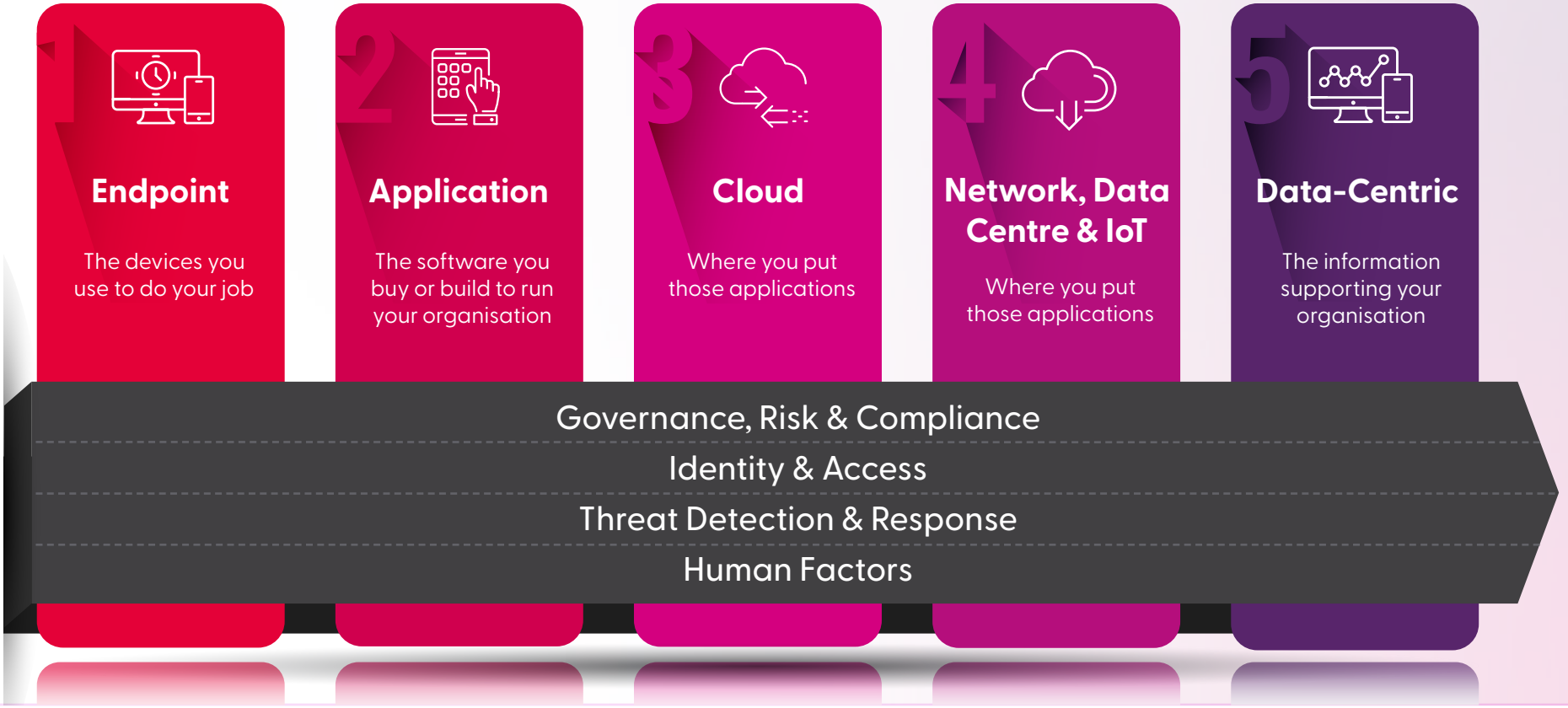
Insight's Human Factors in Security Guide

Insight

Introduction

At Insight, we recognise the importance of a holistic approach to security. Attackers will look for your weakest area, not your strongest. We have technical expertise in the five technology domain areas (Endpoints, Applications, Cloud, Network, Datacentre and IOT, and Data centric) – but as a leading solution integrator, we believe you should also pay close attention to the interactions between these technology domains (Governance, Risk and Compliance, Identity and Access, Threat Detection and Response, and Human Factors). The gaps where the technology domains connect are often where additional value can be achieved, helping improve your overall security posture in a cost-effective manner.

Insight's holistic security model



What are human factors and why are they important?

