Your guide to: Identity and Access Management (IAM)

An information security eBook by TSC

Raise awareness

Develop knowledge

Change behaviour

Develop security culture

Welcome to TSC's guide to Identity and Access Management (IAM) cyber security.

IAM, or simply identity management, refers to a service or platform that identifies individuals and controls their access to system resources through user rights and restrictions. Identity management and authorisation is important for security and increases the productivity of employees as they don't need to keep track of several different credentials and passwords. However, with speed and efficiency comes increased cyber risk.

Your partner in cyber security and culture change

As you embark on your journey as a cyber security leader, working with a trusted cyber security awareness training and culture change provider like The Security Company can significantly enhance your efforts. The Security Company offers a wide range of services and products tailored to help you educate the uninitiated, engage budget-deciding stakeholders, and empower your workforce to become a proactive line of defence against cyber threats.

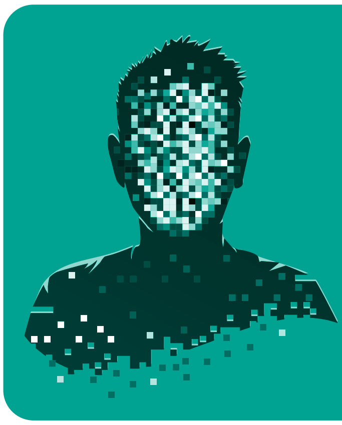
In this comprehensive eBook, we'll review what Identity and Access Management is, why access management is an essential part of every modern organisation's security and touch on IAM best practices.

Below is a table of contents:

Contents

Introduction

Ensuring the security of sensitive information is paramount to your organisation's reputation and financial wellbeing. Identity and Access Management (IAM) is a fundamental concept in the realm of cyber security, addressing the challenges associated with granting and managing access to resources in a controlled and secure manner. IAM serves as a crucial framework that enables organisations to strike a balance between granting legitimate access to authorised users while thwarting unauthorised access attempts. We will explore IAM's core principles, historical evolution, and the associated benefits and risks.

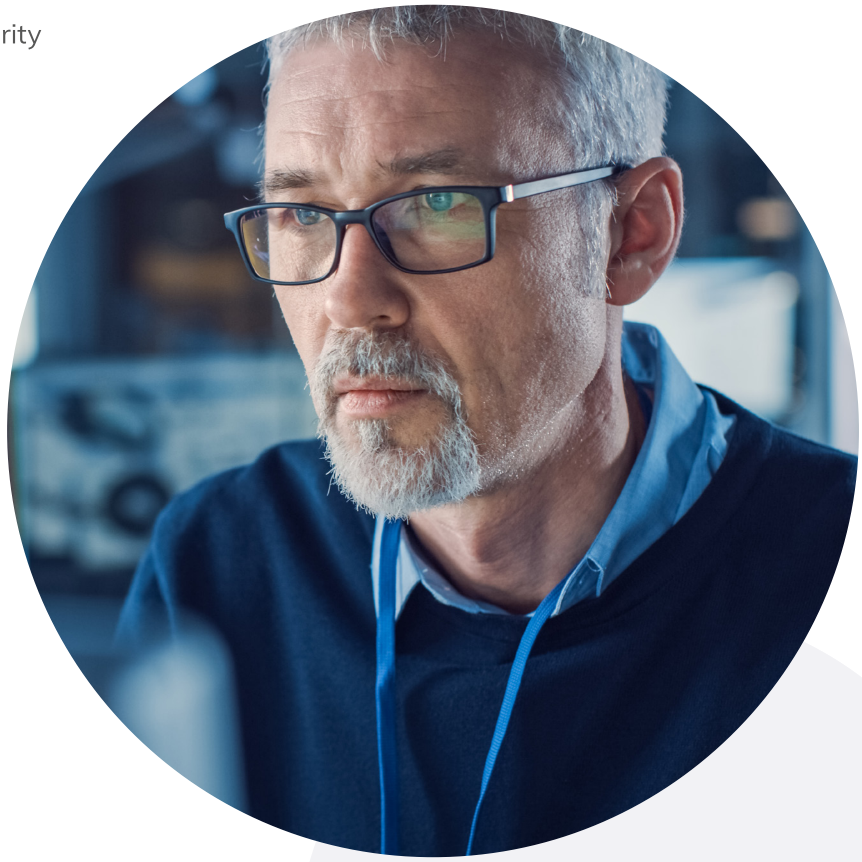


60% of medium-sized companies were affected by a hack, impacting 250-5000 employees, who requested to work remotely. 56% of these companies had reported theft of their credentials and 48% had incidents of social engineering such as phishing[1].

