Cyber ​​Awareness and Cyber ​​Subculture for All

Although Security Awareness is foreseen as cyber security training for employees today, it is actually a subject that needs to be evaluated in a broader context. Cyber ​​Security employees have to receive constantly updated training on cyber security attacks and defense ways, with the training they will receive.

policies against various phishing and ransomware attacks, the procedures applied in the event of an attack, and the scope of training received should have content and curriculum that should be constantly updated and renewed. It is not a matter that can be limited to the fact that only cyber security employees receive this training and awareness, companies and other employees feel safe in the corporate sense. Because, in the basic sense, the concepts and practices of cyber security should be adopted and subcultured by both company managers and non-cyber security employees at a minimum level.

Repetition and comprehensive updating of security trainings to cyber security workers; Raising awareness on those other than cyber security employees will make a significant contribution to the stimulation of social cyber security culture and awareness.

The main target of the phishing attacks, which are changing and developing day by day, are the mistakes and unconscious actions of the employees other than cyber security, and the company managers who see the investment in cyber security as unnecessary as a waste of time and financial loss.

The way of working and the use of technology in companies bring many cyber attacks.

Considering the great losses arising from simple mistakes such as sharing personal information by falling victim to the personalized and complex methods of the attacks, the biggest target audience is employees and managers other than technical personnel (excluding cyber security employees who are tasked with fighting the attack).

Therefore, trained employees are the front line in protecting all personnel and the company against phishing.

It is the formation of the same consciousness, consciousness and awareness in all members of the company from head to toe for "total quality management (TQM)," which means meeting the human, business, product and/or service quality requirements used to meet customer needs, with a systematic approach and with the contributions of all employees.

Employees and managers who are misinformed about cyber security, who do not know what to do against risks or attacks, can unconsciously endanger the rest of the company. With the outbreak of the COVID-19, which is a global crisis, we have seen that the behaviors that we thought to be harmless until now, the insignificant mistakes we make can cause serious losses.

Many companies that want to be protected from attacks feel the need to invest in cyber security awareness trainings every day to raise awareness of both their employees and managers. Therefore, there will be a serious growth in the cyber security education market. According to a study, it is estimated that the cyber security market will reach a volume of 10 billion dollars in 2027. If these expenditures and investments are not made, it is very difficult to estimate the extent of the damage.

But the numbers tell a different story when we talk about cybercrime. Damages related to cybercrime are expected to reach $6 trillion in 2021 alone. With the rise of remote work due to the COVID-19 pandemic, it is also a fact that companies are more targeted by hackers than ever before.[[1]](#footnote-1)

Ninety percent of companies have faced an increase in cyberattacks due to the pandemic, according to a survey conducted in June 2020. More worryingly, 93% of these companies said they had to delay security projects to help manage their company's transition to remote work.

In many countries, most notably the UK, a large proportion of companies continue to lack personnel with the technical skills, risk-suspicious incident response skills, and the governance skills needed to manage their cybersecurity.

Nearly 680,000 businesses (50%) have a basic skills gap. In other words, those responsible for cybersecurity in these businesses lack the confidence to perform the kind of core tasks set out in the government-approved Cyber ​​Basics.

In the same survey, it was seen in qualitative interviews conducted at these companies that cybersecurity skills were not sufficiently understood and given enough importance among both the boards of directors and IT teams. Therefore, it is crucial for cyber leaders to have the skills to influence behavior and culture in their organization and to discuss cybersecurity in terms of business risk with senior executives.[[2]](#footnote-2)

Unless everyone in the company, from senior employees to new hires, has the same level of cybersecurity awareness, security is unlikely to be achieved unless they strive with the same determination to prevent phishing attacks.

Therefore, in today's world where the threats we face are diversified and different phishing attacks are planned, each individual has a responsibility to ensure cyber security, and this responsibility is increasing day by day as the variety and risk of attack increases.

1. <https://www.talentlms.com/blog/cybersecurity-statistics-survey/> last visited on 28 March 2022 [↑](#footnote-ref-1)
2. <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1042429/Cyber_skills_in_the_labour_market_report_v6_.pdf> last visited on 29 March 2022 [↑](#footnote-ref-2)