The Emerging IoT Cybersecurity Crisis

Authored by: Garry Drummond, CISSP, CWNA, CWSP
CEO LOCH Technologies, Inc.™
12 December 2019

Foreword

The proliferation of IoT devices is proving to be a double-edged sword. For all the benefits that IoT brings, the sheer volume of billions of intelligent IoT endpoints is proving to be a cybersecurity nightmare: there is now an ever-expanding attack surface, with each IoT device becoming an entry point for attacks.

It's important to reflect on where we are today as it relates to IoT Security. Breaches are on the increase and there seems to be no slow-down on new ways to compromise a device or network. The first half of 2019 has seen more IoT attacks than in all of 2018, a 300% increase. (12). If we take a closer look at IoT and what that has introduced into our environment, 80% of IoT devices are wirelessly connected, not wired, therefore, the approach of identifying, analyzing, and determining the risk to our environment requires a fundamentally different approach.

When you start to look at IoT devices and how they actually behave and operate, due to the lack of Memory, CPU Processing Power, and Storage, security had to be an afterthought. Many devices run non-standard operating systems and don't have a patching schedule from the vendors, or are not patchable. Also, the communication stack between one another is rather rudimentary as the UDP (User Datagram Protocol) often does not support encryption or authentication. If a device becomes compromised/infected the propagation of 'things' like worms across the IoT/OT network becomes rather simple. Unfortunately, we don't apply the same IT protections that traditional wired networks implement. In addition, we do not have visibility into the communication interchanges that are occurring between the diverse IoT devices deployed since they don't necessarily operate on the same network backbone and often work autonomously.

What does all this mean:

IoT introduces a plethora of new operating systems, new protocols, and frequencies that traditional IT and Information Security teams are unfamiliar with - creating the security blind-spot.

It's no longer about looking for a rogue on the Enterprise Network, that's where we've been focused for the last 30 years. Is there an Amazon Echo connected to my network? Is there a video camera connected to my network wirelessly?

With IoT (Internet of Things) and IIoT (Industrial Internet of Things) devices now have the ability to be autonomous/operate on separate networks within your environment. Many organizations are still relying/focused on their Enterprise Network SEIM (Security Event Information Management) to alert them to risk exposures but often missing the IoT/IIoT threats.

A new risk vector called, Nearby IoT also presents a major risk to the business and is 100% off the production network, devices like Drones, Rogue Cellular Towers, and Spy cameras are nefarious communications devices that can lead to data exfiltration.

©LOCH Technologies, Inc.™, 1285 66th St, Emeryville, CA 94608. All trademarks and Rights are acknowledged to their respective owners/company. All right reserved.

The Emerging IoT Cybersecurity Crisis

In August 2019, security researchers in the Microsoft Threat Intelligence Center warned that hackers working for the Russian government have been using poor security, misconfiguration, and outdated patches in IoT devices to infiltrate corporate networks. In several cases, the hackers simply used manufacturers' default passwords. Earlier, the FBI found that the same hacking group to be behind a Malware infection affecting more than 500,000 routers in 54 countries.

In January 2019, the US Intelligence Community Worldwide Threat Assessment report identified and evaluated the various threats to the nation. Among the cyber-related takeaways from the report were:(1)

"China, Russia, Iran, and North Korea increasingly use cyber operations to threaten both minds and machines in an expanding number of ways—to steal information, to influence our citizens, or to disrupt critical infrastructure," and "as we connect and integrate billions of new digital devices into our lives and business processes, adversaries and strategic competitors almost certainly will gain greater insight into and access to our protected information."(2)

The rise of state-sponsored hackers and cybercriminals is particularly worrisome as they are likely to possess the resources and tools to create serious harm, especially to critical infrastructure and IIoT/Industry 4.0 systems. At the Aspen Security Forum in July 2019, Microsoft revealed that its data showed the "significant extent to which nation-states continue to rely on cyber attacks as a tool to gain intelligence, influence geopolitics, or achieve other objectives."