1a. What is IAM security?

Identity and Access Management (IAM) Security is a comprehensive approach to managing digital identities and controlling access to various resources within an organisation's IT infrastructure.

At its core, IAM encompasses strategies, policies, technologies, and processes that collectively ensure the right individuals are granted the appropriate level of access to data, systems, applications, and other critical organisational assets. IAM security solutions enable organisations to authenticate the identity of users, authorise their access based on roles and permissions, and monitor and manage these privileges throughout the user lifecycle – making access alterations where appropriate.



Nearly 90% of financial organisations have been impacted by data breaches, with 60% of those incidents involving identity theft[2].

[1] Expert Insights, 2023.
[2] Identity and Access Management Forecast 2023-2032, Global Market Insights.

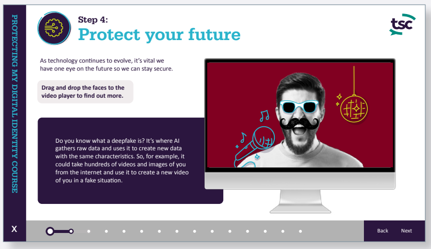
Awareness and training with The Security Company

The Security Company has over 20 years of experience delivering awareness training and materials to global organisations.

Our identity security and access/authentication products include:

- Password security eLearning course
- Credential stuffing password cracker game
- Protecting my identity animated infographic
- Protecting my identity top tips
- Authentication hacks animated infographic
- None shall pass(word) – authentication hacks game
- ... and much more on working remotely, reporting incidents, safe use of the web, GDPR, classifications, cloud security and emerging threats.

With our expertise and comprehensive range of services, The Security Company can support you throughout your journey.


PROTECTING MY DIGITAL IDENTITY COURSE

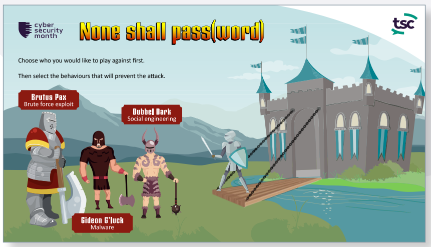
Step 4:
Protect your future

As technology continues to evolve, it's vital we have one eye on the future so we can stay secure.

Drag and drop the faces to the video player to find out more.

Do you know what a deepfake is? It's where AI gathers raw data and uses it to create new data with the same characteristics. So, for example, it could take hundreds of videos and images of you from the internet and use it to create a new video of you in a fake situation.

but loser for passwords


None shall pass(word)

Choose who you would like to play against first.

Then select the behaviours that will prevent the attack.

1b. The three pillars of IAM

IAM Security is built upon three foundational pillars that collectively form a robust framework for safeguarding digital assets:

- **Identification:** The first pillar involves accurately establishing the identity of individuals seeking access to resources. This typically involves username-password combinations.
- **Authentication:** Once an identity is established, authentication mechanisms validate the identity's legitimacy. This can include something the user knows (password), something they have (ID badge), or something they are (biometric data).
- **Authorisation:** After confirming an individual's identity, the next step is to determine what resources they are permitted to access and what actions they can perform. Authorisation is typically based on the individual's role, responsibilities, and the principle of least privilege.

4th pillar Auditing? The most commonly overlooked pillar in almost every identity solution is the auditing component. The most likely reason for this is the complexity and enormity of the problem and **one of the key reasons why organisations implement identity management solutions**[3].

[3] Microsoft, 2023.

