National Cyber Security Centre
a part of GCHQ

Guidance (/)

10 Steps: User Education and Awareness

Created: 29 Sep 2015
Updated: 08 Aug 2016
Part of: 10 Steps to Cyber Security (/guidance/10-steps-cyber-security)
This section from within the NCSC's '10 Steps To Cyber Security' concerns User Education and Awareness.

Summary

Users have a critical role to play in their organisation's security and so it's important that security rules and the technology provided enable users to do their job as well as help keep the organisation secure. This can be supported by a systematic delivery of awareness programmes and training that deliver security expertise as well helping to establish a security-conscious culture.

What is the risk?

Users have a critical role to play in helping to keep the organisation secure, but they must also be able to effectively do their jobs. Organisations that do not effectively support employees with the right tools and awareness may be vulnerable to the following risks:

- **Removable media and personally owned devices:**Without clearly defined and usable policies on the use of removable media and personally owned devices, staff may connect devices to the corporate infrastructure that might lead to the inadvertent import of malware or compromise of sensitive information
- **Legal and regulatory sanction:** If users are not aware and supported in how they handle particular classes of sensitive information, the organisation may be subject to legal and regulatory sanction
- **Incident reporting culture:** Without an effective reporting culture there will be poor dialogue between users and the security team. This is essential to uncovering near misses and areas where technology and processes can be improved, as well as reporting actual incidents.
- **Security Operating Procedures:** If security operating procedures are not balanced to support how users perform their duties, security can be seen as a blocker and possibly ignored entirely. Alternatively, if users follow the procedures carefully this might damage legitimate business activity.
- **External attack:** Since users have legitimate system accesses and rights, they can be a primary focus for external attackers. Attacks such as phishing or social engineering attempts rely on taking advantage of legitimate user capabilities and functions.
- **Insider threat:** Changes over time in an employee's personal situation could make them vulnerable to coercion, and they may release personal or sensitive commercial information to others. Dissatisfied employees may try to abuse their system level privileges or coerce other employees to gain access to information or systems to which they are not authorised. Equally, they may attempt to steal or physically deface computer resources.

How can the risk be managed?

Produce a user security policy: Develop a user security policy, as part of the overarching corporate security policy. Security procedures for all systems should be produced with consideration to different business roles and processes. A 'one size fits all' approach is typically not appropriate for many organisations. Policies and procedures should be described in simple business-relevant terms with limited jargon.

Establish a staff induction process: New users (including contractors and third party users) should be made aware of their personal responsibility to comply with the corporate security policies as part of the induction process. The terms and conditions for their employment, or contract, should be formally acknowledged and retained to support any subsequent disciplinary action.

Maintain user awareness of the security risks faced by the organisation: All users should receive regular refresher training on the security risks to the organisation. Consider providing a platform for users to enquire about security risks and discuss the advice they are given. On the whole, users want to do the right thing, so giving them guidance to put security advice into practice will help.

Support the formal assessment of security skills: Staff in security roles should be encouraged to develop and formally validate their security skills through enrolment on a recognised certification scheme. Some security related roles such as system administrators, incident management team members and forensic investigators may require specialist training.

Monitor the effectiveness of security training: Establish mechanisms to test the effectiveness and value of the security training provided to all users. This will allow training improvements and the opportunity to clarify any possible misunderstandings. Ideally the training provided will allow for a two-way dialogue between the security team and users.

Promote an incident reporting culture: The organisation should enable a security culture that empowers staff to voice their concerns about poor security practices and security incidents to senior managers, without fear of recrimination. This should be reciprocated with a culture where security professionals acknowledge that security-related effort by non-security staff is time away from their work, and is helping to protect the organisation.

Establish a formal disciplinary process: All staff should be made aware that any abuse of the organisation's security policies will result in disciplinary action being taken against them. All sanctions detailed in policy should be enforceable at a practical level.

Topics

Skills and training(/topics/skills-and-training)
Cyber attacks(/topics/cyber-attacks)

Was this guidance helpful?

We need your feedback to improve this content.

Yes No