WHAT IS CYBERSECURITY CULTURE AND WHY IS IT CRUCIAL FOR BUSINESSES?

By Olga Papadimitriou – Sales Administrator

Attacks by ransomware are among the worst cyberattacks for any business, causing significant losses. Ransomware attacks are growing, which is quite serious since hackers are difficult to stop. Research shows that cyber-attacks almost double every year with most of the firms experiencing several attacks. That indicates that businesses must improve their security. The adoption of iCloud technology, security skills shortages, and the "zero trust" theory are all contributing factors to the rise in cyberattacks. A significant influence is also played by digital transformation.

Hackers explore the systems. Governments or healthcare systems are not the targets of their internet scanning. All teams search continuously for little security gaps, and once someone clicks on the link, they succeed in getting access to the systems. For their own financial protection, firms must invest in cyber security. Worldwide, thousands of websites are hacked every day, with email accounts comprising almost half of intrusions. Therefore, the need for the adoption of a cybersecurity culture is crucial.

But what exactly is cybersecurity culture, and why is it crucial?

The phrase "cyber security culture" relates to an organization's workforce's attitudes, knowledge, presumptions, conventions, and values toward cyber security. These are influenced by the organization's objectives, organizational structure, guiding principles, and leadership. By encouraging a cybersecurity culture, employers may be confident that staff members are aware of potential hazards and know how to handle or report them.

Beyond the antivirus software and firewalls a firm invests in, perceptions of cybersecurity are increasingly important in defending a corporation and its digital assets. Identifying social needs, or the expectations we have for the human capital of the organizations, is a crucial component. You must comprehend the workers, their needs, their challenges, and any issues they could be having at work or even at home.

Another crucial factor is privacy confidentiality. As sensitive information is frequently gathered by third parties without even being considered hacked by the user who obtained it. Physical and mental health have a significant influence on privacy too. Security, privacy, resiliency, ethics, honesty, and openness are all crucial components of digital trust. Thus, employers are increasingly

seeking candidates with soft skills. By obtaining such employees, they will be better able to reduce the danger of cyberattacks on their clients' and customers' companies.

It's important to understand how significant the risk from cyberattacks is. There is a great need for skilled personnel with soft skills in businesses. Organizations are seeking someone who can think critically, communicate effectively, and pay attention to detail. Government, security, information technology, and risk compliance are all impacted by digital trust. Equally important is maintaining the trust of consumers and clients.

In conclusion, Cybersecurity is a never-ending race for businesses and individuals. Cyberattacks are becoming more frequent worldwide as hackers use AI and other cutting-edge technology. We must understand that cybersecurity is not a technological challenge but rather a business one. Therefore, it must be a top priority for organizations to properly defend themselves from malicious attacks. Having an IT department or not, if you are planning to update or establish a new cybersecurity strategy for your business, the IT experts of IBSCY can help you by offering Technology Audit services and IT Solutions in Cyprus and abroad.