1c. The history of IAM

Access management is inherent to human nature with security and restricted access observed in ancient civilisations such as the Egyptians, Greeks and Chinese dynasties via passphrases used to access restricted areas. The evolution of digital IAM can be traced back to the early days of computing when simple access controls were implemented. However, with the rise of networked systems and the internet, the need for a more structured and scalable approach to identity and access management became evident. Protocols like the Kerberos authentication protocol, created in the 1980s at MIT to provide a consistent approach to authentication and access control for several systems through an insecure channel, i.e., digital network, were developed. Over the years, IAM solutions evolved from rudimentary access controls to sophisticated platforms that integrate advanced authentication methods and single sign-on (SSO) capabilities.

1d. The benefits and risks of IAM

Benefits:

1. **Enhanced security:** IAM security minimises the risk of unauthorised access by ensuring only authenticated and authorised users can access resources, reducing the risk of phishing attacks, identity theft and unlawful access to sensitive information.

2. **Improved compliance:** IAM assists organisations in adhering to regulatory requirements (HIPAA, GDPR, etc.) by providing audit trails and access controls. IAM can also be reconfigured as data regulatory conditions are no stranger to updates and changes.

3. **Efficiency and productivity:** IAM streamlines user management processes, reducing administrative overheads and enabling employees to access the resources they need quickly. It also improves ease-of-access as IAM protocols can include things like remote access and multiple-device management.

4. **Centralised management:** IAM provides a centralised platform to manage user identities, reducing the complexity of access management and easing the burden on security administrators. It also makes it easier to withdraw improper access privileges, identify access violations and revoke credentials when necessary.

Risks:

1. **Single point of failure:** Overreliance on IAM systems can create a single point of failure, making them attractive targets for attackers.

2. **Cloud vulnerabilities:** IAM security brings with it the same risks one would expect from any cloud environment. This means industrial espionage, negligent third-party vendors and malicious privileged users pose a large threat.

3. **Account credibility:** As more and more IAM processes moved to the cloud, account credibility has become a massive issue. Here, an organisation may mistakenly give access to a user with no credentials and fail to spot they have done so.

4. **Complexity:** Implementing and managing IAM systems can be complex and resource intensive and may not necessarily be the solution for your business.

5. **User resistance:** Complex IAM processes can lead to user frustration and resistance, potentially impacting productivity and security. Resistance can be greater for organisations that have not focused on their security culture at all.

6. **Data breaches:** If IAM is improperly configured or managed, it can lead to data breaches and unauthorised access to sensitive information. One of the common risks in IAM security is granting too many permissions to too many users, thus enabling security vulnerability via a tool meant to dissolve it.

IAM risk is a serious security problem for any business. Companies should adopt a risk-based approach to IAM, including risk-based policies, procedures, and controls, to reduce the risk of unauthorised access to IAM data, maintain regulatory compliance, and protect against data loss.

Key identity management challenges

Navigating the intricacies of identity management can be a daunting task. Organisations often struggle with determining who should have access to which resources and at what level.

Additionally, striking the right balance between security measures and user convenience is a delicate endeavour.

- **Managing complex user identities:** Modern organisations operate in dynamic environments where users have multiple roles and access needs. Managing these complex user identities, including contractors, partners, customers, and employees, becomes intricate. Ensuring proper provisioning and de-provisioning of user accounts, especially in larger enterprises, is a significant challenge.
- **Secure access across devices and locations:** The modern working landscape includes mobile and remote work and employees expect seamless access to resources from various devices and locations. This presents a challenge in ensuring secure access without compromising data integrity. Providing this level of access while safeguarding against unauthorised entry requires robust authentication and authorisation mechanisms.
- **Balancing employee convenience with cyber security:** Striking the right balance between user convenience and stringent cyber security measures is an ongoing challenge that will shapeshift and change with new employees and fresh access requests. Complex and cumbersome authentication processes can lead to user frustration and potentially circumvented security protocols. Conversely, overly lenient authentication can expose organisations to security breaches.

2a. Dealing with privileged access management

Managing privileged users, who have elevated access to critical systems and data, is a significant challenge. Effective privileged access management (PAM) is essential to prevent misuse of these powerful privileges. Additionally, organisations must adopt advanced identity authentication methods, such as multi-factor authentication (MFA), to thwart identity-based attacks like phishing and credential theft.

