IIoT Security Risk Mitigation in the Industry 4.0 Era

Convenience can sometimes come at a price. If there's one thing all technological analysts agree with, it's that the Internet of Things (IoT) will continue to gain traction and that decisions made in the space will have ripple effects across enterprises in the Industry 4.0 era.[1] Manufacturers of IoT technologies, including endpoint and network security software and platform middleware, will come and go. Paranoia regarding IoT and security will carry over from 2017, as around a third of IT leaders cited security as a barrier to IoT's success.

> **32%** of IT leaders cite security as a top barrier to IoT's success.
> —*Gartner's 2016 IoT Backbone Survey*

The Current State of IIoT Use in the Industry 4.0 Era

By 2020, the global spending on IoT is forecast to reach US$457 billion at a compound annual growth rate (CAGR) of 28.5 percent.[2] The majority of enterprises that currently adopting IoT use metrics and key performance indicators that reflect operational improvement, customer experience, logistics, and supply chain gains.

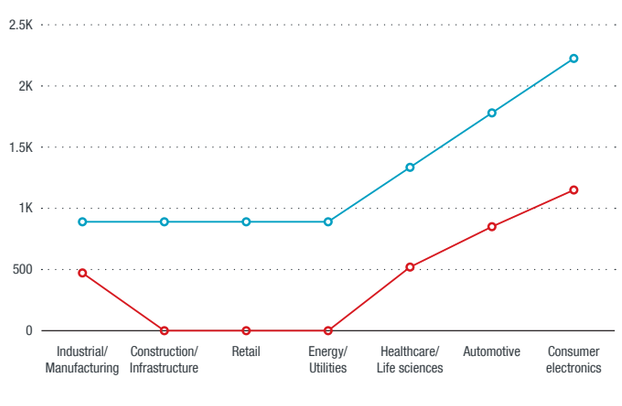

Figure 1: Size of the global IoT market, 2014 versus 2020, by industry (in US$B; https://www.statista.com/statistics/512673/worldwide-internet-of-things-market/)

In the enterprise space, industrial IoT (IIoT)—the way by which companies use big data and IoT to lower costs and speed up processes—is also gaining momentum. IoT allows disparate machines (robots, machine sensors, devices, etc.) to communicate using data, allowing managers to predict faults before they occur.

Discrete manufacturing (automotive, aerospace, etc.), transportation and logistics (railway, etc.), and utilities (electricity, oil and gas, etc.) are just a few of the verticals that have already adopted IIoT. Smart grids and meters are typical components of smart cities in various parts of the world.[3] Robots and machine sensors, meanwhile, have become mainstream in car and similar smart manufacturing plants.[4]

Figure 2: Smart city components

Industry 4.0 Threats to an Enterprise's Bottom Line

Today's smart factories (Industry 4.0) were borne out of yesterday's steam engines (Industry 1.0), mass-production lines (Industry 2.0), and IT-enabled manufacturing plants (Industry 3.0).[5]

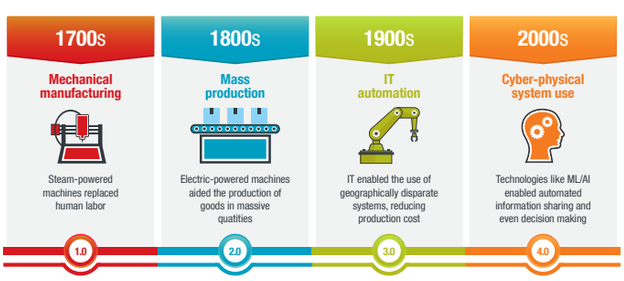

Figure 3: From Industry 1.0 to Industry 4.0

Much like any other development, the introduction of better, and in this case, "smarter" way of producing goods—in bigger quantities, less time, and at cheaper costs—brought unforeseen risks to the fore.

