# "There is a need to provide a comprehensive defence solution"

Eyal Weintraub, Founder C.E.O. of Presale1: "There is a need to provide a comprehensive defence solution that combines the three dimensions - human, physical and cyber, with a focus on preventing commercial espionage."

This article is available also in the Hebrew and French language - click here

Original article was published on "The People and Computers" "Daily Maily" Link to article - click here
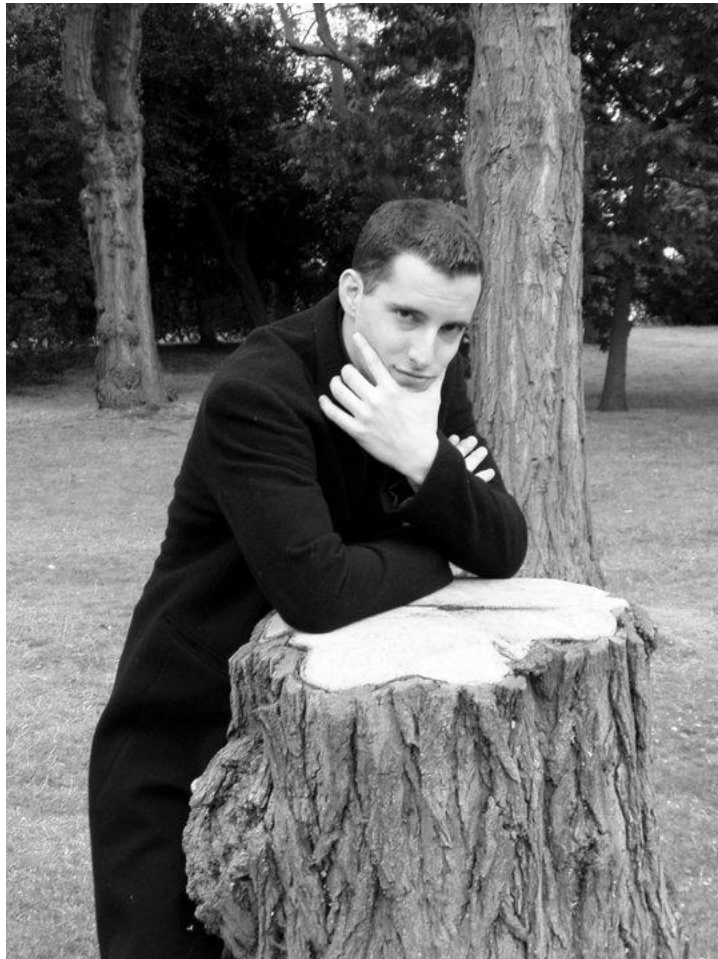
Cyber threats have become multidimensional. Attackers no longer operate with tables, but rather with graphs. While in the past, attackers exploited different types of attacks, such as distributed denial of service, known as DDoS, SQL injection or 'executive fraud' (BEC – Business Email Compromise), in recent years most attackers have become multidimensional experts – exploiting, Eyal Weintraub , CEO and founder of Presale1, an international information security and cyber project management group, said.

According to Eyal Weintraub, "organisations don't pay enough attention to the human dimension of the threat, - malicious or inadvertent. This threat can come from maintenance staff, IT staff - whether they are disgruntled employees or those who plan to leave the company with a lot of confidential information to set up their own business. To do this, they can exploit loopholes in access privileges that traditional security technologies will not detect."

Another dimension, highlighted by Eyal Weintraub, "is the physical security of information. That is, getting into places that contain sensitive information by exploiting weaknesses in access control systems of all kinds, from video surveillance to code-based access control systems, biometrics, etc."

The third dimension that needs to be addressed, he added, "is in relatively new areas, such as attacks based on the use of cheap and accessible IT tools for online purchase. These do not require extensive resources and technical expertise.

The fourth dimension, he noted, "relates to the lack of alignment between the structure of the organisation, physical security - which is the responsibility of the

security officer, and information security - which is the responsibility of the information security officer.

There is a need to provide a comprehensive defence solution, which combines the three dimensions - human, physical and cyber, with an emphasis on preventing business intelligence.

"Under my leadership," he said, "the company allows organisations to focus on their core business - while we provide tailored information security solutions that integrate seamlessly and efficiently into the enterprise. We work with our clients to find the most appropriate and advanced security solutions from dozens of security vendors - local and international, in a variety of areas - XDR, mobile protection, secure development processes, password management, access control. We manage security projects that protect our clients' data, from the Proof Of Concept (PoC) phase, through implementation and into operation, with our 24-hour support. For example, Presale1's advisors have successfully worked with enterprise customers in planning complex security infrastructures, sophisticated penetration testing and solution development, including those that include integrated technologies, security architectures and complex topologies.

One of Presale1's consultant said: "As a security consultant and expert, I work for a close connection between the three dimensions - human, physical and cyber. The CISO and the security director must work together, otherwise security holes will be created and the organisation will fall through the cracks." Recently , "I participated in an international conference on cyber defence held in the La Défense district of Paris, and organised by the France-Israel Chamber of Commerce, with the participation of hundreds of cyber defence experts and dozens of companies in the field. During the conference, I spoke about the difference between economic intelligence and cyber defence. We also presented the Cyfox XDR solution, which combines ten security engines for maximum protection. In order to effectively minimise cyber risks", the two men concluded, "multi-layered cyber risk management must be conducted in three dimensions. A traditional one-dimensional solution is not enough.