IT Security – The Challenge of Protecting your Data, and that of Your Organisation

Overview

We live in an age where information is becoming increasingly valuable, so the need to safeguard that information is becoming increasingly important. However, the way that individuals now interact and purchase goods and services, and that organisations and businesses now operate, demands that greater and greater amounts of information be more freely available online. This has many benefits, but an undesirable side effect is that cybercrime is becoming more widespread. Methods of illicitly gathering information, for example, phishing, spamming, and hacking are becoming more sophisticated. To counter this, greater awareness of the most important concepts and skills relating to IT security is required among the large and rapidly expanding proportion of the population who are active online.

The Challenges Facing IT Security – Humans are as Vulnerable as Systems

IT security can be divided into two distinct categories – an individual protecting their home and organisations protecting the workplace. However, despite the increased levels of automation in the workplace, it is still the actions of the individual worker that will expose an organisation to IT security threats[1]. As humans can be the most vulnerable link in the information security chain, there is an increasing need for a greater awareness and understanding of security issues, including the need to develop a 'culture of security'. This can be described as a focus on security in the development of information systems and networks, and the adoption of new ways of thinking and behaving when using and interacting within information systems and networks[2]. The IT security of an organisation is therefore inextricably linked to the user's behaviour, and there are several approaches that organisations currently take to try to minimise their own exposure to security breaches and to protect themselves and their data from theft or from malicious attack.

IT Security Measures that Organisations Introduce – and their Failings

Vendors of IT security products – anti-virus, malware, spyware etc – can sometimes suggest that their products will, in a fully automated fashion, tackle all internal and external security threats. Also organisations often feel that heightened in-house IT security policies will protect them. However, the technologies intended to provide security ultimately depend on their effective implementation by people, thus

[1] G. Stoneburner, A. Goguen and A. Feringa: Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology, SP800-30

[2] OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security 2002

reinforcing the argument for modifying the behaviour of those people[3]. Organisations attempt to minimise security risks by applying very stringent IT security measures to internal networks, and by implementing seemingly exhaustive and highly organisation-specific security policies for employees; these policy measures, while effective, cannot of themselves wholly eradicate IT security threats. While it is extremely rare that employees intentionally set out to sabotage or endanger employers' networks and operations (such as in the case of a disgruntled worker), the IT security measures outlined above do not always ensure that well-meaning employees don't inadvertently compromise the security of their organisation through seemingly harmless actions. Just because extensive network security measures are in place, if a worker downloads software from an unauthorised source, or unwittingly hits a website that exposes their device to any number of threats – for example, viruses, Trojans etc. – their actions have the potential to take down the entire business' network.

There are many examples that highlight how it is impossible to create a completely secure environment through firewalls, anti-virus software, and prescriptive IT security policies alone; what is crucial is positively influencing the knowledge, general awareness, and behaviour of the user. By understanding and being able to identify the main concepts underlying the secure use of ICT in daily life, and by being aware of the necessary skills and knowledge needed to maintain a secure network connection and use the Internet, the user will then be able to protect their data – and that of their company – from being compromised, despite the rapid evolution of technologies used to perform breaches of security. One way of establishing good IT security practices for the individual, and by extension for the organisation, is by implementing recognised training programmes and certifications that benchmark the user's levels of skills and knowledge against an internationally recognised standard. Programmes such as the ECDL / ICDL Module 12 – IT Security have been designed with just this objective in mind. This module is a security-specific module intended for the end-user in a home or work environment; it is intended to influence a user's attitude, awareness and behaviour so that they become more security conscious, rather than being centred on the use of specific applications or software.

Additionally, concepts of security threats, privacy, and identity theft equally apply to the ever-growing sphere of social networking. Much media attention has been focused on the privacy of social networking sites – especially in relation to third-party access to personal data – so if a user is aware of vulnerability of their data, and the threats to it, they can more effectively protect it.

Conclusion

Ultimately, it is the actions of the human user that increase the level of exposure to IT

[3] The Impact of Information Security Awareness Training on Information Security Behaviour – Anthony Stephanou 2008

security breaches. Installing the most heightened automated security measures and prescriptive policies, whilst reducing the level of risk, is only a partial solution. To improve and maintain IT security both on an individual and organisational level, the awareness levels and behaviour of the user must be positively influenced so as to create what the OECD has referred to as a 'culture of security'. Skills and knowledge development programmes that are focused on the most important and current IT security threats are the best tools for achieving this aim.

About ECDL Foundation

ECDL Foundation's mission is to enable proficient use of ICT that empowers individuals, organisations and society, through the development, promotion and delivery of quality certification programmes throughout the world. Further information on ECDL Foundation is available at www.ecdl.org