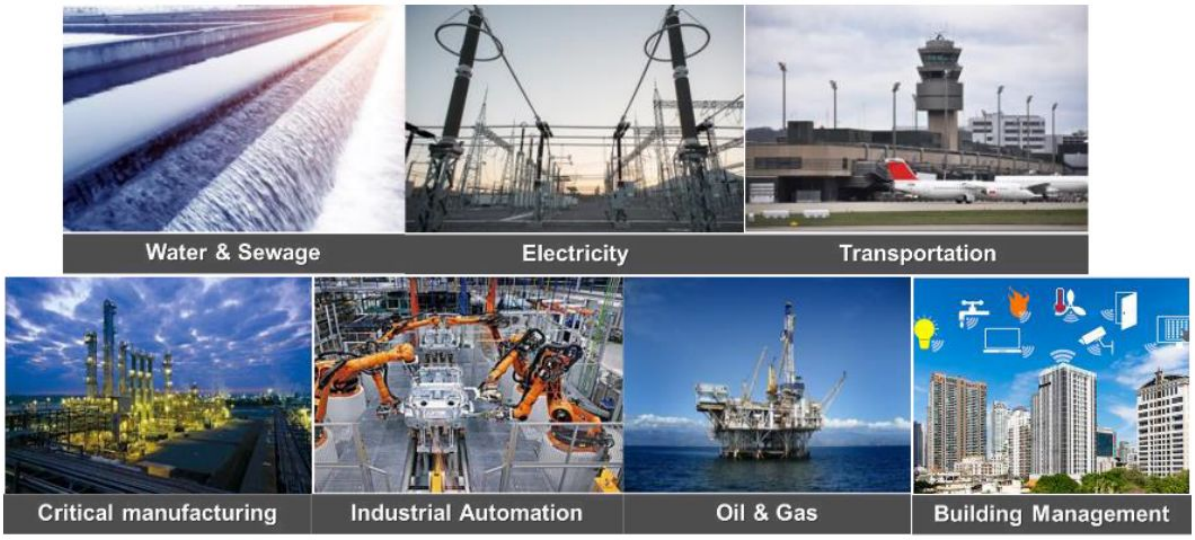
The downside of connecting our industrial and critical infrastructure systems to the Internet is that these once isolated and air-gapped systems, are now potentially exposed to foreign adversaries. Any disruption to industrial and critical infrastructure systems can have serious safety and economic consequences for society.

The Next Cyber Battleground - Critical Infrastructure and OT Systems

While the cyber attacks on IT systems are troublesome and costly, the damage wrought is generally confined to the organization and its customers and partners. There is another type of cyber attack that already exists. These attacks are targeted at the critical infrastructure and the operational technologies (OT) used by industries, economies, and society. Critical Infrastructure serves society's essential functions and needs.

©LOCH Technologies, Inc.™, 1285 66th St, Emeryville, CA 94608. All trademarks and Rights are acknowledged to their respective owners/company. All right reserved.

Disruptions to these systems from cyber attacks can have catastrophic consequences.



Source: Checkpoint

Operational technology (OT) refers to computing systems that are used to manage industrial operations such as electrical power generation, water utilities, smart grid, chemical processing, factory production, mining operations, oil and gas extraction, pharmaceuticals, and transportation systems. OT systems typically include mission-critical applications with high-availability requirements and are designed to operate for years and even many decades. (3)

Part of the challenge lies in the fact that OT systems were not built with cybersecurity in mind but instead with reliability, safety and continuity as the top priorities. Most OT systems typically ran on closed platforms using proprietary protocols and were isolated (or air-gapped) from the Internet. But they were still not immune to cyber attacks from hackers and adversaries.

Industrial Control Systems (ICS

A major element within the operational technology (OT) sector is industrial control systems (ICS), a collective term used to describe the technologies used to control and monitor industrial, buildings and critical infrastructure processes and facilities. Industrial routers, switches, and workstations complement the setup. The systems rely on protocols such as Modbus, OPC, and DNP3 for communications.

