Deloitte.

Security Awareness

People and Technology

New technology risk is inevitable. People must learn how to handle it.

Technology advancements and the people using these technologies introduce information security risks. The human element is one of the biggest sources of information security risk identified, as well as one of the most difficult to control. According to a Deloitte's Technology, Media, and Telecommunications (TMT) Global Security Study, 70% of the TMT organizations surveyed rate their employees' lack of security awareness as an "average" or "high" vulnerability. Employees without sufficient awareness of security issues may put an organization at risk by talking about work, responding to phishing emails, letting unauthorized people inside the organization, or even selling intellectual property to other companies.

Your Challenge

- We rely on humans to implement controls and policy because we cannot "engineer around the end user" - avoiding incidents remains highly dependent of what your end users do.

Lack of Sufficient Security Awareness is one of the Top vulnerabilities (perceived as average or high threat)

70%

Lack of sufficient awareness with employees

- In addition, people do not act security by nature, and secure behaviour erodes with time, especially when there is a lack of security awareness. This makes life easier for any malicious party; *you don't need to hack the system if you can compromise the human.*
- To further complicate matters, significant changes in behaviour are often required - but few things are harder to change than security culture - which is an integral part of company culture.

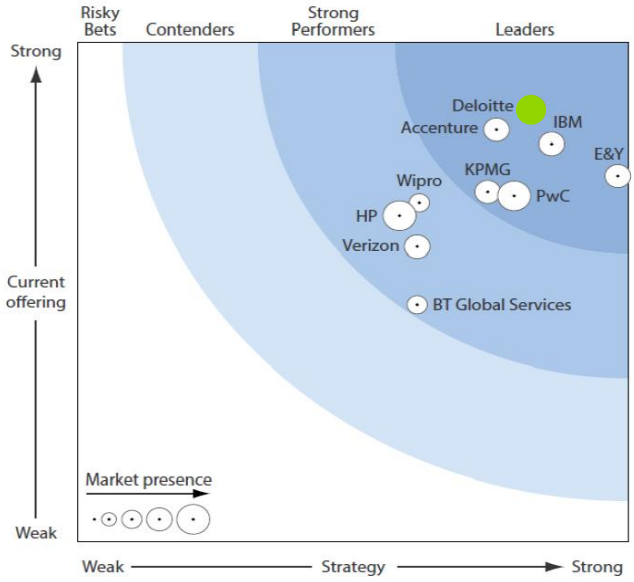
Deloitte.

Our Solution

- We have a variety of services allowing the organisation to instil knowledge, ability and inclination in people to act securely.
- We cover the complete scope of activities required to develop and improve security awareness: assessments (to what extent are people acting securely or not), designing and delivering content, measuring how security awareness improves and perhaps most importantly, providing the support you need to change the security culture of your organisation.
- Security awareness starts at the top which is why our approach to security awareness starts with the identification of key stakeholders and joint development of the security strategy with the stakeholders. This significantly improves the chances of achieving the required change in security culture.

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.



Bringing the right team to your organization

Contact

Do you want your cyber readiness and user awareness tested by our team of ethical hackers? Contact us:

Panicos Papamichael
Partner – Risk Advisory
(+357) 22 360 805
ppapamichael@deloitte.com

Yiannis Ioannides
Manager- Hacking services
(+357) 25 868 849
ymioannides@deloitte.com