Even though security infrastructure and tools and controls are continuously improved and invested in, breaches are still happening, and they are not easy to identify and resolve. There are many specialized security controls for different kinds of threats, from attacks on endpoints to attacks on supply chains – but when you examine how these attacks actually happened, the main three reasons are:

- **Passwords –** an insecure password was cracked, a default password was left unchanged, or the same password was used on multiple sites.
- **Phishing –** a user was misled into either giving away their credentials, visiting a compromised website or opening a hostile attachment.
- **Patching –** a known vulnerability was left unpatched for too long and was exploited by malware, or some risky software was installed by a user which was compromised.

IT teams can use technology to help lower the chance of breaches, but end users will always have a role in supporting the security of an organisation. IT teams often concentrate on the technology, and sometimes the process, then forget the people side, when people can determine the failure or success of a project.

Process: the written policies explaining what users should or shouldn't do takes many forms, such as information security policies, contracts of employment, staff handbooks, acceptable use policies, or incident response plans.

Technology: the tools, systems, and controls which provide guiderails and restrictions to what users can do, need to be tight enough to restrict the obvious risky activities, but permissive enough to allow some flexibility and not break business processes

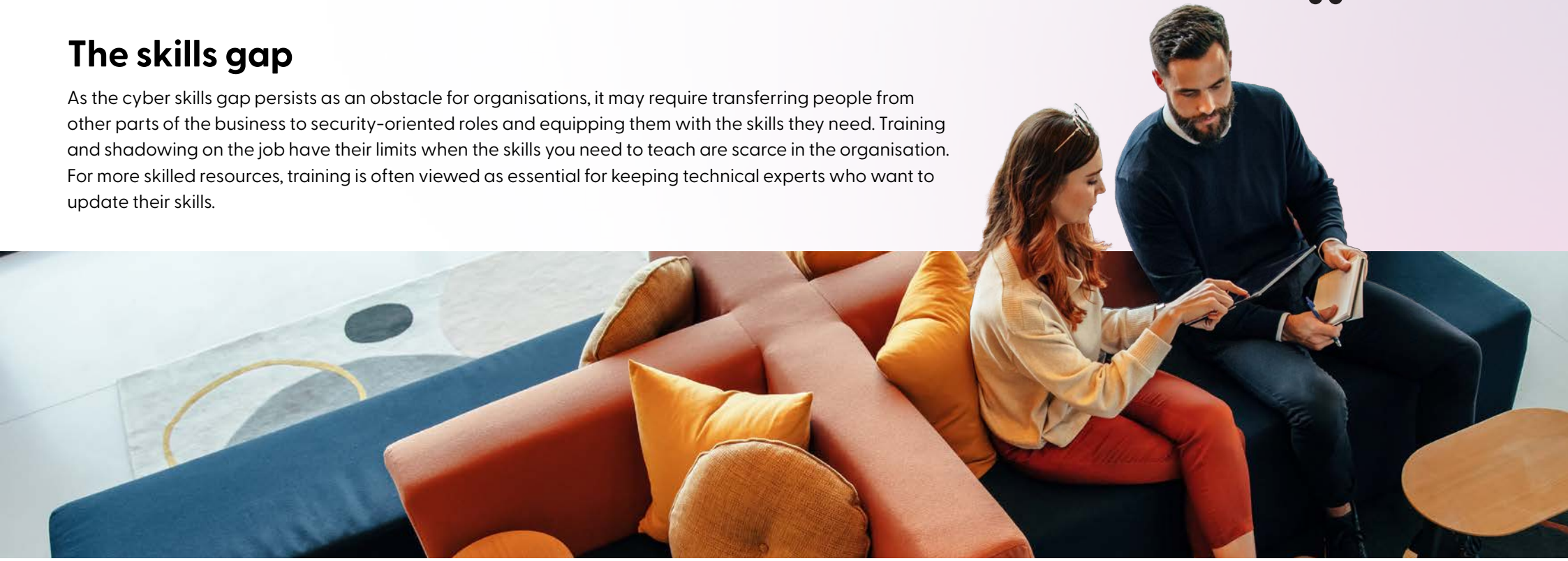
People: when there are no documented process or people do not know it, they have to use their own judgement. Or when a t echnology fails to prevent a new threat, people are often the first and last line of defence, relying only on their current skills and training.

