Deloitte.

Social Engineering
Information on the look-out

”Data is only as good as the person inputting it, and security is only as good as the person writing the policies and implementing them. A computer just sits there until someone turns it on, and a company is only secure until someone breaches it“. Sans Institute

Malicious attackers pose as someone else to gain information they otherwise cannot access. Further to this, they then take the information acquired from their victims and cause destruction on network resources, steal or delete files, and even commit industrial intelligence or some other form of fraud against the organisation they’re attacking.

Our Service Offering

In a social engineering attempt, we will evaluate your employees’ level of security consciousness done through personal contact; we will persuade them into conveying confidential information to us, primarily user IDs and passwords. Our social engineer, i.e. attacker, will counterfeit a specific trustworthy identity to a member of the organisations’ staff in order to gather the preferred information.

Our Appoach

Our approach to Social Engineering is to find the details of organisational processes and information systems to perform our attack. With this information, we will give effort in finding all critical evidence in order to pursue our task. We simulate and perform social engineering attacks in three steps:

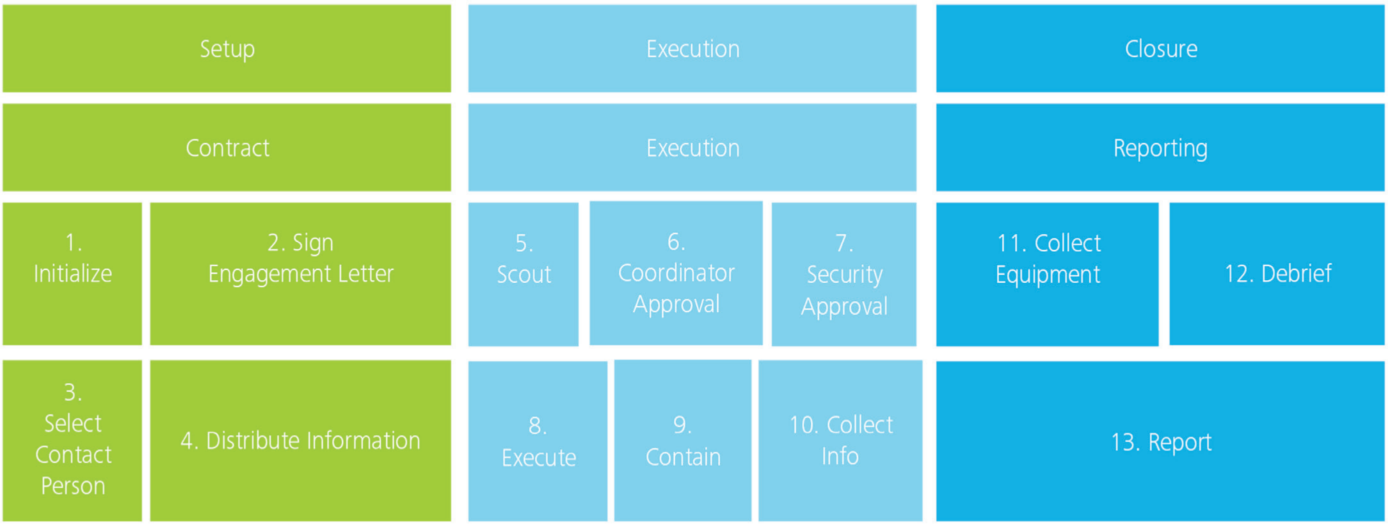
- Setup
- Execution
- Closure

> *”Also, the human part of the security set-up is the most essential. There is not a computer system on earth that doesn’t rely on the humans. This means that this security weakness is universal, independent of the platform, software, network or age of equipment.*
>
> *Kevin Mitnick*

Through our experience and exposure to the industry it is indicated that thirty percent of all hacking comes from outsiders: that is people who are not working for the attacked organisation. This means that seventy percent of hackers come from within the organisation. Our attempt will be conducted by an interloper who will use a variety of psychological tricks on a computer user to get the information necessary in order to access a computer or network.

