# Cybersecurity: everybody's imperative

## The strategic role of Cybersecurity

Cyber Security has recently become of strategic importance and a principle concern among organizations, influencing not only technical staff but also CEOs and board members. This is a consequence of the unprecedented and rapid increase of high-profile attacks during the past few years causing significant disruption to operations and in extend having major adverse impact on the bottom line of organizations.

While attacks increase in volume and number, their complexity and sophistication increase as well. **A recent study[1] estimates that a Ransomware Attack, which is just one of many types of cyberattack vectors, is executed every 40 seconds and predicts that this will drop to 14 seconds in 2019**. From a financial point of view, the global Cyber Security market is expected to reach €100 billion in 2018, €170 billion by 2020 and that it will reach €800 billion cumulatively over the next five years[1]. On the other hand, it is estimated that the impact of cybercrime attacks will exceed the cost of €500 billion in 2018 for businesses[2], without considering the impact of the GDPR EU regulation for personal data protection, which can also bring huge consequences and fines in the undesirable event of a data breach. Moreover, **according to Cyber Security Ventures report, the total cost of cybercrime, is expected to exceed the $6 trillion dollars annually by 2021[1].**

Accordingly, it is vital for organizations to keep their systems as secure as possible. Cyber security aims to reduce the risk of cyber-attacks and to protect organizations and individuals from the unauthorized exploitation of systems, networks and technologies.

## How can we actually achieve effective Cyber Security?

In order to effectively reduce, mitigate and manage information security risks, a holistic, coherent and structured Cyber Security strategy that is applied on every side of the triangle People – Process – Technology is imperatively required.

Damian Saunders of Citrix Systems, in an article stated: "I take a contentious view and say that IT outages are rarely to do with technology," he said. "There's normally a role that technology plays in the outage, but when I look at the root cause, by far the greatest cause is people and processes."

Cyber Security is definitely not just technology. People are the primary targets of cybercriminals and they are frequently stricken via the execution of carefully targeted Social Engineering attacks. Thus everyone in an organization, from board members to IT personnel, should be aware of their role in preventing and reducing cyber threats, whether it's handling sensitive data, understanding how to spot phishing emails and in general know about the cyber security policy and procedures of the organization. As to the specialized technical staff that has the overall responsibility of cyber security in an organization, they need to be fully up to date with the latest skills and qualifications to ensure that appropriate controls, technologies and practices are implemented to fight the latest cyber threats.

Processes are also key to the implementation of an effective cyber security program. They are crucial in defining how the organization's activities, roles and documentation are used to mitigate the risks to the organization’s information. Processes also need to be continually reviewed as cyber threats change quickly and processes need to adapt with them. But again processes are nothing if people don’t follow them correctly.

Finally, technology, plays a vital role and is clearly an essential element of an effective Cyber Security Framework. Nowadays, while the threat landscape is expanding, protecting only the perimeter of the organization is definitely not enough. Cloud services, tele-workers, outsourcing and remote access necessitate the design and implementation of solutions that can provide the same, high level and intelligent protection for both on premise and off-premise access to systems and information.

The gradual and continual improvement of such controls is a crucial part of effective Cyber Security. Nowadays, safeguards who only focus on limiting the impact of potential Cyber Security incidents are not enough. Additional mechanisms should be designed and implemented to assist in prompt detection of such attacks, immediate response and eradication of the incident alongside with recovery controls to restore any capabilities or services that were affected by an attack.

**How does Logicom Solutions help organizations build an effective Cyber Security strategy?**

Building a successful security program today requires extremely talented professionals who can develop a cyber-security strategy and provide all the options to choose the right mix of services, technology and governance framework for building an effective program.

**At Logicom Solutions, we are committed to helping organizations plan, build and run successful cyber security programs**. Starting with value adding consulting services complemented by the right business and infrastructure solutions and relevant implementation services**, our experts and partners provide a comprehensive suite of products, services and solutions that enable businesses, governments and organizations to operate more securely in a world where everything is increasingly linked together**. From awareness sessions to full security assessments and governance frameworks, from technology installations to major architecture design and implementation, our unique approach, depth and breadth of offerings, and exceptional team help organizations operate securely in an increasingly digital world.

Logicom Solutions is a leading provider of total integrated IT solutions and business consulting services in Cyprus, Greece, Malta, UAE and the neighboring countries and a member of the Logicom Group of Companies with presence in over 25 countries.

1. https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf
2. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf