Social Engineering Audit and Security Awareness Programme

Every chain is as hard as its weakest link, and in for information security this chain-link is often human factors. Employees often have direct access to protected assets, making them the most obvious target of those with malicious intent for gaining access to sensitive information. If they by-pass security controls via Social Engineering methods, such potential attackers are able to base their attacks on a lack of user awareness.

Every enterprise possesses secure data, whose illegal publication or modification can result in negative consequences for the business. Typically, employees do not know enough about Social Engineering tricks and techniques and are unaware that they could unwillingly help an attacker with seemingly unimportant information. Taking these phenomenon into consideration, identification of the human risks, assessing the awareness level of the organisation and implementation of a security awareness programme are significant challenges.

How can we help?

KPMG’s IT Risk Advisory group offers several services to improve the security awareness level of organisations. We have effective and efficient methods to test and assess the awareness of employees and improve it according to objectives defined from identified deficiencies. We recommend implementing a security awareness programme as follows.

First, we suggest the assessment of the current level of user awareness and effectiveness of security controls, which can take place via use of our Social Engineering Audit Programme. The results of this project comprise identified awareness deficiencies, inadequately implemented security countermeasures and ineffective controls. The audit findings can be used towards the modification of the enterprise’s current information security regulation and its implementing new countermeasures. Out of necessity, the Security Awareness Programme is based on an awareness training, which should be repeated yearly, and, lastly, upon an awareness campaign, which is designed to help maintain vigilance regarding the subject.

Read more about our Security Awareness Services in the following summary.
Assessment of security awareness level – Social Engineering Audit

Social engineering is a collection of attack methods and techniques, which exploit the deficiencies of user awareness. Illegal access to sensitive information, data leaks or other security breaches could be based on employees not knowing the contents of security policies, or not observing the rules. Technological solutions do not provide complete security against Social Engineering attacks; the only one effective countermeasure is the improvement of security awareness.

The best method to measure security awareness of an organisation’s employees is to perform a Social Engineering Audit. In the course of this project the current security controls will be tested by testing human factors. Below is an outline of the tasks of our audit programme based on the most frequent attack types and the most common security awareness deficiencies.

**Possible tasks of a Social Engineering audit**

### Gathering basic information for attacks
Social Engineering attacks based on information gathered about the targets: the company and its employees. For this reason the first step of our audit (as in the case of a real attack) is the gathering of all available public data on the Internet: e-mail addresses, phone numbers, organisational charts and other information that a potential attacker can use to their benefit.

### Facility intrusion
The purpose of this task is to test how an attacker might enter into a building or offices of the enterprise illegally and how can he/she could bypass entrance security controls.

### Attacks within the facility
After a successful illegal intrusion into an enterprise’s building we will inspect possible vulnerabilities which emanate from human factors, i.e.: What kinds of devices and information can we access in an empty office and what could be done with them if we were people with malicious intent? As part of this test we may steal notebooks or other devices, install programmes that simulate keylogger software, copy sensitive information to a pendrive, or we might even install a wireless network device to be able to access the company’s internal network outside of the office.

### Impersonation via telephone
Attacks via telephone involve our auditor impersonating a fictive employee of the organisation or one of its partners in which he/she asks the target to send a sensitive document (assigned before starting the project) via e-mail to outside of the organisation, or he/she persuades the employee to disclose his/her password. The result of this audit task is to assess the ability of users to filter suspicious questions and requests, test how employees ascertain the caller’s identity and determine that they are aware of the sensitivity of requested information.

### Dumpster diving
Dumpster diving is a method of gathering sensitive data from an enterprise’s waste bin. By checking the contents of the trash we can gain evidence on the usage of containers collecting sensitive documents or shredders, and how employees have applied security classification of information to this waste.

### Field inspection
In case of a field inspection we make a supervised visit to an enterprise’s facilities to inspect how the company’s employees observe security rules and policies. Are their computers locked if they leave them unattended? Do they leave sensitive documents on their desks unguarded? Do they retrieve printed documents or are these forgotten in the tray of the printer?

### Phishing
The purpose of phishing attacks is to test users’ reaction to messages sent via e-mail or other communication channels, which, at first sight, appear to emanate from their workplace. Such communications request the divulging of sensitive information like user IDs and passwords.

### Spreading malware via e-mail (attachment or link)
In this task we send to all employees of the enterprise an attached file (PDF, Excel, Word document or even an executable file), or a link to a website which simulates a malicious code, and we measure how many users open the content and/or click-through.

### Baiting
Baiting happens when we “lose” some pendrives or CDs/DVDs in the client’s office building and observe what the company’s employees do with them. All of these storage devices contain an executable file which tracks if someone opens it. This enables us to ascertain how users mind the rules and recommendations of handling lost data travelers.

Based on these audit tasks we offer several audit packages containing customised, organisation-specific audit scopes to enable selection of the most suitable audit programme for your company.
Security awareness training

After identifying security weaknesses emanating from human factors, the organisation can determine the requirements of security awareness, followed up by training for employees. Its purpose is to inform colleagues about the security policies and rules of the organization and the necessity of observing them, as well as creating awareness of threats and attack types which target users. Deficiencies and weaknesses identified by a Social Engineering Audit can be useful examples for the training to demonstrate the relevance of these risks.

According to the most frequently experienced security awareness weaknesses and deficiencies, our Awareness Training contains a review of the types of attacks which exploit human factors (for example, physical intrusion, mystification, phishing, malware and other Internet risks) and how to mitigate the risk of these potential dangers. It also interprets the company’s related policies and rules and transmits organisation and position-specific security knowledge.

We recommend establishing our Training Programme at three levels: separate trainings for all users, for management and for the IT function. Specified training materials support participants in recognising the relevant threats and related security countermeasures.

When a Social Engineering project is performed before security awareness training, trainings might rely upon test methods and their results. Simulated attacks are the best examples to draw the attention of employees to the reality and relevance of such threats. According to our experience, participants can acquire awareness knowledge more effectively if attack methods are demonstrated through the results of a Social Engineering Audit.

Training levels

All users
A general security awareness training represents threats and vulnerabilities concerning all employees of the company. Training material contains the most typical attack techniques and prevention methods.

Management
Management training is more specialised and focussed on the demands of chief officers. Training is based on general awareness knowledge but contains specialised risks which cause concern for management (for example the security of mobile devices) and methods as to how they can motivate colleagues in improving awareness attitudes and/or behaviour.

IT operation
Employees working as IT operator or system administrators bear a higher level of security awareness than other users. Accordingly, they receive a shorter general security awareness training and the training material prepared for them will contain specialised topics for IT operation like the basics of operation security, network security and business continuity.
**Security awareness campaign**

Beyond assessing the level of users’ security awareness and periodically organised awareness trainings, it is also important to sustain employees’ awareness. The most effective method to achieve this is to organise a campaign, which can help remind employees every day of the most important security concerns.

Possible elements of the campaign:

- A fictional character or “comic book”-like series containing motivating messages
- Posters in the office promoting security awareness
- Screensavers highlighting human factor threats
- Monthly newsletters
- Tests, exercises and games.

KPMG’s Security Awareness Services are implemented according to our methodology based and tested on numerous successful Social Engineering Audits and information security training. During the course of such projects we have acquired a substantial knowledge base on organisation-specified security awareness weaknesses and deficiencies, which can be used to plan the most suitable security awareness assessment and training for your company.

---

**Contact**

György Sallai  
**Director**  
T: + 36 1 887 6620  
E: gyorgy.sallai@kpmg.hu  

kpmg.hu