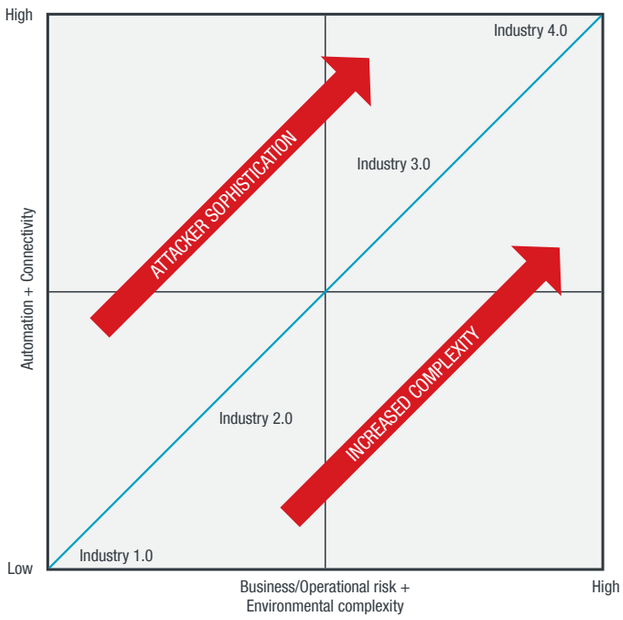

Figure 4: Risk matrix from Industry 1.0 to Industry 4.0

Any enterprise in the business of providing goods should make business continuity and disaster recovery a top priority. An IT downtime can cost a business an average of US$5,600 per minute.[6] And the bigger a company is, the bigger the cost incurred when a critical process is interrupted.

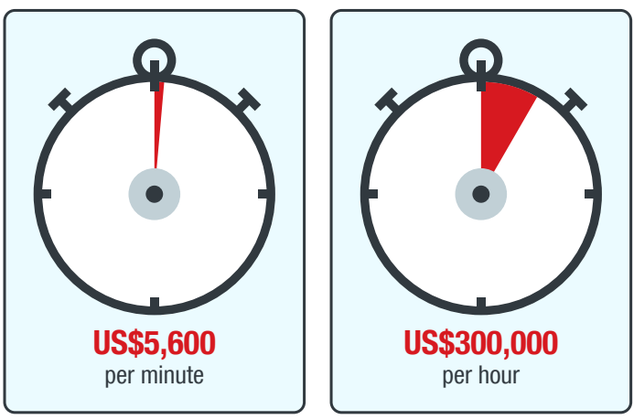

Figure 5: Average IT downtime cost; http://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/

Cases in point[7] would include a distributed denial-of-service (DDoS) attack on Dyn's servers that brought down major sites, including PayPal, Spotify, Netflix, and Twitter on 31 October 2016;[8] an IT failure which drove British Airways to freeze thousands of its Executive Club frequent-flier accounts on 27 March 2015 after confirming unauthorized activity from a third party;[9] the Amazon Web Services outage on 28 February 2017, which led to either partial or full outages on a number of popular websites, apps, and devices;[10] a break-in at one of Vodafone's datacenters on 28 February 2011 that caused mobile disruptions for several hundred thousands of customers across southern England;[11] and the nationwide blackout in Armenia brought on by an individual digging for scrap metal who accidentally damaged land cables on 6 April 2011.[12]

Cyber- and physical threats can disrupt business operations and, in turn, adversely affect an enterprise's bottom line.

Mitigating Industry 4.0 Threats

Business disruption can be caused by fires, adverse publicity, loss of key personnel, loss or denial of access to premises, floods and severe weather conditions, computer failures or loss of data, theft, bomb threats, technical or environmental failures, power failures, product contaminations, or failure of critical suppliers to deliver. And these could result in the complete failure of a business; income loss; reputation damage or loss of customers; financial, legal, and regulatory penalties; human resource issues; and adverse effects on insurance payments.[13]

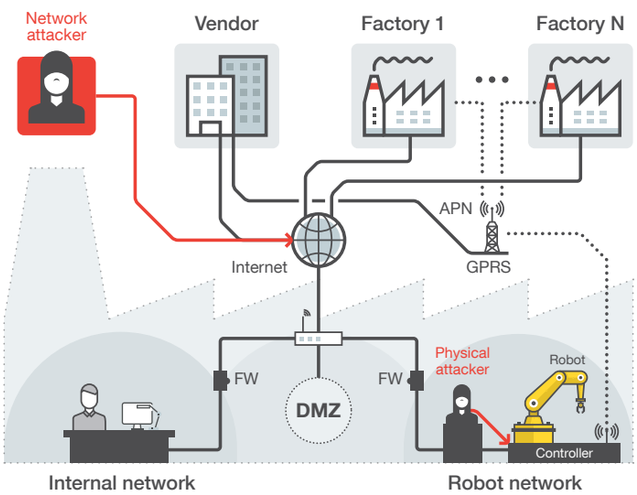

Figure 6: How smart factory attacks are carried out

Smart factories face an even bigger challenge in that they also have to worry about cyberthreats, not just physical disrupters. Their digital supply networks are at risk of threats to shared data and vendor processes. Shared data is at risk of theft via hacking or a breach[14] or, these days, being held hostage.[15] Vendor processes can be targeted to disrupt goods authenticity certification, disallow product movement tracking, and muddle returns and recalls through improper product categorization.[16]

