GUIDELINES TO CYBER SECURITY WITH ISO/IEC 27032
The importance of Cybersecurity

Considering the impact of security threats in our everyday life, cybersecurity becomes very important on its role. Maybe Cybersecurity is not needed if we consider that only physical threats might affect us by harming our body. However, we are all concerned about the information we have which is processed every day, and if we do not consider this as a very important fact, then this could lead to any sort of damage.

Information could be crucial for a person or a company. A healthy organization should align all the endeavors to contribute to minimal information theft incidents. Cybersecurity focuses on protecting computers, mobile devices, networks, applications, and data from unauthorized access. It is very important that all employees understand the importance of cybersecurity to ensure their protection, as well as the company where they work.

Organizations should implement a policy that emphasizes the awareness of cybersecurity to all employees, including the process instructing how to handle cyber attacks. We always have to remember the cost of an information theft, and this leads us to a prior plan on how to manage these situations. When we talk about information, we have to think about any important information that a company has and considers it as an asset. It can be a personal information, patent, information of its clients, information about the company strategy and objectives, trademarks, copyrights, etc.

There are lots of techniques used by hackers to obtain information or to prevent companies from offering services, which lead to disastrous impact on business. Many techniques involve gaining access to information people have on their devices like laptops, tablets and smartphones. This can be done in many ways, including phishing, DNS poisoning, Trojan horses, DDoS on cloud services. When asking people, they don’t even know they are using modified webpages which may embed malicious software specially crafted to aim our personal data.

This could be also linked to the Internet of things: on average, people usually carry three connected devices, which makes it easier for the hackers to get as much information as they can. Anything that could be found valuable for the hackers in these devices, not only personal data but also information about the office and the company that we work for.

Cybersecurity is about protecting all digital assets, which are in a simpler form: all information likely to be shared on the Internet.

Top three Cyber threats organizations have faced during 2015 are Social Engineering, Insider Threats, and Advanced Persistent Threat.

Due to a frequent number of cyber-attacks that companies have undergone, the International Organization for Standardization have developed an ISO/IEC 27032 standard that provides guidelines to cybersecurity, through which companies are advised to implement to ensure more secure information flow for the company.
How organizations can benefit from this standard?

ISO/IEC 27032 gives guidelines and explanations on how companies can fulfill the necessary criteria to ensure safer data processing. There are security issues that are not covered by current information security, network security and security application, as there are gaps between these domains as a result of the lack of communication between the organizations. This is the area of focus for this International Standard, to address Cyberspace security or Cybersecurity issues which concentrate on bridging the gaps between different security domains in Cyberspace.

Differences between ISO/IEC 27001 and ISO/IEC 27032 - The main difference between ISO/IEC 27032 and ISO/IEC 27001 is in its respective scope. ISO/IEC 27032 derives from and supports ISO/IEC 27001, which is related to the Information Security, not regarding the nature of the asset to protect; while ISO/IEC 27032 considers only digital assets, naturally included into information security assets. Moreover, ISO/IEC 27032 focuses on information system and includes guidelines to prevent information leakage, to encrypt communication channels and to make sure information will not be deciphered if accessed by “external” people (from the company).

According to a survey conducted in 2015 by ISACA, 46 percent of the respondents expected their organizations to face Cyber attack in 2015. In this survey, 86 percent declared that there was a global shortage of skilled cybersecurity professionals, and 38 percent felt prepared to fend off sophisticated attacks.

Cyber-attacks are costing businesses $400 to $500 billion a year, an amount which doesn’t include a large number of cyber-attacks which are not reported. As long as we face such a cost from information security incidents, there is a lot to be done. Companies have to invest more on Cybersecurity to minimize the cost of the security incidents that might happen.

According to this information, organizations should implement a strategy and recovery steps to follow in case they face activities that might lead to information security incidents. This is to ensure its cost reduction in managing information security, as well as having a healthy company.
Implementation of ISO/IEC 27032

An organization implementing ISO/IEC 27032 will make significant improvement of Cybersecurity, drawing out the unique aspects of that activity and its dependencies on other security domains, in particular:

- information security,
- network security,
- internet security, and
- critical information infrastructure protection (CIIP).

It covers the baseline security practices for stakeholders in the Cyberspace. This International Standard provides:

- an overview of Cybersecurity,
- an explanation of the relationship between Cybersecurity and other types of security,
- a definition of stakeholders and a description of their roles in Cybersecurity,
- guidance for addressing common Cybersecurity issues, and
- a framework to enable stakeholders to collaborate on resolving Cybersecurity issues.

This international standard also provides a framework for information sharing, coordination, and the process of incident handling.

In order to address the risk and threats of Cybercrimes, organizations should embed Cybersecurity as an integral part into their overall governance and risk management framework. Organizations need to ensure that the Cybersecurity is integrated as cross-functional with integration of all the following:

- Overall organization security
- Information security
- IT service continuity management
- Business continuity management
- Organizational processes
- Information protection approach

Here at PECB, we take cyber security very seriously, and in order to help professionals and companies worldwide be better prepared, we have embraced the ISO/IEC 27032 standard in our offerings. PECB is a certification body for persons, management systems, and products on a wide range of international standards. As a global provider of training, examination, audit, and certification services, PECB offers its expertise on multiple fields, including ISO/IEC 27032 Cybersecurity courses.

For further information, please visit: https://pecb.com/iso-iec-27032-lead-cybersecurity-manager-course

Author:

Gezim Zeneli is an Account Manager for Information Security at PECB. He is in charge of conducting market research while developing and providing information related to Information Security Standards. If you have any question, please do not hesitate to contact: marketing.sec@pecb.com.

Contributors:

Pierre Dewez, CEO at Altirian, Luxembourg
Dirk De Nijs, Founder and Senior Consultant at ModuleBuilder, Belgium
Eric Fourn, Virtualization Architect at Engineering Fabrics, France