By 2027, 50% of large enterprise chief information security officers (CISOs) will have adopted human-centric security design practices to minimise cybersecurity-induced friction and maximise control adoption.

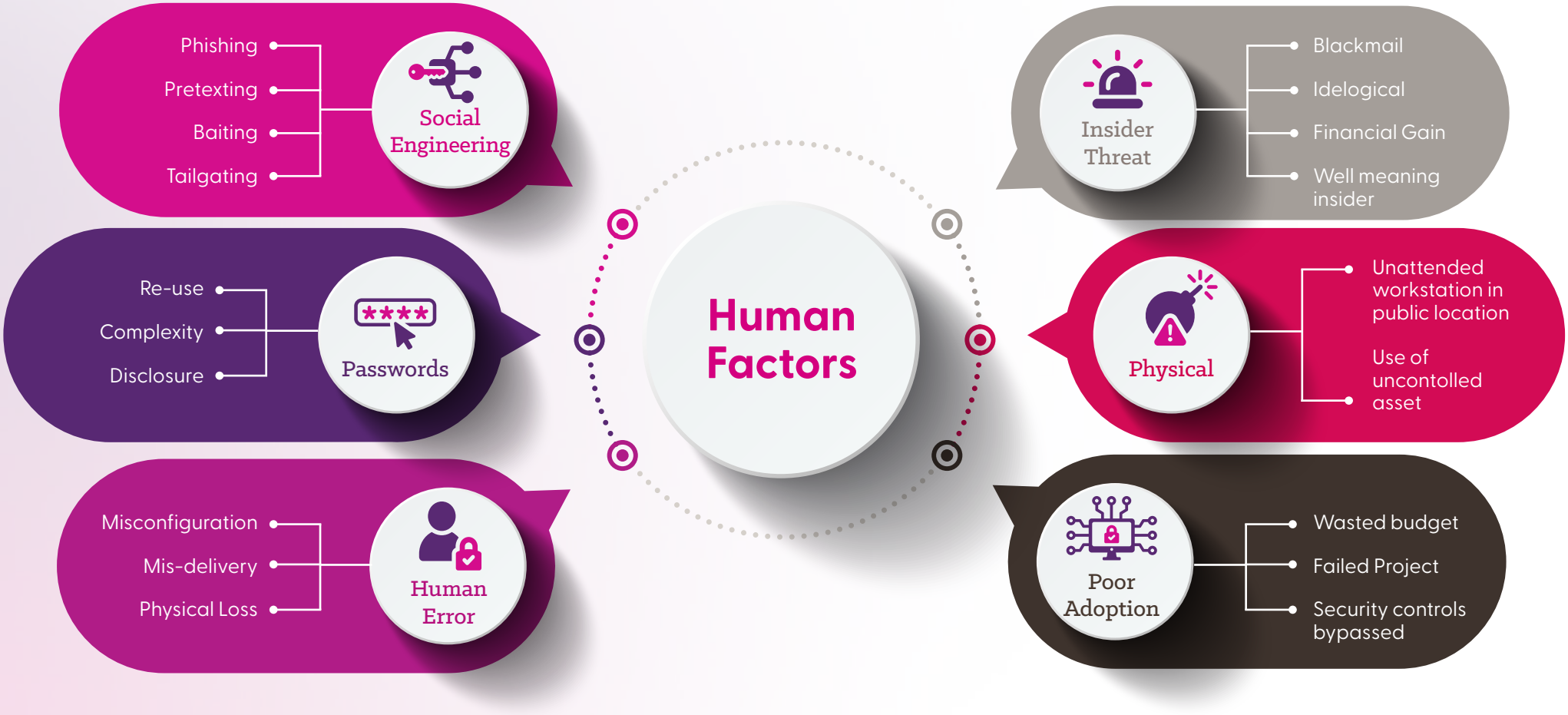
- Gartner Identifies the Top Cybersecurity trends for 2023.

The skills gap

As the cyber skills gap persists as an obstacle for organisations, it may require transferring people from other parts of the business to security-oriented roles and equipping them with the skills they need. Training and shadowing on the job have their limits when the skills you need to teach are scarce in the organisation. For more skilled resources, training is often viewed as essential for keeping technical experts who want to update their skills.



Human factors can impact on almost every aspect of your security strategy



The importance of personas

You should tailor your human factors in security strategy to the different kinds of users, or personas, in your organisation. A generic approach will not be very effective – people need to be empowered in relation to their current role, and to understand how they can personally help with organisational security.