As organisations continue to adopt cloud computing, IoT (Internet of Things) devices, and other emerging technologies, these challenges become even more complex. Addressing these identity management challenges requires a holistic approach that incorporates cutting-edge technology, well-defined policies, user education, and ongoing monitoring and adaptation. By understanding and mitigating these challenges, organisations can enhance their IAM security posture and better protect their digital assets from evolving cyber threats.

Regulations, compliance and consequences

Identity and Access Management (IAM) plays a critical role in helping organisations achieve and maintain compliance with various regulatory frameworks. IAM serves as a foundational component to ensure that sensitive information is accessed and managed in accordance with legal and industry-specific requirements.

This section explores the intricate relationship between IAM and compliance, highlighting the regulatory landscape and real-world case studies that emphasise the consequences of non-compliance.

Around 40-50%, of organisations are forecasted to have adopted Cloud Identity and Access Management (CIAM) in 12 – 24 months[4].

3a. Regulatory landscape

The regulatory landscape surrounding data protection and privacy is continuously evolving. Organisations worldwide must adhere to a variety of regulations, such as the General Data Protection Regulation (GDPR) in the European Union, UK GDPR, the Health Insurance Portability and Accountability Act (HIPAA) in the United States, and the Personal Data Protection Act (PDPA) in Singapore, among others.

These regulations impose stringent requirements on how organisations collect, store, process, and share personal and sensitive data. For example, the HIPAA Privacy Rule requires organisations to block employee access to PHI (Protected Health Information) as soon as the employee leaves the organisation or is terminated. Similarly, the GDPR and California Consumer Privacy Act (CCPA) laws require businesses to maintain access management and strong authentication methods to protect data related to their customers.

By 2026, 70% of identity-first security strategies will fail unless organisations adopt context-based access policies that are continuous and consistent[5].

[4] https://www.bloomberg.com/press-releases/2022-08-10/okta-study-finds-high-ciam-adoption-in-apac-but-low-maturity
[5] Identity-First Security Maximizes Cybersecurity Effectiveness, Gartner, Dec 2022.

The importance of securing the cloud

75%

There has been a dramatic increase in the level of sensitive data stored in the cloud. Three quarters (75%) of businesses said that more than 40% of data stored in the cloud is classified as sensitive, compared to 49% of businesses this time last year[6].

4a. IAM in the cloud environment

Cloud computing transforms the traditional IT landscape by enabling organisations to leverage remote resources, scale dynamically, and improve operational efficiency. However, the distributed nature of the cloud and the diversity of services introduce complexities in managing identities and access. Cloud IAM focuses on ensuring that the right users have appropriate access to cloud resources, regardless of their location or device. IAM solutions in the cloud encompass user authentication, authorisation, and user lifecycle management, helping organisations maintain control over their cloud infrastructure.

74% of data breaches begin with the misusing of privileged credentials[7].

[6] Thales, Cloud assets the biggest target for cyberattacks, July 2023.
[7] Privileged Access Management Centrify Survey, Forbes, 2023.

4b. Cloud IAM best practices

Implementing effective cloud IAM requires adherence to a set of best practices to mitigate risks and ensure a secure environment:

- **Single Sign-On (SSO):** Implement SSO to enable users to access multiple cloud services with a single set of credentials, enhancing user experience while maintaining security.
- **Multi-factor authentication (MFA):** Enforce MFA for enhanced authentication, requiring users to provide multiple forms of verification before gaining access.
- **Role-based access control (RBAC):** Assign permissions based on roles, ensuring users only have access to resources necessary for their responsibilities.
- **Regular auditing and monitoring:** Continuously monitor user activities and access patterns, promptly detecting and addressing suspicious behaviour.
- **Automated provisioning and deprovisioning:** Automate the process of granting and revoking access to cloud resources as users join or leave the organisation.
- **HR security awareness:** Add IAM as a step to inductions and exit protocols.
- **Separation of duties (SoD):** To prevent fraud or damaging errors, you could deploy SoD protocols, which involves sharing a set of responsibilities and privileges among multiple users to prevent one user being the be all and end all.
- **Centralised management:** With centralised management of cloud systems, your organisation's security team gains the visibility needed for proper oversight.
- **Principle of least privilege:** One option for ensuring security with cloud IAM is to practice the principle of least privilege; this ensures that users receive the minimum permissions required to fulfil their roles and can significantly reduce the blast radius in the event of a network breach.