Vulnerabilities exist in the various elements of industrial control systems and several have been exploited by adversaries. For example, Stuxnet modified the PLCs that controlled Iran's nuclear centrifuges. A hacking campaign using the BlackEnergy malware targeted the HMI software from several vendors. Threat actors who want to target ICS to cripple infrastructure are actively engaged in research and creating backdoors to facilitate future attacks. (4)

©LOCH Technologies, Inc.™, 1285 66th St, Emeryville, CA 94608. All trademarks and Rights are acknowledged to their respective owners/company. All right reserved.

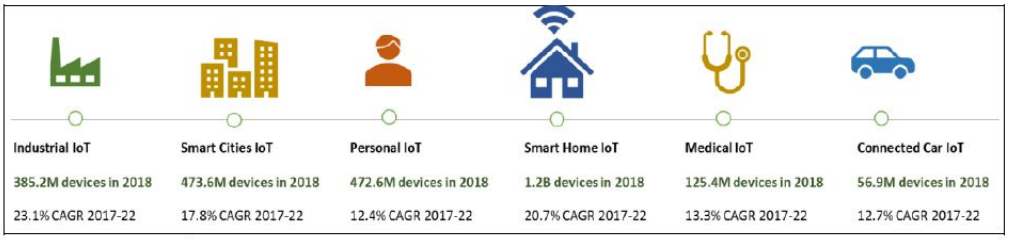
IoT and the Increased Cyber Attack Surface

Much has been written about the Internet of Things (IoT) and how they are poised to transform the way in which our physical and digital worlds interact. The “things” in IoT is a broad concept and are sometimes referred to as smart devices, connected machines or intelligent endpoints. In general, these “things” are physical objects (or systems of objects) that have to permit two-way communications over the Internet.

A jet engine could be a “thing”, as could the airplane it powers. Oil refineries, connected cars, industrial robots, locomotives, smart factories, and large power transformers are all examples of “things” that are now capable of being interconnected over the Internet. Other examples include HVACs, smart thermostats, IP security cameras, personal fitness trackers, smart speakers, and smoke detectors. We are also seeing a growing class of IoT devices geared towards medical needs – the Internet of Medical Things.

The forecast and the growth rate for the number of connected IoT devices worldwide vary widely, but the consensus is for double-digit unit growth. According to Gartner, 20 billion IoT devices will be in use worldwide by 2020, and more than 65 percent of enterprises will adopt IoT products. Another market researcher, IHS Markit, predicts that the global installed base of IoT devices will rise from 27 billion in 2017 to 73 billion in 2025. (5)

Billions of attack surfaces poised to cause cyber mischief.

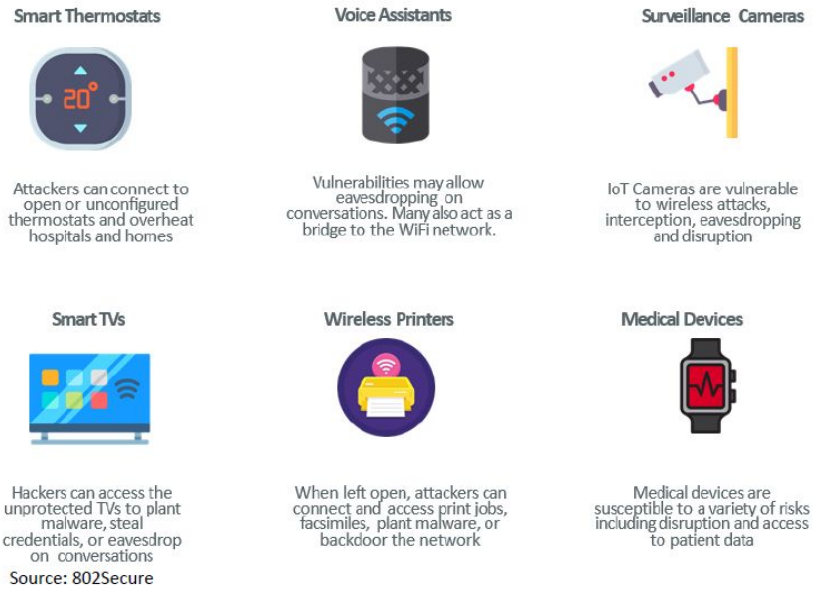


Source: IHS Markit

For all the benefits that IoT brings, the sheer volume of billions of intelligent IoT endpoints is proving to be a cybersecurity nightmare - there is now an expanding attack surface with each IoT device becoming an entry point for attacks. IoT devices, especially consumer-grade IoT, have a history of being poorly designed featuring many weaknesses and vulnerabilities that are exploitable.

