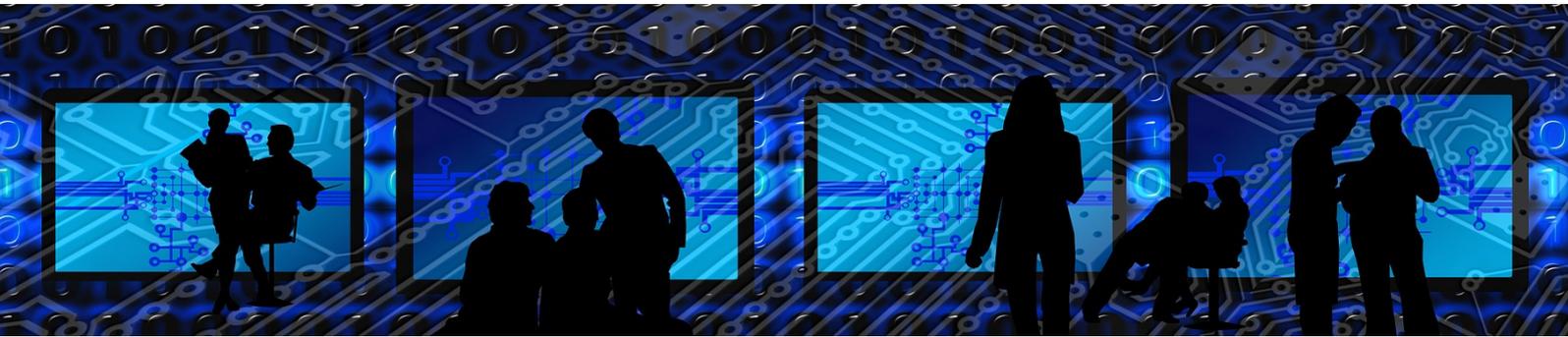




SECURITY AWARENESS TRAINING



As part of our **Advise** services the Security Awareness Training (SAT) ensures employees understand the key risks, threats and vulnerabilities and most importantly the impact that a breach can have on the business and their own lives. Delivered on client site, our training is designed to be vibrant and interactive, removing technical jargon and making the content relevant to the delegates.

Information and cyber security landscapes have changed significantly in recent times with cyber-attacks and data breaches becoming headline news in the media. As many as 46% of companies suffered from a cyber-attack or breach of their computer systems last year compared with just 24% the year before, according to figures from the Department for Culture, Media and Sport (DCMS) Cyber Security Breaches Survey 2017.

"The most common types of breaches are related to staff receiving fraudulent emails (in 72% of cases where firms identified a breach or attack). The next most common related to viruses, spyware and malware (33%), people impersonating the organisation in emails or online (27%) and ransomware (17%). This highlights how, as well as having good technical measures in place, the awareness and vigilance of all staff are important to a business's cyber security."

Technical controls are becoming more sophisticated but so too are the cyber-attacks taking place and the techniques being used. The biggest threat or the weakest link in any organisation remains the employees. However, whilst technologies have improved, the cyber-security knowledge and awareness of employees has not kept up with trends.

Our Approach

Our approach to security awareness training is to deliver the content by breaking it down into easily understandable sections. The Security Awareness Training (SAT) is delivered in a non-technical manner to individuals without any knowledge of IT or cyber security to give a good general understanding.

The training is informal and is delivered on the customers site to minimise disruption. We use day to day real world examples of breaches, to help you bring the risks to life. Providing more context to our personal lives we use examples of threats that we all see on a daily basis, such as phishing emails and scams sent to our personal emails.

Delivered in a vibrant and interactive manner, our training helps employees understand the key risks, threats and vulnerabilities and most importantly the impact that a breach can have on the business and their own lives. A key takeaway will be that whilst humans are typically the 'weak link', they can also be the strongest form of defence. Whilst an organisation may have the latest and greatest security technologies and controls, these can be undermined by a simple slip of the tongue, clicking on the wrong link or opening the wrong attachment.

Our Scope

Our SAT service is designed to deliver security awareness to all employees within your organisation. It is therefore not technical in nature but rather focuses on;

- Why security is important and why it impacts delegates
- Types of security threats – and where they come from
- What the 'threat landscape' means and why this is important
- How to recognise a threat or a security incident and what to do
- Key attack techniques, including phishing, spear-phishing, ransomware and more
- Why humans are a weak link but can also be the first line of defence
- Practical things to do and think about to improve security across the business
- How these threats impact employee's personal lives

Your Benefit

By providing a functional real world understanding of cyber security to your staff we will improve your security culture by creating awareness while providing actionable, usable rules as takeaways

The SAT will contribute to transitioning your staff from your weakest link to your first line of defence.

The Engagement

As an example, a typical training package is £1,300 (ex VAT), based on;

- One days training delivered on client site
- 45-60min sessions, typically 4 sessions per day
- 10-15 people in each session
- Standard SAT material



About ICA Consultancy

ICA Consultancy provides advisory and consultancy services, and Virtual CISO engagements to organisations to help them identify, manage and mitigate risks relating to information and cyber security. Through experienced resources they deliver pragmatic and sustainable solutions, enabling clients to improve their maturity whilst maximising the benefits from their investments.

ICA Consultancy's services are grouped into three offerings, designed to **Assess** an organisations maturity, **Assist** in making the required sustainable improvements and **Advise** on how to maintain their security posture going forward.



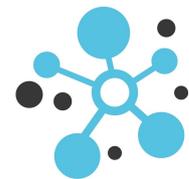
Assess

Our Assess services are designed to provide an organisation with a view of the maturity of their security controls. Ranging from posture reviews through to specific control assessments we will identify risks and provide pragmatic, prioritised recommendations.



Assist

Our Assist services, including our Virtual CISO offering, are designed to support organisations delivering maturity improvements, defining or implementing strategies, engage with their board members or manage day-to-day operations.



Advise

Our Advise services are designed to help organisations maintain their security posture, providing access to expertise and experience required to deliver training and awareness, support hiring processes, or select product or service providers.

ICA Consultancy can also bespoke engagements to client requirements and will always work with clients to define and deliver the most appropriate service based on their needs. ICA Consultancy are technology agnostic and remain independent. This ensures clients receive a service that is contextualised to their business environment and challenges.

To understand how ICA Consultancy can help your organisation, email info@icaconsultancy.co.uk or visit <https://icaconsultancy.co.uk> for more information.