policies to determine whether someone should have privilege or not.
- This makes an IAM approach more resilient and flexible.

Reviewing and scanning privileged permissions

- Who has the power not just to access the system, but make modifications? Who are your admins?
- Can you justify generic admin accounts? Is it enough to know who has access to the account if you cannot identify which individual was accountable in the event of a data breach?
- Consider making permissions temporary, so users must re-request on a regular basis. They only need permission for as long as it is required for the work they are doing.
- Don't forget your apps! They are users too, and must follow the same rules.

2

Good IAM Strategy and Governance

Just like everything else in business best practice, IAM too needs a strategy behind it. Strategy can help you understand the who, what, when, where, why and how of IAM, allowing you to implement critical policies aligned to the wider organizational plan.

Then there's good governance. Governance is like the right hand of the strategy – helping record, monitor and update IAM policies at regular intervals, and ensuring it's all stored safely and securely.

WHY IS IAM STRATEGY/GOVERNANCE SO IMPORTANT?

As we discussed, strategy is your guiding plan. With a carefully designed strategy, you'll be able to articulate who needs access to what, when, why, and how that will occur (and for how long it is granted). Additionally, this will fit with your wider business strategy and risk appetite, to ensure it suits your needs.

From here, you'll understand where you need to get to with your IAM investment. This understanding can help you transform more efficiently, as you'll know to invest in only what your unique business requires in terms of training, tools and time to achieve the devised plan.

Then, by keeping up good governance, you'll be recording each of these new policy changes and keeping them updated. This will help you prove to regulators that you tried your best in the event of any audit or data breach.

Learn more: 'How to implement digital transformation'

2

PRACTICAL TIPS FOR IMPLEMENTING IAM STRATEGY/GOVERNANCE

1. **Understand your five Ws and H**
   a. **Why** are we investing in IAM? What is the purpose? How do we define success?
   b. **Who** in our organization has access to the system, and who requires it? What training do they already have?
   c. **Where** are our users located? Will this remain constant or change? Can it be adaptable? (i.e. remote working)
   d. **What** devices are people using, what training do they have, what existing IAM policies already exist and what tools are we already using (if any)?
   e. **When** do people need access, and for how long will they need it?
   f. **How** do people use the current system, and how disruptive will change be? What change management is required to carry staff from A to B?

2. **Other important considerations**
   a. Determine how you will measure the success of the transformation and plan to revisit these KPIs in six to 12 months to check in on progress.
   b. Assign owners to the new policy. Who owns the IT systems, who owns the policy, who is accountable, who is going to keep it up to date and measure success?
   c. Involve the board in discussions on access so they understand why it is changing and the importance of the change (and to ensure they abide by the policy, too). When presenting to the board, translate any IT jargon into business language so it is accessible and can be quickly understood.

3

Password Management

Credentials might be relatively easy to compromise, but we can make it harder. Password management is a set of principles and best practices to be followed by users to help them create strong passwords which are harder to crack.

WHY IS PASSWORD MANAGEMENT IMPORTANT?

A strong password can be the difference between a hacker breaking in instantly through a user's account or never getting in at all. They are, essentially, the first line of defence.

- **Bonus fact:** Weak or stolen passwords are responsible for more than 80% of hacking related breaches (Verizon)

Strong passwords are harder to guess, or brute force.

Unique passwords, where users have a different password for every account, ensure that if one such password is compromised, bad actors still have only limited access – they can't get into everything.

PASSWORD BEST PRACTICES

- Unique password for every account inside and outside of work.
- Minimum of 8 characters, using upper and lower case, symbols and numbers.
- Don't use personal information.
- Change passwords regularly.
- Never share your password.
- Always click 'never' if a browser or system wants to remember your password.

Bonus fact: Hackers with the tools to brute force a password can crack phrases of less than 8 characters and no symbols/numbers instantly. However, up that password to 13 characters and include upper and lower case letters (not even numbers or symbols) and it would take 16,000 years. (Hive Systems)

What about your apps?

Password and access management for applications is quite a bit more technical – a lot more than we could write in this guide. For expert help securing your third-party vendors, contact us today and we can talk about your organization's unique needs.

4

Multi-factor Authentication

Multi-factor authentication (MfA) is a type of electronic authentication where users aren't granted access unless they can present two or more pieces of evidence – i.e. a password and then confirmation number sent via email or SMS.

Some authentications also require multiple devices (like Facebook's Code Generator). Other examples include identifying questions, fingerprint scans, face ID, voice recognition, and so on.

