Hutsix

A Guide to Security Awareness Training

2024/25

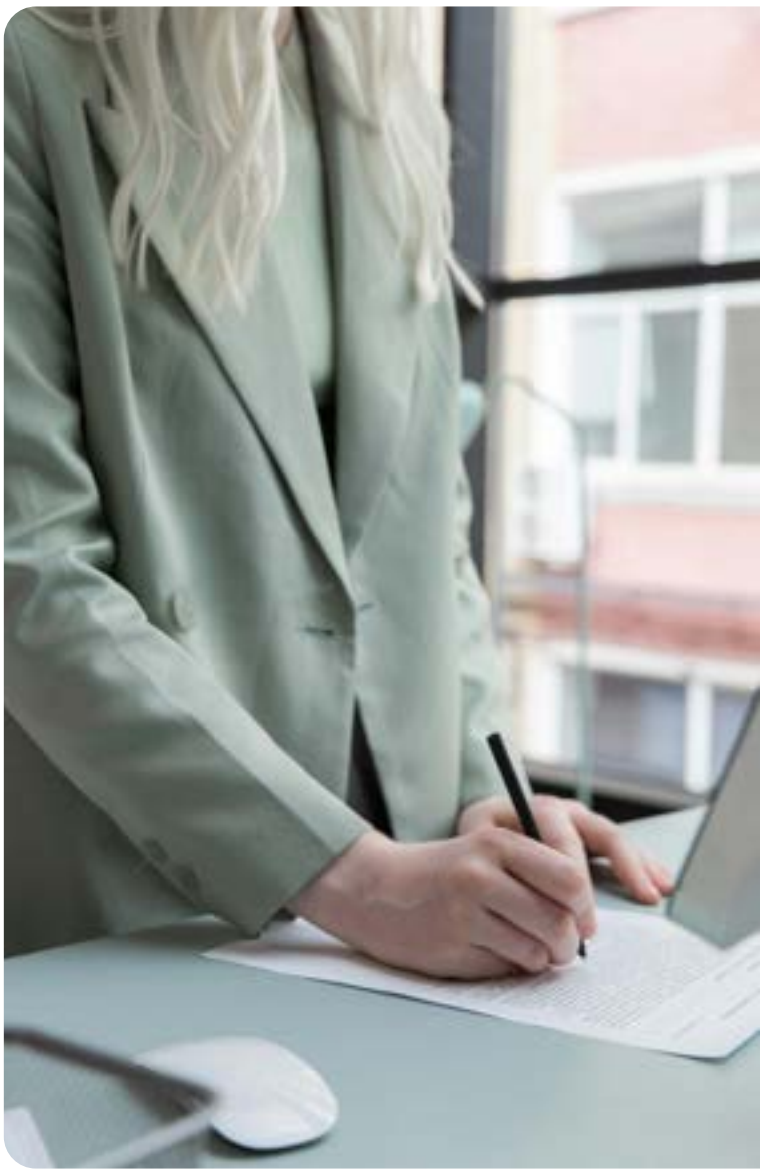
Introduction

Welcome to the Hut Six Guide to Security Awareness Training, your essential resource for building a robust security-conscious culture within your organisation.

As cyber threats continue to evolve, equipping employees with the knowledge and skills to protect sensitive information is more crucial than ever.

This guide provides comprehensive insights into effective training strategies, interactive learning methods, and measurable progress indicators.

Whether you are new to security awareness or looking to enhance your existing programme, this guide will help you foster a vigilant workforce, mitigate risks, and safeguard your digital assets in today's dynamic cyber landscape.



Contents

The Security Landscape in 2024

> **In 2024, the cybersecurity landscape continues to grow more complex and challenging. It's estimated that a staggering 70% of data breaches involve human error or oversight. Whether it's due to social engineering attacks, inadvertent mistakes, or misuse of resources, the need for effective security awareness training has never been more evident.**

Evolving Threats

Cyber threats are becoming increasingly sophisticated, with attackers leveraging advanced tactics to exploit vulnerabilities. Phishing attacks, particularly spear phishing, have become more targeted and convincing, making it harder for employees to discern malicious communications from legitimate ones.

Remote Work and Hybrid Environments

The shift to remote work and hybrid environments has introduced new security challenges. Employees accessing sensitive data from various locations and devices create potential entry points for attackers. Ensuring that employees understand and adhere to security protocols, regardless of where they work, is crucial to maintaining a secure organisational network.