4c. Securing cloud identities and data

Securing cloud identities and data involves a multi-faceted approach:

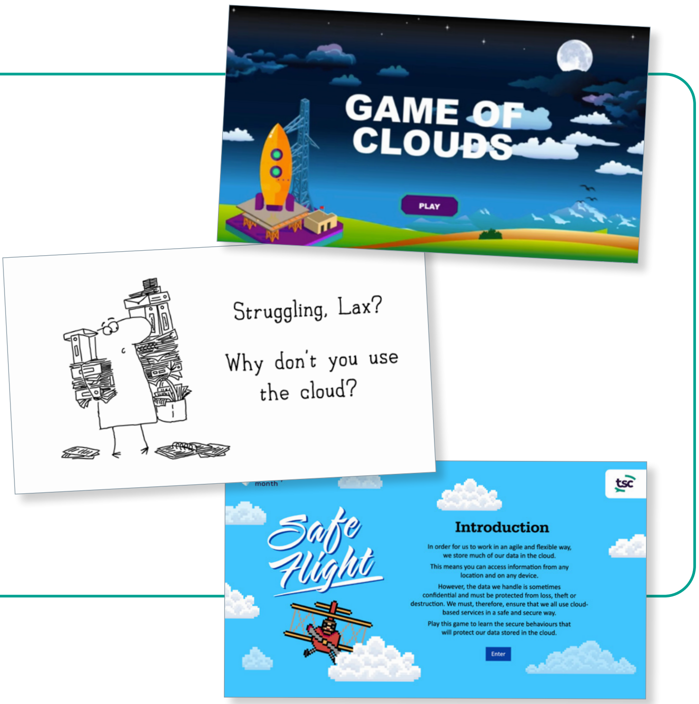
- **Data encryption:** Employ encryption mechanisms to protect data at rest and in transit, preventing unauthorised access to sensitive information.
- **Secure APIs:** Ensure that Application programming interfaces (APIs) used to interact with cloud services are secure and properly authenticated to prevent potential vulnerabilities.
- **Data loss prevention (DLP):** Implement DLP measures to monitor and prevent the unauthorised sharing of sensitive data in the cloud. This will include training and awareness in data protection behaviours and regulations.
- **Identity governance and administration (IGA):** Establish robust IGA processes to manage user identities, access requests, and entitlements effectively.
- **Regular security assessments:** Conduct regular security assessments and penetration testing to identify and rectify vulnerabilities in cloud environments and your security culture as a whole.

Securing cloud identities and data not only safeguards sensitive information but also upholds the organisation's reputation and customer trust in an increasingly interconnected digital landscape.

Cloud security awareness and training with The Security Company

Our cloud security materials are available in non-customised, customised and bespoke versions and can be requested in multiple languages for your global workforce.

- 'Game of Clouds' interactive game
- 'The Cloud with Lax' character-based animation
- 'Safe flight/Using the cloud' interactive game
- ... and much, much more!



Introduction

In order for us to work in an agile and flexible way, we store much of our data in the cloud.

This means you can access information from any location and on any device.

However, the data we handle is sometimes confidential and must be protected from loss, theft or destruction. We must, therefore, ensure that we all use cloud-based services in a safe and secure way.

Play this game to learn the secure behaviours that will protect our data stored in the cloud.

Best practices for IAM professionals

Effective Identity and Access Management (IAM) implementation requires a strategic and well-executed approach. IAM professionals play a crucial role in designing, deploying, and maintaining robust IAM systems that enhance security, streamline user access, and uphold regulatory compliance. This section outlines essential best practices for IAM professionals to ensure successful IAM implementation and operation.

TSC your partner in board engagement

We are passionate about developing a strong security culture in every organisation we work with. Behaviour change projects have a greater chance of success if you receive board engagement. This is why our board engagement strategies are key in getting approval for surveys of your organisation's security maturity. We contextualise cyber risks with language that board-level executives can understand in order to get backing and support. The goal is to provide all of our clients with a long-term strategy to sustain and grow their security culture.