This is the classic form of social engineering where we will use the direct conversation with our victim, via telephone or personally on site, to obtain the desired information or to gain physical access to any protected info. People are usually the weakest link in the security chain. Our skilled social engineers will try to exploit human weakness before spending time and effort on other methods to crack passwords or gain access to systems. Our approach is usually based in the following characteristics:

- A tendency to trust people. Human nature is to actually trust others until they prove that they are not trustworthy.
- The fear of getting into trouble.
- The willingness to cut corners. Posting passwords on the screen or leave important material lying out.



Setup	Execution	Closure
Contract	Execution	Reporting
1. Initialize 2. Sign Engagement Letter	5. Scout 6. Coordinator Approval 7. Security Approval	11. Collect Equipment 12. Debrief
3. Select Contact Person 4. Distribute Information	8. Execute 9. Contain 10. Collect Info	13. Report

Several potential security breaches are so mundane that they hardly seem to be of concern. With all the fires that we have to battle each day and the deadlines we have to meet, sometimes the most obvious is often unnoticed.

Social engineering is an unbreakable form of attack to protect against since it cannot be safeguarded with hardware or software alone. In our effort to expose the policy procedures and security awareness, we will use various ways to obtain the desired information, either by sending the users a form of an e-mail messages or leading them to a Web site which is seemingly trustworthy, as is done in "Phishing" attacks. By doing so, the user will be asked to reveal specific login data or to download software manipulated by our engineering team.

Passwords are the number one access point for our social engineer. System-generated passwords are too long and employees have to write them down to remember them.

Information on the Look-out

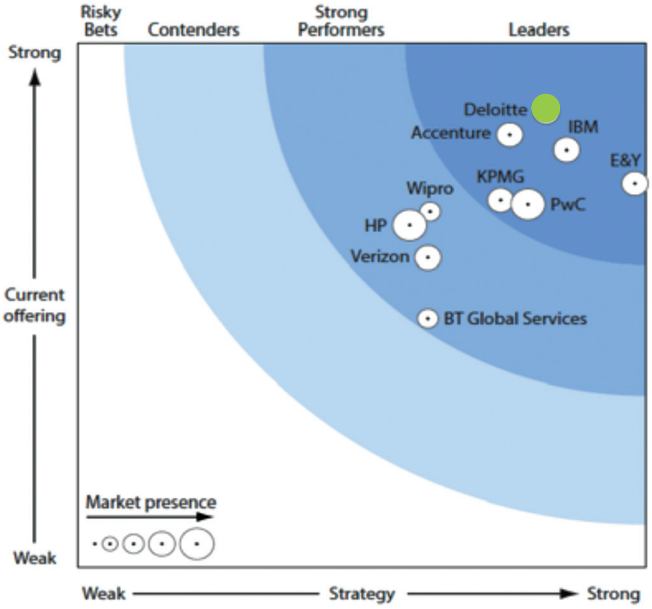
- Internal phone lists
- Organisational charts
- Employee handbooks, which often contain security policies
- Network diagrams
- Password lists
- Meeting notes
- Spreadsheets and reports
- Printouts of e-mails that contain confidential information

All findings will be reviewed, analyzed and compiled in a report. We will discuss the findings with you and elaborate on measures aimed at raising awareness to increase the company's internal security level permanently.

After this project is completed, a successful defence will require effective information security architecture starting with policies and standards and following through with a vulnerability assessment process again to verify that compliance is met.

World class services

- Our security experts have the same skills and methods hackers use, but can also translate technical issues into business risks.
- Deloitte has a global reach, with a presence in over 150 countries worldwide.
- We can support you in solving security issues as a trusted advisor in a vendor-agnostic, but knowledgeable way.
- Deloitte has been named a leader by Forrester Research, Inc. in Information Security Consulting in a new report, The Forrester Wave™: Information Security Consulting Services, Q1 2013.



Cybercrime.
Be ready.

Deloitte.

For more information on Deloitte's Cyber Risk Services, please contact:

Panicos Papamichael
Partner, Enterprise Risk Services
Tel.: +357 22 360805
E-mail: ppapamichael@deloitte.com

Deloitte Limited is a private company registered in Cyprus (Reg. No. 162812). Offices: Nicosia, Limassol, Larnaca.