Insider Threats

Not all threats come from external sources. Insider threats, whether malicious or accidental, pose significant risks to organisations. Employees with access to sensitive information can inadvertently or intentionally cause data breaches.

Regulatory Compliance

Organisations must navigate an increasingly stringent regulatory landscape. Compliance with data protection laws such as the General Data Protection Regulation (GDPR). Non-compliance can result in severe penalties and reputational damage, emphasising the importance of comprehensive security awareness training.

Technological Advancements

As organisations adopt new technologies like artificial intelligence, cloud computing, and the Internet of Things (IoT), the attack surface expands. Each new technology introduces unique vulnerabilities that cybercriminals are quick to exploit.

The Role of Security Culture

Building a robust security culture within an organisation is essential. This involves not just training employees on specific security practices but also instilling a mindset where security is a shared responsibility. A strong security culture ensures that employees remain vigilant and proactive in protecting the organisation's assets.

In this dynamic security landscape, continuous education and awareness are key to defending against cyber threats.

This Guide to Security Awareness Training aims to equip your organisation with the knowledge and tools needed to foster a security-conscious workforce, mitigate risks, and safeguard your digital assets.

Understanding Human Error

> **At its core, human error is simply unintentional action. These actions can vary dramatically in their severity, from inconsequential and perhaps unnoticed to extremely damaging, potentially posing an existential threat to an organisation.**

Broadly speaking, human error is typically divided into two distinct types:
skill-based errors and ***knowledge-based errors.***

Skill-based errors are minor lapses and small mistakes that occur when an individual is performing familiar tasks. Although the individual understands how to perform these actions correctly, inattention, distraction, or negligence leads to a temporary failure to follow proper procedures.

In contrast, a knowledge-based error occurs when an individual lacks the necessary information to avoid a mistake. When faced with a novel situation, the individual may not even realise they have made an error in judgement.

Common Forms of Human Error

Password Process

Maintaining robust password practices is crucial. Common errors include reusing passwords and improper storage. Policies against password reuse, reliable password management solutions, and training users to create strong passwords are essential.

Data Mishandling

All organisations handle sensitive information, which requires strict precautions. Mis-delivery of information is a common error. Ensuring employees are trained to handle data correctly helps prevent breaches and avoid substantial fines under regulations like UK GDPR.

Phishing Emails

Clicking on phishing emails can be highly damaging. Phishing exploits human instincts like curiosity and urgency. Training users to inspect links, double-check details, and avoid opening certain file types can significantly reduce these errors.

The Importance of Information Security Training

> **Cyber security awareness training is a form of education that teaches employees how to identify, prevent, and respond to cyber threats. The goal is to create a culture of security awareness within an organisation, so that all employees are better equipped to protect their organisation from cyber attacks.**

Security awareness training for employees is far from a box-ticking exercise; it is a crucial investment in an organisation's overall resilience.

Here are five compelling reasons why prioritising such training for employees is of utmost importance:

1 Cyber Threat Landscape Evolution

The digital landscape is ever evolving, and so are cyber threats. Security Awareness Training ensures that employees stay abreast of the latest threats, empowering them to recognise and mitigate potential risks effectively.

2 Organisational Risk Mitigation

Employees, being the frontline of defence, play a pivotal role in mitigating organisational risks. Training instils a sense of responsibility, making them active contributors to a secure work environment.

3 Human Firewall Against Attacks

In many cyber attacks, human error is the weakest link. Security awareness training builds a human firewall, equipping employees with the knowledge to identify phishing attempts, social engineering, and other tactics employed by cybercriminals.

4 Legal and Compliance Requirements

Meeting legal and compliance standards is non-negotiable. Security training ensures that employees understand and adhere to these standards, reducing the risk of legal consequences and reputational damage.

5 Cultivating a Security Culture

Training goes beyond imparting knowledge; it cultivates a security-first culture. When every employee is well-versed in security practices, it creates a collective consciousness that strengthens the organisation's overall security posture.

Does Security Training Work?

> **The success of a security awareness program hinges on several factors, including the quality of content, employee engagement, and the organisation's commitment to continuous improvement. When executed effectively, a security awareness program can significantly enhance an organisation's overall security posture by mitigating the risk of security breaches and incidents.**

5 Reasons Security Awareness Training Fails

1 Generic Approach

A one-size-fits-all strategy often fails to engage employees. Tailoring training to specific roles and departments is crucial.

2 Uninspiring Delivery

Traditional methods like lengthy lectures lead to disinterest and poor retention.