An example of how you could categorise user types in a typical organisation is shown here, but each organisation is different.

End-user

- Varying levels of IT skills, some may have only very basic knowledge
- Multi-language likely to be a requirement in global organisations
- Topics may be related to phishing, GDPR, physical security etc.

Developer

- Typically will be advanced technically, but may be unaware of secure coding techniques
- Likely to require very niche training, using the same programming language of the developer
- Gamification and hands-on learning likely to have a better impact then non-interactive

IT Administrator

- Technically advanced users want to be able to develop their existing skills even further and to be challenged
- Gamification and competition can help to drive adoption
- Like a pilot, hands on skills in a safe simulator environment used regularly can help with responding to real high-stress security situations

Business Leader

- Focus on team-based group learning activities to stress-test decision making processes and roles and responsibility definitions
- Business-centric
- Can involve many different roles to test team dynamics

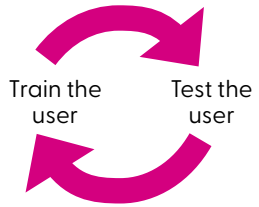
How Insight can help

Managed End-User Security Awareness

In the current digital environment, where most business operations are done online, it is vital that end-users are security conscious. Organisations need to make sure that their employees know about the possible dangers of cyber attacks and how they can reduce those dangers. This involves teaching employees how to follow good practices for password management, secure browsing habits, and how to spot and report dubious emails.

Phishing attacks are one of the biggest risks to an organisation's cybersecurity. These attacks try to fool people into giving away personal information like usernames, passwords, or financial information. Phishing simulations are a useful way to teach employees how to protect themselves from these attacks. By making fake phishing emails that look like real ones, employees can learn to spot and report dubious messages.

We work with KnowBe4, an expert in security awareness training for end-users, who provide a complete platform that has training modules, phishing simulations, and other tools that teach employees about the latest threats and how to avoid them. The platform uses engaging methods, such as videos, quizzes, and interactive games, to involve employees and make the training experience more fun.



Their methodology is based on a cycle of training and testing – not once a year, but regularly in small chunks so that training is reinforced, and improvements can be measured. Training can then be targeted in the right amounts, on the right people.

We offer a complete end-to-end solution that leverages the KnowBe4 platform to deliver effective security awareness training to our clients. Our managed service includes ongoing monitoring and reporting, enabling us to identify areas where additional training may be needed and provide timely feedback to our clients. Organisations can then focus on their core business activities while we take care of their security awareness training needs, helping to keep them safe from cyber threats.

Cyber workforce resilience platform

A SaaS based platform designed to continuously exercise, benchmark, upskill, and prove an organisation's cyber workforce resilience.

For individuals:

An engaging, gamified learning environment that covers the full spectrum of hands-on technical training for the enterprise.

- Offensive and defensive cyber professionals
- Developers and application security experts
- Cloud and infrastructure security professionals

For teams:

Responding to security threats requires a team effort from techs to execs. We engage teams from across your organisation to enhance their crisis decision-making and technical response skills to adaptably and effectively respond to cyber risk.

- Executive teams
- Crisis management teams
- Technical cyber teams

For the organisation:

Skills development exercises that drive transformative behavioural change across the organisation.

- Senior leaders
- Front-line employees
- High-risk targets of cyber attacks

All of these elements are accessible from anywhere with a simple web browser, so can even be used by people outside of the organisations, for example as part of a recruitment assessment pre-hire.

As a business you will be able to:

- Continuously prove cyber capability
- Improve the speed and quality of response.
- Improve recruitment and career development.
- Reduce cloud and application vulnerabilities.
- Reduce cybersecurity costs.

Adoption and Change Management

Adoption and change management play a crucial role in supporting the human factors in cybersecurity by ensuring that security measures, policies, and technologies are effectively embraced and integrated into an organisation's culture and practices. Human factors, such as user behaviour, awareness, and habits, are often the weakest links in cybersecurity, as they can be exploited by malicious actors.

Here's how Insights adoption and change management can benefit in addressing these human factors:

User Awareness and Education: Adoption and change management involves educating users about cybersecurity threats, best practices, and the importance of security. By providing training and clear communication, users become more aware of potential risks and are empowered to make informed decisions that enhance security.

