SMEs are the weakest link in supply chain cybersecurity

Small to medium enterprises are at greatest risk from cybersecurity threats, and their vulnerability in turn poses a danger to the major corporations that they do business with.

Steven A. Melnyk speaking at the Sapics Spring Conference

This is the contention of Steven A. Melnyk, Professor of Supply Chain Management at Michigan State University in the United States, who recently shared his insights with South African supply chain professionals at the inaugural Sapics Spring Conference. This event was hosted by Sapics, The Professional Body for Supply Chain Management.

Said Melnyk:

> *"Blockchain is vastly overrated; supply chain cybersecurity is underrated; and we are not spending enough time on small to medium enterprises. We need to growthem; but they are a challenge in terms of cybersecurity."*
>
> "The problem with small to medium sized enterprises is that they are in the unique position of having disproportionate access to important information. They are often mission critical suppliers that produce niche products. They are protected by governmental regulations and requirements. However, they generally have the weakest cybersecurity arrangements in terms of size, resources and expertise. They open up large clients to leapfrog cybersecurity attacks."

Melnyk cited the example of a well-respected American chemical company that was hacked through its supply chain. The hackers obtained information about customers and orders, including quotes. They saw details of items that the company – which was renowned for innovation – was getting ready to patent, he revealed. "The hackers altered the master production schedule; they changed due dates, order quantities and order quality levels. Deliveries were compromised. A new supplier then entered the market, with the precise items that the customers wanted, at prices under the current variable costs. This supplier also patented the firm's innovations."

General Electric suffered a cybersecurity breach in which hackers got the business's target prices, while Macey's and the Bank of America have also been targeted. "Every significant breach has occurred through the supply chain," Melnyk told Sapics Spring Conference delegates. He said that 69% of firms have experienced an attempted cybersecurity breach or incurred a significant loss of data as a result of one. "Companies spend an estimated $84-billion to defend against breaches that cost them about $2-trillion. The average cost of a cyber breach is $7.9-million and the average time to contain a breach is 276 days."

The growth of the digital economy and digital supply chain is contributing to the growing cybersecurity threat, with four billion people predicted to be connected to the internet daily in 2020.

Melnyk said that companies must consider the threat of collateral damage when assessing their cybersecurity risk. "In June 2017, Russia launched the 'NotPetya' attack against Ukraine. Its targets were banks, energy providers, governments, airports and hospitals, and its goal was to wipe data from computers. Companies including Merck, FedEx, Maersk and Mondelez suffered significant collateral damage," he revealed. The attack cost pharmaceutical company Merck $870-million, incurred as a result of collateral damage through its connection to hospitals. Melnyk says that Maersk was reportedly so ill-prepared for the threat that the firm's IT people were running down corridors telling employees not to turn on their computers.

He urged supply chain professionals to consider cybersecurity prevention, detection and recovery measures, and to understand how contamination might occur. "It is time to act now. Cybersecurity is not an IT issue, it is a supply chain issue. Cyber attacks are on the rise."

Melnyk said that the current global cost of ransomware damages is more than $5-billion, and by 2021, it will exceed $6-trillion. "Blockchain offers some protection, but it is not enough. If you want to develop a competitive edge in South Africa, offer your customers secure supply chains," he concluded.