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 Four - The Future of the Internet of Things

JANUARY 29, 2018
By: Ken Daubenspeck

Over the next decade, the internet of things will increasingly permeate all aspects of society. Cities such as Barcelona and Amsterdam have already begun to integrate IoT into civil infrastructure, and more dramatically, Alphabet (Google's parent company) is planning to redevelop 800 acres of Toronto's waterfront into a hyperconnected "smart district". This latter project provides a foundation for a precipitous increase in IoT-integrated services, including self-driving vehicles, data-driven health and community services, responsive transportation management, automated freight transport, and sensors for community-wide data collection.

These civic initiatives illustrate the extent to which IoT brings cybersecurity issues into the physical world. The birth of IoT marks the death of the divide between physical security and cybersecurity—the disruption of an IoT device could affect the physical environment associated with the device, potentially posing a security risk (e.g. if a device controls room access) or a safety risk (e.g. if a device controls machinery). These dangers are particularly relevant for firms that combine IoT devices with machinery controlled by operational technology (OT). OT has traditionally had no need for cybersecurity, and is thus more likely to lack protection against attack.

"The birth of IoT marks the death of the divide between physical security and cybersecurity."

In the context of the transformations outlined above, today's IoT landscape poses a major problem for the future. The low replacement rate of many connected devices (e.g. CCTV systems) makes it likely that current low-security hardware will remain in use for years. As IoT becomes integrated into every part of the economy, the potential damage from the presence of a single vulnerable device within a supply chain will rise sharply.

Further, as IoT service provision consolidates around a few major vendors, there is a risk that attacks on these vendors will result in catastrophic damages. For instance, services such as Microsoft Azure and Amazon Web Services (AWS) are becoming vital to industrial IoT platforms. Should they be successfully attacked, firms without contingency plans could face severe operational disruption.

These systemically important vendors are usually well-secured; however, AWS has already been disrupted by Mirai's attack on its DNS server—a successful attack against a key service remains an active possibility. Cisco analysts even believe that current botnets could be laying the groundwork for an attack powerful enough to disrupt the internet itself. This may be why Sam George, Microsoft's Director of Engineering for Azure IoT, is among those advocating for IoT security regulation.

These risks are further compounded by ongoing advances in cybercrime technology, such as malware that utilizes artificial intelligence programming to spread more efficiently and hide from cybersecurity. For instance, the Hajime botnet, which has infected over 300,000 devices, can analyze a network's traffic patterns to learn how to mimic human behaviour. With this increased sophistication also comes an increased ability to inflict damage—the Brickerbot botnet spreads similarly to Mirai, but uses permanent denial of service (PDoS) attacks to "destroy" infected devices by corrupting their storage. Cisco predicts that new IoT malware will start to employ "destruction of service" (DeoS) attacks that eliminate a target's ability to restore their systems and data, limiting their ability to recover from attacks.

Clearly, the current level of vulnerability in the IoT market does not scale well with the future. As the economy's operational integration with IoT increases, most business processes will come to require end-to-end cyber-protection. In this high threat environment, a firm's ability to maximize the value of its IoT devices will depend on its ability to avoid preventable disruptions and efficiently recover from unavoidable ones.