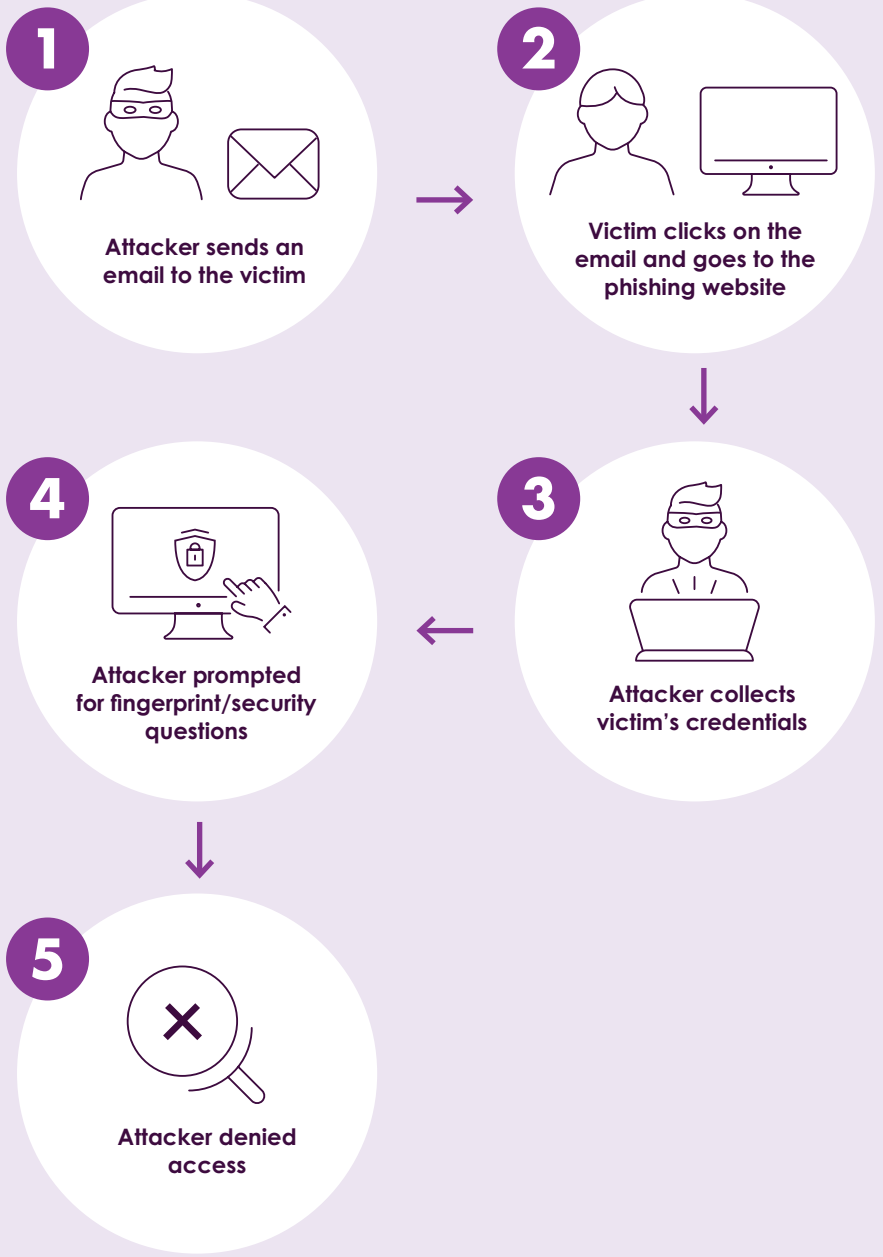
WHY IS MFA SO IMPORTANT?

MfA takes the best of password management and makes it even stronger.

Should a hacker manage to steal an employee's credentials, they still only have one half of what they need to log in. In theory, this means the system is protected by an additional security layer even if users have weak, forcible passwords.

A bonus here is this can help protect businesses from the rising risk of staff using personal devices, which are typically easier to compromise than a company computer.

Finally, MfA is also looked upon favourably by regulators, enabling organizations to improve their compliance levels.



4

PRACTICAL TIPS FOR IMPLEMENTING MFA

MfA is implemented through an MfA solution, which means choosing a provider.

- Fully scrutinize all MfA providers to determine cost, flexibility, scalability, service functions and options, support, updates, and the security policies of the company itself (i.e. how is the vendor protecting its own systems).
- We should also note that many apps are now building MfA natively into their services. As such, some third-party MfA authenticators may not be compatible with your apps – so you'll need to do some research to find the best solution for your needs.

COMMON MFA AUTHENTICATORS

- Google Authenticator
  (Download via Google Play or the Apple App Store)
- Microsoft Authenticator
- Duo Security
- Last Pass
- Ping Identity

OTHER MFA BEST PRACTICES

- Prioritize privileged and important users first for roll-out, in addition to any roles where a breach would have high impact on the company.
- Try to make MfA easy on employees – offer a choice of factors so they can select those which suit them best. Not everyone will want to use, say, voice recognition, or SMS codes.
- Communicate regularly and engage staff with training. Change management is vital for staff to accept transformation.
- Assign an owner or owners for the MfA system so there is accountability and a chain of command – someone to go to for support.
- Determine how to measure success of the MfA rollout and monitor these KPIs regularly to gauge success and look for opportunities to optimize.

