

Cybersecurity as significant skill of every individual and business entity



Authors: Natasha Nikolaidou, Researcher and Dr. Jovana Milenkovic, R&D Manager, Atlantis Engineering S.A., Greece

Today's world moves in very high speed and things can change in the blink of an eye. For instance, take all the technological advancements that have occurred over the last decade.

Social media, cloud computing and artificial intelligence are just few that have come to affect our everyday lives. On the other hand, this fast-changing reality can become really frustrating for a great number of people who struggle to cope with all these challenges. The fact that an individual is asked to make use of innovative services and products, while being ignorant about the possible risks involved, makes them fall victims of fraudulent activity very often.

Furthermore, according to the European Union Agency for Cybersecurity¹, small and medium-sized enterprises (SMEs) are the backbone of EU's economy and they represent 99% of all businesses in the EU employing around 100 million people. Also, the SMEs account for more than half of Europe's GDP play a key role in adding value in all sectors of the EU economy. Despite this, small businesses do not usually have the best way to deal with cyber – threats (68% of SMEs have no systematic approach for ensuring cyber infrastructure) and therefore are soft targets for cyber criminals. Unfortunately, small businesses are usually dealing with lack of necessary resources, personnel as well as budget that can be invested to properly treat cyber-risks and to invest in information security the way larger businesses can. According to the statistics², 60% of all cyber-attacks or breaches happened at SMEs and 60% of the SMEs which were victims, did not recover and had to shut down within the sixth months.

What is Cybersecurity?

Cybersecurity is related to adopted and various actions and safety measures that are to defend information systems and to preserve the unauthorised users access and attack, ensuring the confidentiality, integrity and availability of data (Bettina Jakobsen[Member of European Court of Auditors] et al., 2019, p. 6, p. 57). Also, [Merriam-Webster online dictionary](#) defines cybersecurity as *measures taken to protect a computer or computer system against unauthorized access or attack*.

Why is it important for individuals?

Almost everything we do in our daily routine includes the use of the Internet, e.g., communication with friends through a variety of online applications, such as Viber, Instagram, Facebook, and so on. In most cases, scammers steal money getting easy access to one's bank accounts, credit cards or use personal information from social media accounts in order to use the identity and try taking

¹ <https://www.enisa.europa.eu/events/workshop-on-enisa-report-cybersecurity-for-smes-challenges-and-recommendations>

² <https://docs.broadcom.com/doc/istr-24-2019-en>

advantage of other people. What is more, especially since the emergence of Covid-19, the majority of people shop and work online. In all these instances, information is stored, processed and shared in a digital form. As a result, it seems of vital importance to protect our devices and our personal information from malicious attacks.

Why is it important for small businesses?

Desire for easy profit, revenge, thrill of causing mess, disclosing and accessing the SMEs valuable information are just few of the several reasons why cyber criminals select small business to attack. Thus, for small business, the overall effect of cyber-attacks can have tremendously high costs as they are often not prepared enough to handle such incidents³. Furthermore, what must be taken into consideration is the human error and human vulnerabilities, as aspects of internal threats, that result in some cyber breaches. Consequently, it would be good for employees of the small businesses to be trained on cybersecurity and get familiarized with cybersecurity methods.

Conclusion

In both cases, either an individual or a business, it is important to prevent cybercriminal and gain knowledge on Cybersecurity. It is of vital importance to protect both businesses and individuals, although it is not possible to be completely secure and be educated in the cybersecurity practices. Finally, it is in everybody's best interest to protect their private and sensitive information from theft, disclosure and misuse by implementing a strong information security program that can help balance security with the need and capabilities of a company or an individual.

³ NISTIR 7621 Revision 1, Small Business Information Security: The Fundamentals, National Institute of Standards and Technology 2016 (<https://doi.org/10.6028/NIST.IR.7621r1>)