5a. Top tips for successful IAM implementation

- **Start with a strategy:** Develop a comprehensive IAM strategy aligned with organisational goals, security requirements, and regulatory compliance. Ensure buy-in from stakeholders across the organisation.

- **Understand user needs:** Gain a deep understanding of user roles, responsibilities, and access requirements to design an IAM system that meets diverse user needs without damaging productivity.

- **Embrace standardisation:** Adopt industry best practices and standards for IAM implementation to ensure consistency, interoperability and a consistent baseline in identity and access management across systems, departments and levels.

- **Leverage technology:** Choose IAM solutions that align with your organisation's needs and budget, considering factors like scalability, integration capabilities, and vendor reputation.

- **Implement strong authentication:** Enforce strong authentication mechanisms, such as multi-factor authentication (MFA), to enhance user identity verification on access requests.

- **Balance security with user experience:** You must balance security measures with user convenience to ease friction, encourage adoption and minimise user resistance.

- **Role-based access control (RBAC):** Implement RBAC to assign permissions based on job roles, ensuring the principle of least privilege and minimising access creep.

- **Automate provisioning and deprovisioning:** Streamline user lifecycle management through automated provisioning and deprovisioning processes, minimising human error and negligent security in order to enhance security.

- **Continuous monitoring and auditing:** Implement robust monitoring and auditing mechanisms to detect and respond to security incidents promptly. Continuously audit your IAM protocols and authorised access list for creepers and unsanctioned users.

- **Regular training and education:** Provide ongoing training to users, administrators, and IAM professionals to keep them informed about security best practices and system changes. Best practices and IAM threats do not stand still, and neither can your stance on training and education ... or you will be sending your employees out to the battlefield armed with a cardboard shield and a sword made of playing cards.

61% of all breaches involve credentials, whether they be stolen via social engineering or hacked using brute force[8].

[8] Verizon 2023 Data Breach Incident Report.

Let’s start communicating...

6a. The role of security awareness training in IAM

In the realm of IAM, technical measures and solutions alone are insufficient to maintain a robust security posture. Human behaviour and awareness play a critical role in safeguarding sensitive data and preventing unauthorised access.

Security awareness training serves as a foundational component of IAM, educating employees and users about the importance of security, their role in maintaining it and best practices for secure access.

44% of security professionals believe that an IAM solution will address their current security gaps[9].

- **Cultivating a security mindset:** Security awareness training fosters a culture of vigilance and responsibility, ensuring that individuals at all levels understand the potential risks and consequences of security breaches. A security culture also means that employees are looking out for each other rather than remaining individually focused.

- **Mitigating insider threats:** Employees who are well-informed about security risks are more likely to recognise and report suspicious activities, mitigating the potential for insider threats. Investing in the training and development of your employers also fosters a sense of belonging and could lead to less malicious internal activity.

- **Combatting social engineering:** Security awareness helps users identify and thwart social engineering attacks, such as phishing, where attackers manipulate individuals into divulging sensitive information.

- **Strengthening compliance:** Awareness training uses case studies and relevant information to ensure that employees comprehend the importance of regulatory requirements and the proper handling of sensitive data, thus reducing the risk of unintentional non-compliance.

[9] The state of the security team: are executives the problem?, LogRhythm, 2023.

Bonjour! Hola! Salut! Ni Hao!

Multiple languages available.
All of our products are customisable and available, upon request, in over 15 languages to maximise employee engagement and knowledge retention.

6b. Identity management training: educate your workforce

- **Understanding IAM concepts:** Train employees on the basics of IAM, including authentication, authorisation, and role-based access control, helping them appreciate the importance of controlled access.

- **Account security:** Educate users about the significance of strong passwords, password management tools, multi-factor authentication and the risks of password sharing.

- **Phishing awareness:** Teach employees how to recognise phishing emails, suspicious links, and malicious attachments, reducing the likelihood of credential theft.

Security awareness training is a continuous process that requires ongoing reinforcement and adaptation to address emerging threats. By investing in educating the workforce about identity management and access authorisation principles, organisations empower their employees to become active participants in maintaining a secure digital environment, contributing significantly to the success of their IAM strategies.