©LOCH Technologies, Inc.™, 1285 66th St, Emeryville, CA 94608. All trademarks and Rights are acknowledged to their respective owners/company. All right reserved.

Threats posed by common IoT devices.



©LOCH Technologies, Inc.™ All right reserved.

According to research by Forescout, many IoT devices, including surveillance cameras, are set up by default to communicate over unencrypted protocols, allowing for traffic sniffing and tampering of sensitive information. Worryingly, almost half of the companies surveyed could not detect if any of their known IoT devices had been breached.

Shadow IoT

There are many IoT initiatives going on today within an organization that other departments are not aware of - this referred to as shadow IoT. Shadow IoT, which is the use of unauthorized IoT devices, poses new levels of cyber threats much worse than anything previously posed by shadow IT. (6)

The consequence of poor IoT cyber hygiene has led to numerous attacks, some of which have shut down Internet services in several parts of the world. And as IoT devices start becoming mainstays in smart homes, smart cities, medical devices and connected vehicles, poorly secured devices pose increased risk to health and safety to individuals, enterprises, and society.

Examples of IoT device vulnerabilities where IoT devices were compromised or have vulnerabilities.

Mirai

The Mirai botnet is malware that infects IoT devices turning them into a network of remotely controlled bots or zombies. In October 2016, the Mirai botnet comprised of 45,000 IoT bots

©LOCH Technologies, Inc.™, 1285 66th St, Emeryville, CA 94608. All trademarks and Rights are acknowledged to their respective owners/company. All right reserved.

executed a DDoS attack and successfully brought down DYN, the domain provider. As a result, CNN, Twitter, and Netflix, which relied on Dyn for DNS services, were unreachable for several hours. Besides the websites and web services that were affected, Verizon's services from broadband to cell phones was also crippled, limiting the means of communication for the east coast of the US.

Medical Device

In June 2019, the FDA warned that several insulin pumps from Medtronic MiniMed might be of risk of a cybersecurity breach. According to Medtronic, the vulnerability allows an attacker to send radio frequency signals to nearby insulin pumps to change settings, impacting insulin delivery and putting patients' lives at risk.

Smart Thermometer

A Las Vegas casino fell victim to hackers thanks to an Internet-connected smart thermometer it was using to monitor the water and fish of an aquarium in the lobby. The smart thermometer allowed the tank to be monitored and maintained remotely but was also connected to the casino's networks. While the casino had protected IT networks with firewalls from external threats, hackers used the IoT thermometer's internal network connection to find and steal information from the casino's high-roller database. (7)

Smart Home Lock

In 2019, two security researchers were able to demonstrate that a popular smart home lock and hub made by Zipato had three vulnerabilities that can allow hackers to break into a user's home. Two flaws were discovered in the design and implementation of the authentication mechanism in the Zipato Application Programming Interface (API). The third vulnerability was an embedded SSH private key for ROOT which was not unique and could be readily extracted.

A study conducted by Trend Micro and the Polytechnic University of Milan, revealed industrial robots that are connected to the Internet are not secure and prone to cyber attacks. Using search engines such as Shodan, the team found more than 83,000 robots from ABB, Fanuc, Yaskawa, Kawasaki, and Mitsubishi were exposed to the Internet and responded to their queries. If these robots were secured, they would not be directly accessible from an unauthenticated IP address querying them. According to the study, of the more than 83,000 exposed industrial robots, fifty-nine had known vulnerabilities and more than 5,100 had no authentication.

