PECB

When Recognition Matters

THE IMPORTANCE OF INFORMATION SECURITY NOWADAYS

Nowadays living without access to the information of interest at any time, any place through countless types of devices has become unimaginable. However, its security has become more important than information access itself. In fact today information security rules the world…! Why?

At the instant of waking up, the first thing that we do is check the phone while connecting it to the internet, looking for information, doing social networking, banking, shopping and lots of other online functions. We never switch off personal computers where sensitive data such as documents, personal photos, emails, conversations, important numbers and lots of other pieces of information are saved.

Then on the way to work still we are accompanied by smart phones all the way trying to stay connected, searching for wireless, so that our phones can become reachable for thousands of others who are using the same network. Then maybe we stop for breakfast, buy bus ticket, or pay for parking, all through the usage of our credit cards, which also contain important information for us.

Once arriving at the working places at different companies were despite our sensitive information that are saved there are also company's financial results, confidential business plans for years ahead, trade secrets, research and other information that gives company a competitive edge.

All these are made possible thanks to great improvements that occurred in the technology department on last decades. Yet, lately we hear less about innovations regarding stored, used, processed information electronically and transmitted than we hear about unauthorized access, cyber-attacks, hacking, violation of privacy etc. This phenomena is not at the level of individual cases, companies or businesses any more, these raising concerns and issues are causing problems and becoming relevant even on a state level; that of government, and international institutions.

The most heard concepts are: hacking, viruses, worms, Trojans, spoofing, sniffing, denial of services, spay, malware, mobile malware, cryptovirology etc. Their damage can be dreadful, by taking advantage of security gaps, attackers can gain access to a computer system without owner's awareness, making the computer

system not working properly, changing source/destination of IP address packet to show that it originates from a legitimate source, but in fact it might be coming from the hacker, who have access to all packets passed through wires of wireless network, this way bringing down the targeted network and denying the service for legitimate users etc.

To set-down these actions, information security officers during these years have developed systems to protect information, with concepts like: anti-virus, anti-spyware, software, Windows and applications updates, firewalls, content filtering/parental control, smart encryption codes and techniques, methods, and advices that can be found on information security.

As an assumption, this war between security professionals and attackers has advanced more and more, so at the same level that technology protects information security also jeopardizes. A fact that is totally understandable, because as much as the technology advancement is idealized, these advancements are done by humans and again the harm will be caused by humans themselves.

Managing Information Security

Protecting information or better say reassuring security is not just a technology issue anymore. Lately, vast importance is given to actions, plans, policies, awareness that companies, organizations or individuals take to protect information. It is said that “Information security is not an 'IT problem' anymore, it is a business issue.”

Entire management systems inside of organizations and business now are giving enormous attention to policies, proved objectives, self-hacking-audit, training and awareness activities.

Furthermore, compliance with legal and regulatory requirements for security and privacy has become an important factor to address information security. One of the main requirements toward this stands the assessment of risk and its evaluation.

Issues regarding information of customers and personnel, information security, and privacy actions have become one of the most important subjects. In order to show respect toward the customers and reach credibility on information security, customers have to feel certain that their information is guarded.

However, to incorporate these characteristics, rules, strategies and best practices in one management system is not an easy task at all, but there are lots of standards that have become a common language among information users. One of the most important is the International Organization of Standardization, which has a number of standards on how to manage Information Security.

The most prominent are: ISO/IEC 27001 Information Security Management System, ISO/IEC 15408 Evaluation Criteria for IT Security, ISO/IEC 13335IT Security Management for technical security control, ISO 29100 Privacy Framework, ISO 80001 Risk Management for IT-networks incorporating medical devices etc.

An enormous number of ISO standards, which are in charge of information security and more and more to come prove ones again the importance of this subject.

Conclusion

Information has become the most important asset that a person, organization or business needs, and its security is what makes us the best at what we do, that is why the Information Security will always be on the headlines.

Although, to achieve a high level of Information Security, an organization should ensure cooperation of all kind of levels including the use of information, which means incorporation of all parts inside and outside of the organization. In addition systems for information security should be part of continuing involvement on the highest level of organizational management in its design, plan and implementation. Therefore, information security compliances should become part of daily responsibilities, and certified personnel is more than needed.

Professional Evaluation and Certification Board (PECB) is a personnel certification body on a wide range of professional standards. It offers ISO 27001, ISO 29100 and ISO 20000 training and certification services for professionals wanting to support organizations on the implementation of these management systems. ISO Standards and Professional Trainings offered by PECB:

- Certified Lead Implementer (5 days)
- Certified Lead Auditor (5 days)
- Certified Foundation (2 days)
- ISO Introduction (1 day)

Lead Auditor, Lead Implementer and Master are certification schemes accredited by ANSI ISO/IEC 17024.

Rreze Halili is the Technology, Security and Continuity (TSC) Product Manager at PECB. She is in charge of developing and maintaining training courses related to TSC. If you have any questions, please do not hesitate to contact: tsc@pecb.com.

For further information, please visit http://pecb.com/site/renderPage?param=139