Behavioural Change: Change management aims to modify user behaviour in-line with desired security practices. By establishing new routines and habits, users can be encouraged to adopt secure behaviours, such as regularly updating passwords, being cautious about phishing emails, and reporting suspicious activities.

Cultural Shift: Successful adoption and change management initiatives foster a culture of security within the organisation. When cybersecurity becomes ingrained in the organisational culture, employees are more likely to prioritize security in their daily activities, leading to a more secure overall environment. Resistance Reduction: People often resist changes, especially when it disrupts their familiar routines. Effective change management strategies anticipate and address this resistance, helping to mitigate pushback against security measures and facilitating smoother adoption of new practices.

User-Centric Design: Adoption and change management processes involve understanding user needs and tailoring security solutions to match those needs. This user-centric approach increases the likelihood of acceptance and reduces friction in adopting security measures.

Continuous Improvement: Adoption and change management are ongoing processes that involve gathering feedback and adjusting strategies based on real-world experiences. This enables organisations to refine security practices in response to evolving threats and user needs.

Communication Channels: Effective communication is key to fostering trust and transparency in cybersecurity initiatives. Adoption and change management provide avenues for open dialogue between security teams and users, ensuring that concerns are addressed, and misunderstandings are clarified.

Mitigating Insider Threats: By fostering a sense of belonging and loyalty among employees, adoption and change management can help reduce the likelihood of insider threats, where employees intentionally or unintentionally compromise security.

Encouraging Accountability: Change management processes emphasize individual and collective responsibility for security. When users feel accountable for their actions, they are more likely to adhere to security protocols and report potential incidents promptly.

Adapting to New Technologies: Cybersecurity landscape is rapidly evolving, with new technologies emerging frequently. Adoption and change management help users adapt to these changes by providing training and support, ensuring that new technologies are used securely from the outset.

Conclusion

People are the biggest security risk to an organisation and need to be trained regularly and effectively in order to become effective as guardians of your organisation's security. A well-trained individual can be the last line of defence against a breach which has slipped through your technical and process based controls.

Traditional annual security awareness training is something that no-one looks forward to – and if an organisation puts as little effort into security as putting together a dry video and a handful of quiz questions, its not surprising if employees take the same approach to security. Consider some of the following best practices when defining your human factors in security strategy.

User Awareness and Education:

- Use gamification and competition to increase desire from individuals to participate.
- Training interventions should be regular and short – think 10 minutes weekly rather than an hour annually for generalist security awareness training.
- Use testing to ensure at an organisational level that your maturity objectives are being met, and to provide instant feedback to participants that they are learning the material.
- Consider both high targeted individual enablement focussing on technical skills alongside team-based exercises to test processes and team working skills.

Communication and Engagement:

- Speaking to people in their local language and in the right tone can be as important as the content.

Incident Management:

- A robust incident management process, which is stress tested can make the difference between a run-of-the-mill security event and a business-critical incident.

Inclusivity in Security Awareness:

- Your strategy should consider all personas, from the occasional IT user to the most technical security administrator in your organisation. They all have their part to play in maintaining security.

The human aspect of an organisation's security strategy is not just a formality; it's an essential factor that can make the difference between being secure and being exposed. As we have shown, from using modern training methods to ensuring diversity, it's vital to create a comprehensive approach that acknowledges the importance of the human element. By focusing on continuous learning, effective communication, strong incident management, and including all roles within an organisation, we build the basis for a resilient security posture. As technology changes and threats become more advanced, it is the well-trained, aware, and engaged individual who will reliably stand as a strong barrier against possible breaches. Adoption and change management makes sure that security actions, policies, and technologies are smoothly integrated into an organisation's culture and daily practices. It changes the perspective from simple awareness to practical behavioural change, creating a proactive security culture. This change leads to less opposition, supports continuous improvement, and strengthens responsibility among employees. As the cybersecurity landscape changes, keeping up with new technologies becomes crucial. Change management makes sure that organisations not only adjust but flourish amid these changes by using new tools securely and effectively.

Next Steps

By understanding your organisational risk, choosing the right technologies and platforms for the learning journey, and integrating them into your business processes, Insight can help you create and implement a consistent human factors in cybersecurity strategy. We can also track and improve the adoption as the rollout advances. Get in touch with our security consultants or adoption and change management experts for more information.

- **se.insight.com**
- **0852210010**