7. Final thoughts

7a. The evolving landscape of IAM: looking ahead

The field of IAM is dynamic and always evolving, influenced by technological advancements, regulatory changes, and emerging cyber threats. Looking ahead, we anticipate several trends in the IAM landscape:

- **Zero Trust architecture:** Organisations will increasingly adopt a Zero Trust approach, where access is never assumed to be inherently secure, and strict controls are applied to every access attempt. Whilst this significantly lessens productivity, some organisations may be willing to take that hit in efficiency if they see significant savings in fines and errors.

- **Biometric authentication:** Biometric methods, such as facial recognition and fingerprint scanning, are already gaining prominence as reliable and user-friendly authentication options but there remains some hesitancy. Will the need for tighter access controls finally lead to wholesale adoption of biometric authentication?

- **AI and machine learning:** AI and machine learning will play a significant role in IAM, enabling real-time threat detection, user behaviour analysis, and risk assessment.

- **Decentralised identity:** Decentralised identity solutions, such as blockchain credentials of NFT ID badges, may offer users greater control over their own identity and data and a more secure way to store login credentials.

IAM is a multifaceted discipline that demands a comprehensive strategy, careful implementation, and continuous vigilance. By embracing security awareness training, adhering to best practices, and staying attuned to the evolving landscape of IAM, organisations can effectively protect their digital assets, ensure compliance, and adapt to the ever-changing cyber security challenges of the modern world.

Join TSC for a tried and tested security culture journey

We use cyber awareness campaigns, engaging online training, employee development programs and behaviour change strategies to build a strong security culture.

After sitting down and assessing your organisation's security levels, we pinpoint where you are in our 4-step journey and get to work.

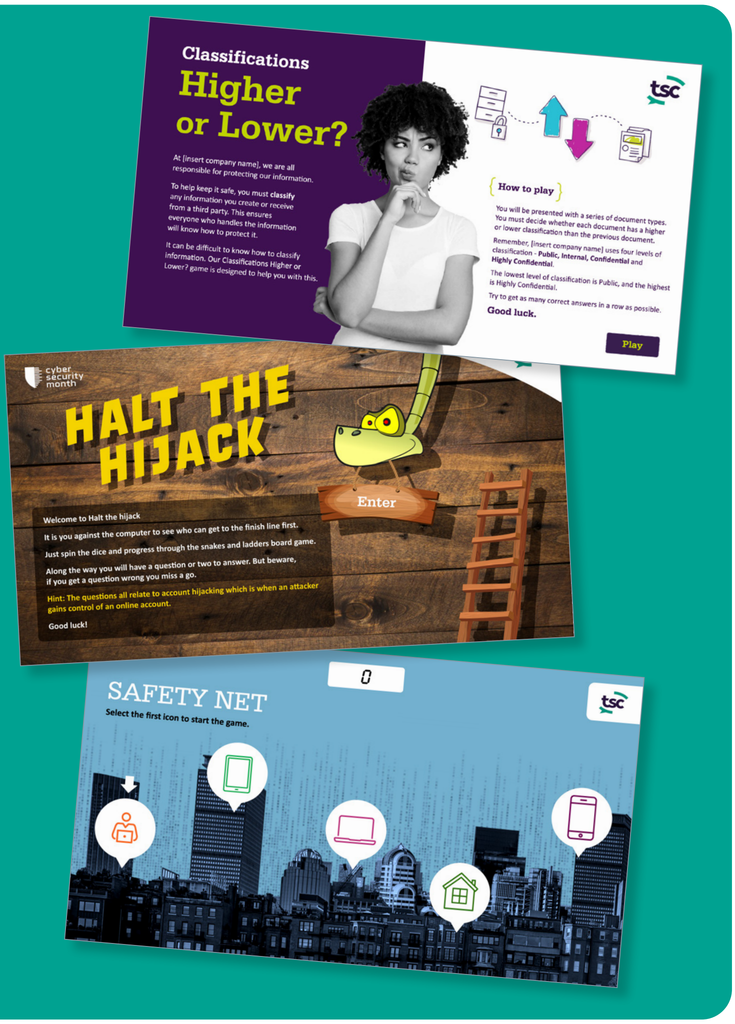
Our 4-step journey

1. Raise awareness: physical and digital materials on risks and threats to increase understanding.
2. Develop Knowledge: Recharge and build new knowledge with games, training, and collaborative opportunities.
3. Change behaviour: Enable effective security behaviours across your workforce.
4. Develop a secure culture: Ongoing promise to support and innovate against emerging threats at the highest levels.

