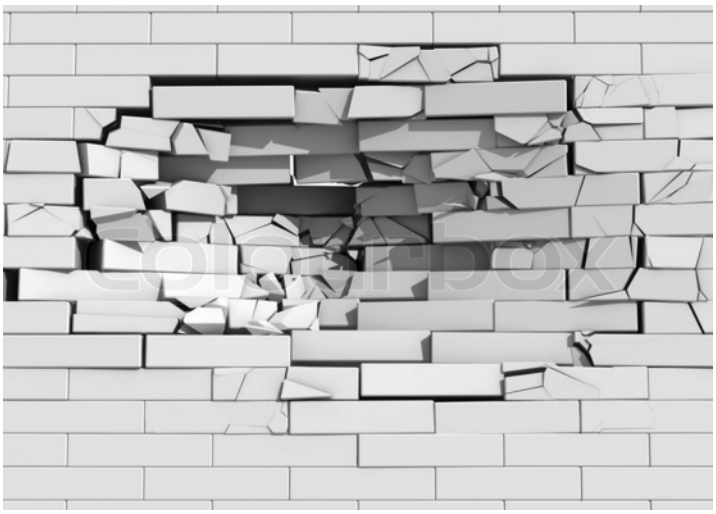
Daubenspeck and Associates
180 N. Stetson Avenue • Suite 1935
Chicago, IL 60601
(312) 297 4100

www.daubenspeck.com

Cybersecurity and the Internet of Things:

Section Two - Tracking the Growth of an Insecure Industry

JANUARY 15, 2017
By: Ken Daubenspeck



In its aftermath, cybersecurity pioneer John McAfee called the Mirai botnet attack a precursor to a "cyber atomic bomb"—a hypothetical malware powerful enough to do significant, permanent damage to major economic processes by disrupting cyber infrastructure and any physical operations that infrastructure may control.

The high threat potential that McAfee describes is the result of the immature internet of things (IoT) industry being actively exploited by the far more mature cybercrime industry. IoT technology only became mass market in 2014, the year that the Industrial Internet Consortium was founded by Cisco, GE, AT&T, Intel, and IBM, and the Consumer Electronics Show featured IoT as its main theme.

The advent of cloud computing and big data were the two technological shifts that allowed the IoT market to transition from niche to powerhouse. The rise of cloud services meant that connected devices didn't need data storage or processing capabilities, and big data analytics made that data more valuable. The combination of these technologies created new opportunities for firms to generate value and drive productivity, and the IoT market has grown rapidly ever since.

"The advent of cloud computing and big data were the two technological shifts that allowed the IoT market to transition from niche to powerhouse."

Garner estimates that over 8.4 billion connected things exist in the market today (31% year-over-year), 3.1 billion of which are used by business. Business spending on IoT products and services currently stands at $964 billion, and will top $1.4 trillion in 2020.

Unfortunately, the industry's development has occurred in a patchwork manner. The foundation of the internet of things is an array of products that were developed to cater to specific verticals, without concern for interoperability or common security standards. Unlike computers, IoT devices are typically built to have limited user input, especially if their functionality centres around automated processes or machine-to-machine (M2M) communication. A lack of user interaction makes it less likely that the user will detect abnormal behaviour, which reduces market incentives for vendors to address vulnerabilities.

This fragmented development path helped to create a situation where, in their rush to market, product developers frequently ignored preventable security issues in order to reduce costs and development time. The result, according to Malwarebytes analyst Chris Boyd, is that many IoT devices are "horribly broken" in security terms. As firms add more devices to their network, they face increased risks that this broken security will become a problem.

In 2014, a Symantec employee referred to the internet of things as the "Internet of Vulnerabilities", remarking "companies are pushing forward quickly, trying to establish a market… hardware and software will flood the market with no thought to security." He was right. IoT's development path turned it into an ecosystem of vulnerabilities, the massive cybercrime shadow economy turned those vulnerabilities into a goldmine, and the creation of destructive botnets such as Mirai became an inevitability.