ELEARNINGNEWS ARTICLE

Year 6 - number 212 Wednesday 20 july 2022

Cyber attacks: what impact on workers' health and safety?

The European Agency for Safety and Health at Work looks at cyber security in relation to the impact on workers when assessing cyber risks.

The European Agency for Safety and Health at Work (EU-OSHA) studies, among other factors, the consequences of digitisation on occupational health and safety in order to provide European decision makers, employers and social partners with the necessary information on emerging challenges in this field.

The global costs of **cybersecurity** will reach USD 10,500 billion by 2025. The problem is not limited to losses due to data theft; there are, in fact, new **emerging risks** to workers' health and safety. But what is the impact of cyber security on workers?

According to the report '**Incorporating occupational safety and health into the assessment of cybersecurity risks**' by Isabella Corradini (Scientific director of Themis Research Center), every company (regardless of sector) is at risk of cyber attack, especially after the rapid digital evolution brought by 2020. In fact, since 2020, 78 per cent of organisations have experienced increases in the volume of cyber attacks due to the shift to remote working. Moreover, cybercrime is becoming increasingly sophisticated and cybercriminals are exploiting all types of vulnerabilities for their attacks.

The impact of cyber attacks on security

Cyber attacks do not only have a technological or economic component: the human factor and the safety of workers are important parts of the issue.

In fact, cyber attacks can cause injuries (even serious or very serious, up to loss of life) and psychological problems (anxiety, frustration). For this reason, **cyber risk assessment** and health and safety risk assessment must be carried out together.

Here are the possible consequences of a cyber attack, at organisational, human and environmental level.

Some examples?

- A cyber attack in a German steel mill in 2014 managed to shut down the furnace with the risk of creating a critical worker safety event;
- In 2017 in the US, the Food and Drug Administration (FDA) recalled 465,000 pacemakers due to security vulnerabilities to possible cyber attacks;
- In Iran, a cyber attack targeted the control of centrifuges used for uranium enrichment.

Not to mention that hacker attacks targeting equipment with wireless signals can create problems controlling vehicles or machinery.

The social and psychological impact of cyber attacks

Cyber attacks can have social consequences (such as loss of trust in digital technology), but also psychological consequences (anxiety, anger and depression).
Depending on the context, workers affected by cyber-attacks may feel a very or even too high burden of guilt, confusion or frustration to handle; think of the case of digital information leakage in a bank.

In fact, research on '**cyber crime victimisation**' points to negative experiences for both companies and individuals. Unsurprisingly, when organisations suffer ransomware attacks, the teams involved suffer damage to professional trust in the company itself.

Human error (opening phishing e-mails or mishandling passwords) is considered the **root cause of 90 per cent of computer security breaches** and can expose organisations to serious consequences, such as the installation of malicious software in the corporate network.

In order to train workers (all those who use computer systems in their work) to prevent cyber attacks from a human perspective, the online course " **Cyber Security - Protecting Company Data and Information**" lasting 1 hour is a very valuable tool.

With regard to human errors, it is very important to consider the psychological factors involved in cybersecurity incidents:

- 52% of workers are more likely to make mistakes when they are stressed,
- 43% when they are tired,
- 26% when they feel exhausted (stress or burnout).

Translated with www.DeepL.com/Translator