

87% of all businesses in Cyprus are exposed to cybersecurity threats

Recently, Microsoft alongside IDC conducted a [survey](#) regarding the security of technological systems in Central and East Europe. The results have shown that the majority of companies are insufficiently protected from cybersecurity threats or do not possess a complete security strategy. Furthermore, according to Eurostat, in 2019 87% of all companies in Cyprus with more than 10 employees did not have any protection against threats concerning their data or systems. These findings cause increasing concern regarding the security of valuable corporate data or users' data as cyberattacks are becoming a common phenomenon.

The most common type of cybersecurity threats that companies face can be found below and if companies do not create a strategic plan against them with the help of an expert these threats can be fatal.

- **Deface:** It is a malicious attack against a website or social profile in which attackers change the appearance of the website. These attacks are like some forms of vandalism and they mostly aim to protest against a policy or harm the reputation of a company.
- **Distributed Denial of Service – DDOS:** It is a kind of cyber attack in which the attacker seeks to make a machine or network unavailable to users by flooding it with requests by taking advantage of capacity limits of the infrastructure that host a service on the internet. According to [Kaspersky](#): *“The DDoS attack will send multiple requests to the attacked web resource – with the aim of exceeding the website’s capacity to handle multiple requests... and prevent the website from functioning correctly.”*
- **Ransomware:** These attacks are becoming increasingly common nowadays as hackers become smarter and more sophisticated. Hackers attempt to steal or lock files and data in order to ask for financial compensation to release the stolen data. Often, these hackers ask for vast amounts of money especially if they manage to steal valuable or sensitive information. If companies do not take preventive measures against such threats, solutions after the occurrence are very difficult to find.
- **Social engineering:** This category includes a broad range of attacks which are often including tricking users into revealing sensitive information in order to publish them or sell them. It is mostly achieved



with “phishing” in which users receive fake messages from familiar people or well-known brands and are encouraged to click a link that will harm their software or reveal some sensitive personal information.

Despite the increased risk that companies face from cyberattacks, many elaborated solutions can be implemented in order to prevent these malicious attacks. More importantly, the aforementioned survey conducted by Microsoft has demonstrated that most companies are intending to switch to cloud solutions within the next 2 years in order to enjoy all the security features that cloud systems can offer. In addition, companies are now giving much more attention in training employees to protect themselves against malicious attacks and gain more knowledge regarding the different kinds of threats.

IBSCY Ltd is an expert provider of IT services and products and has more than 15 years of experience in protecting companies against all kinds of threats. It possesses collaborations with all the major cybersecurity companies and its solutions’ architects can draft the best solution for your needs and requirements. Also, as one of the largest cloud services providers in Cyprus and the greater region, IBS experts can help you migrate your resources to the cloud and enjoy an abundance of features and benefits. For more information, please contact us on info@ibs.com.cy / +357 2525 4553.