Digitalisation

- What is a 'fully digital enterprise'?

A digital enterprise is an organization that uses technology as a competitive advantage in its internal and external operations.

As information technology (IT) has reshaped the infrastructure and operations of enterprises, the digital enterprise evolved to represent businesses that have completed a digital transformation or digitalization to embed digital solutions across the enterprise.

Examples include business processes, products and business models that incorporate digital strategy and digital transformation to compete more effectively in the market.

- What are the cyber Security challenges?

Ransomware

Ransomware is another tactic used by hackers. The objective is to hold a company's data hostage until the affected user pays a specific dollar amount, which can often be hefty. These attacks can use email to penetrate a system, but can also be initiated by visiting an infected website, clicking on an online ad with malicious code, or hackers exploiting network vulnerabilities. Prevention requires a combination of training employees to exercise judicious caution regarding the websites they visit, and remaining diligent in identifying and fixing system vulnerabilities.

Cloud computing issues

The amount of valuable information that resides on multiple data sources has grown exponentially from the early days of computing. The opportunity for organizations of all sizes to have their data compromised grows as the number of devices that store confidential data increases. Cloud storage and the Internet of Things (IoT) have exposed new vulnerabilities. Organizations and businesses must make security plans that take new security threats into consideration, rather than only protecting business computers and mobile devices.

Distributed denial-of-service (DDoS)

The hallmark of these attacks is coordination. A cyber attacker floods the system with a high number of simultaneous functions, such as a request to

a webpage. The goal is to overwhelm networks, systems, or devices. This can ultimately expose vulnerabilities that cyber attackers can exploit. Like other forms of cyber attacks, this method's sophistication has increased as technology has evolved, making it vital for organizations to be aware of the latest innovations to protect against these types of cybersecurity issues.

Artificial intelligence (AI) and machine learning (ML)

In the hands of cyber criminals, artificial intelligence (AI) and machine learning can enable cyber attacks to become more sophisticated and efficient. Both can "learn" which attack methods work and which do not, making them valuable tools for criminals. Fortunately for savvy cybersecurity professionals, AI and machine learning can also be deployed to combat cyber attacks.

Crypto and blockchain attacks

The use of cryptocurrencies and blockchain technology in business continues to increase. According to a report by Allied Market Research, the global cryptocurrency industry (hardware, software, platforms, and services) is projected to reach nearly $5 billion by 2030. This digital form of monetary exchange has become fertile ground for cyber attackers, as the infrastructure needed to safeguard the information associated with these assets has been slow to develop. Those looking to use blockchain in their businesses should take great care to make sure their cybersecurity strategies include protection for these emerging, evolving markets.

Sources:

- Allied Market Research, "Cryptocurrency Market Size, Share and Analysis | Forecast – 2030"
- CSO, "DDoS Explained: How Distributed Denial of Service Attacks Are Evolving"
- Digital Guardian, "Social Engineering Attacks: Common Techniques & How to Prevent an Attack"
- Entech, "Anatomy of a Data Breach, What We Learned from Target"

I agree with the thoughts and the views expressed about the energy crisis.