©LOCH Technologies, Inc.™, 1285 66th St, Emeryville, CA 94608. All trademarks and Rights are acknowledged to their respective owners/company. All right reserved.

Connected Cars

To demonstrate the vulnerabilities associated with connected cars, two security researchers wirelessly hacked a Chrysler Jeep while it was driving on the highway. They were able to use a cellular connection to the Jeep's entertainment system to control the vehicle's air vents, windscreen wipers, dashboard functions, transmission, and brakes. Chrysler subsequently issued a recall notice for 1.4 million vehicles and offered a software patch to fix the problem.

The scale of potential vulnerabilities for connected cars is highlighted by the sheer number of electronic control units (ECUs) and the millions of lines of software code that are making their way into modern vehicles. ECU's today manage engine and transmission control, anti-lock braking, climate control and more, and communicate via a Controller Area Network (CAN) bus. They represent points of attack by hackers, and with so much code there are bound to be numerous software vulnerabilities.

5G Wireless Networks

5G is the fifth generation of mobile networks that promises to usher in new applications for consumers, businesses and society – ranging from self-driving cars, telemedicine, connected factories, machine-to-machine (M2M), vehicle-to-everything (V2X), smart utilities and smart cities. 5G will address many of the limitations of current 4G technologies by lowering network latency, providing throughputs of up to 20 Gbps, and allowing billions of machine-to-machine connections for massively connected Internet of Things (IoT). (8)

5G networks are conceptually different than 4G networks in several ways. In addition to enhanced wireless connectivity, 5G will integrate computing, storage, networking and virtualization into flexible and distributed infrastructures that share the characteristics of today's cloud computing models, built around open source technologies. 4G, by contrast, was a hardware-based and static network designed around closed and proprietary components.

5G is an enabler of multi-access edge computing (MEC), an architecture that uses the network to bring cloud computing resources closer to the edge. MEC brings real-time, high-bandwidth, low-latency to wireless networks, making them invaluable for bandwidth-hungry, low-latency applications that generate high volumes of data interactions, such as autonomous vehicles.

5G technology is currently being developed and commercial launches are expected to start in 2020 with a widespread availability of 5G services expected by around 2025. 5G will coexist with 4G for several years with many network operators managing a hybrid network consisting of the two technologies.

©LOCH Technologies, Inc.™, 1285 66th St, Emeryville, CA 94608. All trademarks and Rights are acknowledged to their respective owners/company. All right reserved.

Cybersecurity Challenges of 5G

While 5G promises many innovative and unprecedented features, it also brings along a series of new security threats. For example, given the distributed nature of the network, hackers could attach themselves to a remote server and gain command and control to other servers to launch crippling attacks. Attackers could also deploy rogue nodes and small cells. As we pointed out earlier, the billions of IoT devices offer a myriad of entry points for cybercriminals.

“In today’s 4G world, a huge botnet formed by hacking into user devices in the home could be used to mount large-scale DDOS attacks on websites. In tomorrow’s 5G world, that same botnet could be used to take out an entire network of self-driving cars in a single city, leading to mayhem on the roads.” (Source: Verizon, CPO). (11)

The flexibility of 5G cloud services and their consumption “as-a-service” will require new types of authentication and trust between devices, users, services and operators. Security will need to align with different service and application needs, rather than those of the network as in the past.

Security challenges of 5G and evolving architectures.

IoT, V2X, M2M	Threats due to peer-to-peer connections and IoT devices with no inbuilt security
Distributed Architectures	Threats due to distributed data centers, edge computing (MEC) and network slicing
Virtualization	Increased complexity in mitigation of side channel attacks (SCA)
Multiple Technologies	Threat due to multiple new and legacy technologies, plus higher traffic volumes to manage

Source: Cisco

The sheer volume of data generated by things using 5G networks, such as IoT devices and autonomous cars, could make it difficult to spot malicious behavior. Threat detection systems using machine learning and artificial intelligence will, therefore, play an important role in 5G cybersecurity networks.