TSC's collection of games will change how your employees learn

All of our products are customisable and available, upon request, in over 15 languages to maximise employee engagement and knowledge retention.

- Password Cracker
- Game of Cloud Security
- Workstation Security
- Classifications: High or Low
- Scam Survival
- Don't take the (phishing) bait
- Spot the risks in the office, on the move and at home
- ID badge identifier
- Strongest password
- Password challenge
- Ransomware Resistance
- Festive scams (Whack-an-elf)
- Cybermaze of threats
- Account hijacking (Snakes and Ladders)
- Authentication hacks
- Safety Net (data loss prevention)



Classifications
Higher or Lower?

At [insert company name], we are all responsible for protecting our information.

To help keep it safe, you must **classify** any information you create or receive from a third party. This ensures everyone who handles the information will know how to protect it.

It can be difficult to know how to classify information. Our Classifications Higher or Lower? game is designed to help you with this.

{ How to play }

You will be presented with a series of document types. You must decide whether each document has a higher or lower classification than the previous document.

Remember, [insert company name] uses four levels of classification - **Public, Internal, Confidential** and **Highly Confidential**.

The lowest level of classification is Public, and the highest is Highly Confidential.

Try to get as many correct answers in a row as possible.

Good luck.

Play

cyber security month

HALT THE HIJACK

Enter

Welcome to Halt the hijack

It is you against the computer to see who can get to the finish line first.

Just spin the dice and progress through the snakes and ladders board game.

Along the way you will have a question or two to answer. But beware, if you get a question wrong you miss a go.

Hint: The questions all relate to account hijacking which is when an attacker gains control of an online account.

Good luck!

SAFETY NET

0

Select the first icon to start the game.

What our clients say:

"We are so impressed by the offering and services TSC has provided we are working with them on more specific role-based eLearning to further develop our specialist employees' understanding of information security" Chris Mortlock, Specsavers

"The Security Company's ability to deliver engaging content time and time again has been invaluable in delivering this cyber security control for Reach plc, so much so that we are now in our 3 year of working with TSC. When looking for cyber security training and awareness material for your organisation, TSC is a must." *Jat Chana, REACH*

"TSC excels at understanding the client's specific requirements and working with the information provided. TSC provided an outstanding level of quality, customer understanding, design implementation, and project management. hey would be my first recommendation to anyone looking for professional security awareness." *David Cowper, TT Electronics*

The Security Company: Your trusted Partner for long-term success

Partnering with The Security Company provides you with a trusted ally in achieving long-term success in your security culture initiatives. With our expertise and comprehensive range of services,

The Security Company can support you throughout your journey.

Here's why we are the ideal partner:

Extensive experience:

With years of experience in the cyber security industry, The Security Company has a deep understanding of the challenges organisations face in building a security-aware culture. We bring a wealth of knowledge and practical insights to guide you through the process.

Tailored solutions:

The Security Company offers customisable solutions that cater to the unique needs and goals of your organisation. Whether you require engaging training materials, effective communication strategies, or change management support, we can tailor our offerings to meet your specific requirements.

Proven track record:

The Security Company has a proven track record of success, having assisted numerous global organisations, from a variety of industries, in transforming their security culture. We have received accolades and recognition for our innovative approach and ability to drive positive behavioural change.

Comprehensive services:

From security awareness training and communication campaigns to board engagement and behavioural analysis, The Security Company offers a wide range of services to support every aspect of your security culture initiatives.

Partnering with The Security Company ensures that you have a dedicated partner committed to your organisation's long-term success in building a security-conscious culture.

www.thesecuritycompany.com @TSCPeopleSec @thesecurityco @thesecurityco