3 Outdated Content

Irrelevant and outdated content makes training ineffective. Regular updates are necessary to address evolving cyber threats

4 Lack of Measurement

Inadequate progress tracking and lack of ongoing support contribute to failures. Continuous assessment and key performance indicators are vital.

5 Cultural Resistance

Resistance to a security-centric culture within the organisation hinders success. A successful programme recognises these challenges and addresses them to foster a vigilant and cyber-aware workforce.

5 Elements of Successful Training

The most effective security approach is holistic and people-centric, encompassing processes and technology:

1 Understanding Risks

Begin with a thorough understanding of your organisation's unique risks and vulnerabilities.

2 Comprehensive Training

Ensure employees are aware of cybersecurity threats and their roles in preventing them.

3 Advanced Technology

Implement advanced technology, such as firewalls, antivirus software, and encryption, to safeguard digital assets

4 Regular Updates

Stay ahead of evolving threats with regular updates and a robust incident response plan.

5 Cultural Shift

Create a culture where every member throughout the organisation takes security seriously. This empowers employees to be vigilant and proactive in identifying and mitigating potential risks.

Essential Topics for Employee Security Training

> **One reason for cyber and information security training becoming a workplace necessity is the rate at which security threats evolve. Cyber attacks are increasing in number, with 4 in 10 of UK businesses reporting a cyber security breach or attack. The costs have risen as well with a data breach damaging finances, customer confidence, reputation and more. Security awareness training is on every board's agenda.**

Phishing

Phishing attacks deceive users into revealing information. These social engineering attacks occur via email, social media, SMS, and instant messaging, enticing users to click links or share personal details.

Spear phishing, a more sophisticated variant, intercepts invoices and sensitive communications, highlighting the need for robust security training.

Password Security

Passwords are essential for securing systems, networks, and devices. Common issues include weak passwords and reuse. Using unique passwords for each account and employing multi-factor authentication for sensitive accounts are vital practices.

A simple method for creating strong passwords is combining four unrelated words.

Mobile Devices

Mobile devices pose significant security risks due to their portability and storage of sensitive information.

Ensuring devices are password-protected, encrypted, and capable of remote wiping helps prevent unauthorised access.

Web Safety

Web safety involves recognising and avoiding malicious websites. Understanding URLs and what constitutes a dangerous webpage is crucial.

Educating users on best practices for social media, online banking, and shopping greatly enhances their cybersecurity.

Malware

Often introduced through phishing emails, can severely damage systems and data. It includes spyware, adware, and ransomware. Defending against malware requires antivirus software and vigilant training.

Wi-Fi

Public Wi-Fi networks can be insecure, making data susceptible to interception through man-in-the-middle attacks. Employees should use VPNs to secure data transmission on public networks.

Social Engineering

Social engineering manipulates individuals to extract information, including through phishing and physical interactions like tailgating. It is crucial to cover this topic in any security awareness training programme.

Backing Up Data

Regular data backups ensure availability even after an attack. Employees should be trained on the importance of data backups to safeguard information and ensure business continuity.

Sensitive Information

Handling sensitive data requires a security-aware mindset. Employees must understand the importance of access control, clean desk policies, and physical security measures to protect business secrets, intellectual property, and personal data.

Identifying and safeguarding sensitive information is paramount.

Encryption

Encryption protects data from unauthorised access, ensuring secure communication. Organisations must properly store and secure customer information, and employees should understand basic encryption methods.

How Often Should Training Be Conducted?

> **When learning a new skill, consistent practice adds up. Well, as many studies have found, the same is true for employees and information security awareness training. While providing employees with a single, or even annual training session may have some level of effect, put simply, a one-time or infrequent training approach is insufficient.**

To ensure that the information security awareness-based knowledge is retained, many researchers (e.g., **Caputo, et al.**, **Kumaraguru, et al.**, and **Jampen, et al.**) have concluded that an information security program needs to be designed as an ongoing process - ideally one which is integrated into users' daily workflow.

Furthermore, knowledge gained from information security awareness training needs to be put into continual practice, in a way which allows individuals to retain this information and adopt these new behaviours into routine.

Termed by some as **'Persistent Tr aining'**, there is still some level of discussion about optimal regularity.

"Training should be designed... as an ongoing process within an organisation... Each user should be exposed to such training at least once every 5 months."

- Reinheimer, B. et al.

In the 2020 study, **An Investigation of Phishing Awareness and Education Over Time: When and How to Best Remind Users**, researchers found that users' ability to correctly identify phishing emails significantly improved directly after and four months after the deployment of training programme; though these anti-phishing skills were not, unfortunately, present six months after the educational intervention.