©LOCH Technologies, Inc.™, 1285 66th St, Emeryville, CA 94608. All trademarks and Rights are acknowledged to their respective owners/company. All right reserved.

5G and National Security

Given the potential benefits of 5G networks, there is universal interest from governments, service providers and equipment manufacturers to support the rollout of this new wireless.

Per IHS Markit, the combined 2G, 3G, 4G, and 5G global mobile infrastructure market for radio access networks (RAN), switching and core equipment fluctuates between $31 billion and $48 billion annually. In terms of 5G, IHS estimates that global hardware revenue is expected to reach $19 billion in 2022, starting from a very low base of early adopters in the USA, followed by 5G rollouts in South Korea and massive 5G trials in China. (8)

Heavy Reading, another market researcher, estimates that mobile operators are expected to invest more than $200 billion on their 5G networks between 2018 and the end of 2023. Developed markets such as the USA and South Korea are at the forefront of 5G rollout, but the Heavy Reading analysts expect China to dominate capital expenditures within five years. (9)

Mobile infrastructure equipment is supplied by a handful of equipment vendors, including Chinese companies, Huawei and ZTE, Samsung from South Korea, Sweden's Ericsson, and Nokia, the Finnish-American-French vendor. The two Chinese vendors have been steadily increasing their global footprint and controlled a combined 42% of the market at the end of 2018.

The growth of Huawei, in particular, has not gone unnoticed, and with 5G imminent, the US government has taken steps to ban the use of Huawei equipment in US telecommunications networks. The US government has also been trying to coerce many Western governments to take similar steps.

Concerns about Chinese telecom equipment vendors were first raised in 2012 when the U.S. House Intelligence Committee published an "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE." The committee was concerned by the close ties of these two companies to the Chinese government - allowing their equipment to be installed in U.S. networks would give the Chinese government the ability to conduct espionage and start online attacks on critical infrastructure.

©LOCH Technologies, Inc.™, 1285 66th St, Emeryville, CA 94608. All trademarks and Rights are acknowledged to their respective owners/company. All right reserved.

In conclusion, for further analysis and perspectives on IoT risk and threats, please contact Garry Drummond, CEO, and Founder of LOCH Technologies, Inc.™ for additional information. He can be reached at 1+ 510-703-6149 or gdrummond@loch.io

Citations and References

Special Acknowledgement to Amar Senan - Cybersecurity IoT, IIoT, ICS Fall Report 2019

1. 29 January 2019 - https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf
2. Madeleine Albright on Leadership, Immigration - https://www.aspeninstitute.org/podcasts/madeleine-albright-on-leadership-immigration-and-her-brooch-collection/
3. OT, ICS, SCADA – What's the difference? - KuppingerCole. https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference

4. Manufacturing - AGMA | AHT Insurance. https://www.ahtins.com/manufacturing-agma/

5. Machine learning and the Internet of Things | ZDNet - . https://www.zdnet.com/article/machine-learning-and-the-internet-of-things/

6. LOCH Reference - https://www.802secure.com/airshield2shadowiotinfographic/

7. Smart Thermometer Hack - https://mashable.com/2018/04/15/casino-smart-thermometer-hacked/

8. The 5G Network: What is 5G and how does it work? - TechGlobal. https://techglobal.ca/what-is-5g-how-fast-is-5g-applications-of-5g/

9. With 2G, 3G and LTE hardware revenues falling, 5G rollouts - https://technology.ihs.com/608641/with-2g-3g-and-lte-hardware-revenues-falling-5g-rollouts-are-coming-to-the-rescue

10. 5G And IoT - How To Deal With Data Expansion As You Scale -. https://www.pioneeringminds.com/5g-iot-data-expansion/

11. 5G and the Future of Cybersecurity - CPO Magazine - https://www.cpomagazine.com/cyber-security/5g-and-the-future-of-cybersecurity/

©LOCH Technologies, Inc.™, 1285 66th St, Emeryville, CA 94608. All trademarks and Rights are acknowledged to their respective owners/company. All right reserved.