Circumference Technology Services

Cyber Security as a Competitive Advantage

EXECUTIVE SUMMARY:

Cyber Security as a Competitive Advantage

A Circumference Executive Sessions meet-up,

First Aid Training Centre

1580 Merivale Road, #506

Ottawa, ON K2G 4B5

May 3, 2018

FEATURED SPEAKERS:

Gavin McLintock, CISSP, PCIP, P.Eng

"Leveraging data security to create competitive advantage in a world of virtual risk and vulnerability."

Andrew Johnston, BSc Computer Engineering

"Interactive training as a key strategy to defeat malicious social engineering."

Cyber Security as a Competitive Advantage

On 3 May 2018, corporate executives gathered in Ottawa to discuss the impacts of cyber security on Industry 4.0. In days gone by, companies tended to equate cyber attacks with temporary shutdowns. They calculated cyber security budgets based on what it would cost to fix “broken” systems, reasoning that it is less expensive to mop up a hacker’s “mess” if their company was ever attacked. These corporate leaders, according to those who gathered, are in a for rude awakening if they persist with this assumption.

Mounting Costs of Inaction

Today, the question is not if your company will be attacked, it’s when you’ll be attacked. Ever-increasing connectivity creates new vulnerabilities that must be carefully managed. One event participant, for example, mentioned an occasion when a casino was hacked via a wifi-enabled aquarium thermometer. Often, many months elapse before companies are even aware that they were hacked. Large companies are typically hacked via backdoors inadvertently created by smaller, less secure companies in their value chains.

These types of vulnerabilities are becoming less and less acceptable. The recent Facebook fiasco highlights growing intolerance for privacy breaches. One of the gathering’s participants quoted a statistic claiming that 80% of small businesses which experienced a breach were out of business within 2 years. In addition to consumer culture shifts, Government General Data Protection Regulation (GDPR) legislation is about to significantly increase the costs of being hacked by forcing companies to publicly report these events.

Solutions

As a result, supply and value chain leaders are setting new standards when evaluating potential new suppliers. Bidders, who have been working with ISO standards for decades need to aggressively embrace these new cyber compliance requirements. Corporations seeking to meet or exceed these standards need to proactively and regularly conduct risk assessments of connected systems and personnel roles by pursuing multiple strategies:

> Isolating vulnerable systems is obviously important. Factories often isolate their plant networks from the internet to improve their security. Some workplaces are taking additional novel steps, like hardening the receptionist role so that it is not possible to reach into an organization without knowledge of and/or relationship with the employee that the customer is trying to reach.

> Training, our event attendees also agreed, is integral to maintaining secure corporate systems. One event participant, for example, shared that their company provides extra training for customer-facing employees who have to work within additional layers of security. These employees, the speaker added, must regularly prove their competence in this area. To build and maintain these core competencies, companies must educate and even incentivise training.

Cyber Security as Market Differentiator

Maintaining these security levels does not come cheap, yet creative corporate leaders are finding creative ways to mitigate these costs. By pre-emptively upgrading their facilities to anticipate or exceed their supply chain's standards, and then advertising these achievements, companies are turning these security investments into competitive advantages. Companies that commission Service Organization Control (SOC) reports, for example, often post the less sensitive SOC3s to their websites to differentiate themselves from their competition. Achieving NIST 800-53 standards can also be marketed to serve the same purpose. In some industries, these standards are already commonplace; in others, standards are still being established.

Conclusion

Regardless of their markets, everyone at the event agreed, the gradual introduction of an Industrial Internet of Things (IIoT) to supply chains will create new security requirements. Corporations seeking to enter or expand their share of supply chains will do well to push ahead of the curve by adopting strong cyber security systems and practices so that they can market themselves as the most reliable available bidders.