Daubenspeck and Associates
180 N. Stetson Avenue • Suite 1935
Chicago, IL 60601
(312) 297 4100

www.daubenspeck.com

Cybersecurity and the Internet of Things:

Section Five - Securing IoT to Maximize Value

FEBRUARY 5, 2018

By: Ken Daubenspeck

The vulnerabilities created by the current internet of things will not stop its market growth. Accenture predicts that by 2030 the industrial internet of things will add $14.2 trillion to the global economy, and the German government's "Industry 4.0" concept reflects the belief that IIoT's emergence will drive changes in manufacturing that constitute a fourth industrial revolution. This belief has been widely accepted by industry and other governments. The opportunities to create added-value through IoT are paradigmatic in scale, and the increased integration of IoT into the economy is an inevitability.

With this in mind, IoT cybersecurity practices should be seen as value-generating operations. In today's cyber-ecosystem, when any number of firms utilize common IoT platforms and devices, the competitive advantage will go to the firm that is best able to reduce disruption from cyber-attack. The ability to manage threats is going to be a major determinant of a firm's ability to employ IoT efficiently.

Effective threat management requires businesses to maintain an inventory of all the devices connected to their network, and to exert strict control over what devices are allowed to connect in the first place.

> *"The potential for major attacks on cyber-infrastructure makes operational **resilience** an integral part of any effective security policy."*

Devices that are allowed to connect should be segregated from the rest of the network in order to reduce the damage of a potential compromise. A firm's specific security needs will also vary depending on the processes that need to be secured—sector-specific guidelines, such as the Industrial Internet Consortium Industrial Security Framework, should be utilized where applicable.

The potential for major attacks on cyber-infrastructure makes operational resilience an integral part of any effective security policy. Not all disruptions can be prevented, particularly if the attack is on a third-party service or involves a previously undiscovered vulnerability. A business continuity plan that outlines how to react-to and recover-from various types of attacks can mitigate their overall damage. For instance, firms can limit the damages caused by a disrupted third-party service provider by pre-arranging to use a backup service.

IoT vulnerabilities are an “environmental” threat that permeates the entire cyber-ecosystem. Worldwide, firms’ networked processes are all embedded within the same unrelenting storm of malicious activity. The most competitive users of IoT will therefore be those that can operate within that storm more efficiently than their peers. Operational resilience and security are not simply matters of risk-aversion, they are the key to leveraging IoT technology as a means to effectively create value.

About Daubenspeck and Associates

Ken Daubenspeck is the founder and President of Daubenspeck and Associates: an international recruiting firm. Daubenspeck specializes in the recruitment of the CIO, CISO, and the building of their capabilities.

The firm is also known for their extensive work in cross-border expatriate executive appointments in financial services, petroleum industry, and higher education.

CONNECT:

https://www.linkedin.com/company/daubenspeck-&-associates-ltd./

https://twitter.com/DaubenSearch