Although biannual training may sound frequent, techniques such as embedded training, which includes simulated phishing attacks linked to resources, means relevant training can be conducted while minimising potential disruption or annoyance.

A further bonus of this form of training being that organisations can gather ongoing information and metrics as to how well their staff can identify and avoid various information security threats, while also steadily and deliberately increasing the breadth of users' knowledge.

Measuring the Effectiveness of Security Training

While measuring the effectiveness of security awareness training can be challenging, it is a crucial aspect of determining the overall impact of training on improving users' security behaviour.

Though no single metric can provide a comprehensive view of the effectiveness of security awareness training, it is advisable to use a combination of these following ten metrics to provide a broad overview:

Pre-Training Assessments

- Establish a baseline of employees' knowledge with questionnaires or online quizzes.
- Identify knowledge gaps to tailor training programs effectively.
- Compare pre- and post-training results to measure impact.

Participation Rates

- Track completion rates to gauge employee engagement.
- Higher rates indicate better commitment and training coverage.
- Active participation suggests improved knowledge retention and behaviour change.

Phishing Simulation Results

- Send mock phishing emails to test employee recognition and reporting.
- Decreased click rates and increased reporting indicate training effectiveness.
- Measure improvements in employees' ability to discern phishing attempts.

Quiz Scores

- Compare scores before and after training to evaluate understanding.
- Identify specific areas needing additional training.
- Regularly monitor scores to assess

Security Incident Metrics

- Track incidents like breaches and malware infections.
- Decreased incidents suggest positive behavioural changes from training.
- Improved adherence to security policies

Employee Feedback

- Collect feedback through surveys to gauge training relevance and effectiveness.
- Identify areas for improvement and any remaining knowledge gaps.
- Use feedback to refine future training programs.

Compliance Metrics

- Monitor adherence to policies like data classification and multi-factor authentication.
- Improved compliance rates indicate effective training.
- Higher compliance reduces the risk of security incidents and breaches.

Completion Rates

- High completion rates show active engagement with training materials.
- Identify barriers to completion and improve training accessibility.
- Ensure content is valuable and engaging to maximise impact.

ROI

- Compare training costs to benefits like reduced incidents and compliance savings.
- ROI analysis justifies investments and optimises resource allocation.
- Continuously evaluate ROI for ongoing improvements.

Continuous Evaluation

- Ongoing monitoring and feedback collection.
- Benchmark against industry trends and incorporate lessons learned.
- Adapt training to address evolving security threats and foster a culture of continuous improvement.

Security Awareness and Culture

Fostering a strong security culture is imperative to mitigate evolving cyber threats. The following are 5 steps to foster an effective information security awareness culture:

1 Awareness Training

Effective awareness training is crucial for building a robust information security culture. It equips employees with essential knowledge to identify and mitigate risks, enhancing their understanding of evolving threats and their role in safeguarding information. Interactive, tailored tutorials empower practical decision-making and proactive defence.

2 Leadership

Leadership sets the security tone by exemplifying commitment to protocols and integrating security into decision-making. Continuous learning ensures leaders are informed, fostering a culture of improvement. Recognising security achievements motivates vigilance and promotes early incident reporting, reinforcing a collective responsibility for security.

3 Recognising Achievement

Acknowledging and rewarding security efforts motivates engagement and supports a culture of reporting. Continuous recognition drives policy improvements and enhances overall security.

4 Reporting

Reporting is critical for early threat detection. An open, safe reporting environment encourages timely incident disclosure. Effective response procedures minimise impact and leverage data insights to refine security strategies.

5 Communication

Transparent communication ensures clarity on security policies and practices. Regular updates empower employees to respond effectively to emerging threats, fostering comprehensive security awareness and vigilance.

Getting Started

Any organisation can fall victim to an information security incident. Despite technical precautions that help mitigate this risk, your employees are the most immediate and vulnerable target for malicious actors - and your first line of defence.

Now more than ever, you rely on your people making the correct choices in the face of security decisions.

Thankfully, with the right knowledge, many of these human vulnerabilities can be easily addressed.

Hut Six's Security Awareness Training solution helps to reduce the risk of a successful cyber-attack. Preventing financial losses, damage to reputation, potential fines, and litigation, robust and engaging information security training is an essential for any organisation looking to improve their information security culture

Try our Training for Free!

Free Trial **Book a Meeting**


Hutsix