5

Single Sign-on

Single sign-on, or SSO, is a system that allows company employees to sign in only once and access all the relevant corporate apps to their access level (like signing in to Google Chrome, which allows you to access Gmail, Drive, Docs, etc., without logging in multiple times).

Instead of needing to invent, store and change multiple passwords for multiple apps, users require only the one.

WHY IS SSO IMPORTANT?

It may seem counterintuitive to suddenly talk about only having one password after stressing the importance of password management. But, there are benefits to SSO platforms.

- **Security:** SSO reduces the attack surface for hackers – they can't pick and choose from a variety of weak passwords, but must crack a central, highly protected system. The central system can be carefully controlled by admins, and training deployed to ensure passwords are strong, MfA is in place, etc.
- **User experience:** Users don't need to remember a number of different passwords but instead must ensure that they keep their single password strong and secure, and updated regularly. Plus they only need to log in once and can then access what they require for that particular task.
- **Admin experience:** By using an SSO platform, access administrators can centrally manage who can access what, when, and in what way. In the event that someone leaves the company, for example, the user will simply have to be unsubscribed from the SSO platform and automatically lose access to all the platforms that adhere to the authentication system.

5

PRACTICAL TIPS FOR IMPLEMENTING SSO

SSO is quite technical and cannot be easily described in a simple PDF guide. To get the best results, we recommend the use of a cyber security expert to help you. The following are general tips to consider as you approach expert help.

- You don't have to do it all at once – consider a phase-based implementation approach starting with priority systems or subsets of users and expand from there. This can reduce complexity and allow for testing.
- Catalogue every app and system that users will require access to, and any specific requirements of these systems.
- Run workshops with app owners and end users to gain an understanding of day-to-day use cases and requirements of apps so the SSO tool can support their work, not hinder.
- Consider whether you will wish to run SSO on-prem or use a cloud-based model (i.e. an SSO vendor).

Learn more:
'5 multicloud security challenges and how to address them'

6

JML Policy

JML stands for joiners, movers and leavers. A JML policy, therefore, is one where there are clear guidelines in place to govern the access levels of anyone being onboarded, moved to a new role or department, or who is resigning.

WHY IS A JML POLICY IMPORTANT?

People are always flowing through a company, coming and going, changing, being promoted. Access levels have to be able to keep up.

So, a strong JML policy is a way for admins to keep track of users as their access needs change. Someone might gain more access as they earn that promotion, or leavers can be removed from the system promptly so as not to create a security vulnerability (i.e. a dead account, no longer updated, and potential avenue for a disgruntled ex-employee to keep accessing sensitive company information).

HR typically owns this process but they might not be aware of the different applications and services that the IT department is using. So, they'll likely need help, or else someone else may become responsible for managing the decommissioning or even onboarding of permissions and access.

PRACTICAL TIPS FOR IMPLEMENTING IT

- Start keeping track of joiners, movers and leavers. This goes for permanent staff, part-timers, interns, contractors, even third-parties. You must track exactly what they can access, where, and when, based on their changing needs.
- Implement procedures to enforce the policy and ensure that all stakeholders are working together to update it (i.e. when a new service is started, or new roles created). HR will generally own this, but needs help.
- Identify any segregation of duties (SoD) in your business, as this will also impact JML access rights.
- Have you hard-coded SoD into a policy which is regularly updated? How confident are you that the policy is being applied when employees join, move or leave?
- Ask yourself: Can you clearly identify in the system who is employed by you and who is not? Understanding the difference will be key to embedding the right access control policies.

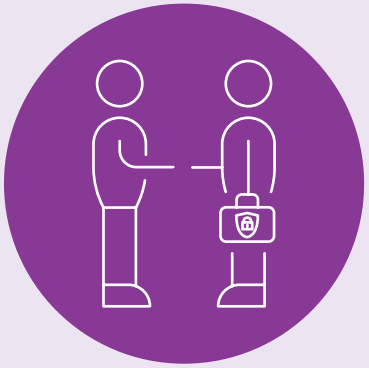
Conclusion

If credentials are one of your company's biggest weak points, identity and access management must be considered a top priority. By implementing the best practices we've discussed today, your business will ensure:

- Employees create strong passwords and update them regularly.
- Access rights can be managed centrally and kept highly secure.
- No one has unlimited access to the system, and access rights are always temporary.
- Staff joining, moving or leaving are kept track of, and access modified as necessary.

With these in place, even should outside actors gain access to your systems – either through phishing, social engineering, brute force, or other means – they will still find their efforts restricted as they can't move easily from one platform to another.

Need help implementing IAM? We're here for you



We can't overstate the importance of IAM, which is why it may pay to seek expert help in implementing your new policies.

At dig8ital, we're experts in the field of cyber security and know what it takes to listen to organizations, understand their unique needs, and design tailored solutions that meet their requirements.

To learn more about what we can do for you specifically, contact us today for a free maturity consultation.

W: dig8ital.com
E: contact@dig8ital.com

dig8ital