Modern industrial control systems—typical components of smart factories—are prone to vulnerabilities that threat actors can take advantage of.[17] Industrial robots or any connected system, when exposed online,[18] can be scanned for existing bugs that can be exploited to produce defective goods or cause accidents. Insufficiently secured routers, cameras, and other devices can be hacked and used to breach a network or made part of botnets for use in DDoS attacks.[19]

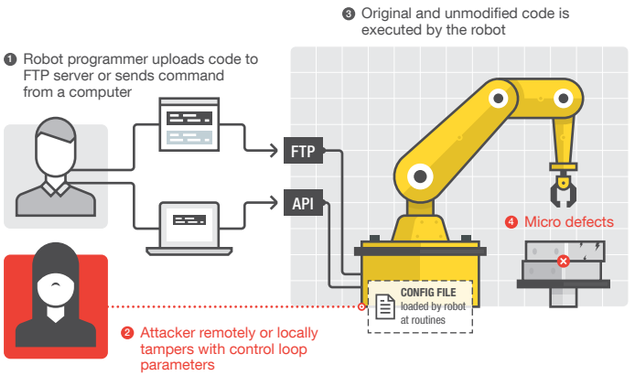

Figure 7: How a rogue robot can be made to produce defective goods

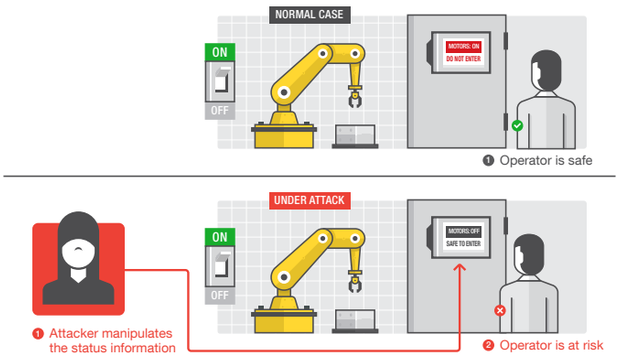

Figure 8: How a rogue robot can cause an accident

As production facilities continue to reduce human intervention, simply protecting devices is no longer enough. To address cybersecurity risks throughout the manufacturing process, make sure to take an integrated approach to security.[20]

Figure 9: Cybersecurity framework

Coming up with a cybersecurity framework is just the first step to securing Industry 4.0 environments. A secure smart factory is one with a sound foundation that uses next-generation intrusion detection and prevention, application whitelisting, integrity monitoring, virtual patching, advance sandboxing analysis, machine learning, behavior analysis, antimalware, risk detection, vulnerability assessment, next-generation firewall, anti-spear-phishing, spam protection, and data leakage technologies. Deploying a risk-reducing architecture and staying abreast of the latest in cybersecurity (threats and possible mitigation steps) by relying on trusted partners are also a must to protect all connected devices and environments on all fronts.

References:

1. https://www.gartner.com/smarterwithgartner/the-iot-effect-opportunities-and-challenges-2/
2. https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#5ae8e6641480
3. https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/securing-smart-cities
4. https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/rogue-robots-testing-industrial-robot-security
5. http://www.apics.org/apics-for-individuals/apics-magazine-home/magazine-detail-page/2017/09/20/industry-1.0-to-4.0-the-evolution-of-smart-factories
6. https://www.zdnet.com/article/the-astonishing-hidden-and-personal-costs-of-it-downtime-and-how-predictive-analytics-might-help/
7. https://www.techradar.com/news/5-of-the-worlds-biggest-network-outages
8. https://blog.trendmicro.com/dyn-servers-attacked-hackers-means-iot/
9. https://www.trendmicro.com/vinfo/au/security/news/cyber-attacks/british-airways-freezes-executive-club-accounts-after-hack
10. https://aws.amazon.com/message/41926/
11. https://www.pcmag.com/article2/0,2817,2381108,00.asp
12. https://www.theguardian.com/world/2011/apr/06/georgian-woman-cuts-web-access
13. https://www.cardiff.gov.uk/ENG/Your-Council/Strategies-plans-and-policies/Emergency-Planning-and-Resilience/Emergency-Planning-and-Resilience/Documents/Coping_with_a_major_business.pdf
14. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/year-in-review-notable-data-breaches-for-2017
15. https://www.trendmicro.com/vinfo/us/security/definition/Ransomware
16. http://deloitte.wsj.com/cio/2018/02/27/cybersecurity-in-the-age-of-smart-manufacturing/
17. https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/the-state-of-scada-hmi-vulnerabilities
18. https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/cities-exposed-in-shodan
19. https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/securing-routers-against-mirai-home-network-attacks
20. https://www.trendmicro.com/en_us/business.html?cm_mmc=VURL:USA-_-Archive-_-Archive-_-business