David Farber Prize:
Cyber Civilization

Lisa Takahashi

Keio University

Policy Management

The development of the computer and the rapid advancements of key technologies have changed the game for humanity. Our security, economy, and way of life have all been impacted in one way or another as our society becomes increasingly connected. However, as the presence of the internet of things (IoT) grows, so do the vulnerabilities associated with it. One of the biggest threats to mankind is the security of critical infrastructure that is connected throughout the cyber world and directly affects our physical safety. It is imperative that ordinary people understand the vulnerability of our critical infrastructure to cyber threats and call on larger stakeholders to act and create a future society that is in fact secure.

Critical infrastructure, according to the U.S. Department of Homeland Security, provides the essential services that underpin a society and serve as the backbone of a nation's economy, security, and health. In the context of the U.S., there are 16 critical infrastructure sectors that comprise assets, systems, and networks, whether physical or virtual, so vital that their destruction would have a debilitating effect on security at all levels. Those 16 sectors include: chemical, commercial facilities, communication, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors and materials and waste, transportation systems, and water and wastewater. The rapid deployment of new technologies such as IoT into the critical infrastructure will expand the vulnerable surfaces that are available to attackers.

In the past, there have been alarming cyber attacks that have caused disruption and even damage to critical infrastructure. The Stuxnet attack in 2010 targeted the Iranian nuclear program ("Cyber-attack"). Stuxnet, a computer worm, was specifically designed to attack Microsoft based industrial computers and take control of Programmable Logic Controllers (PLCs) that influence remote actuators. The virus was, in fact, infecting the Microsoft operating system by exploiting a vulnerability that the program's creator was unaware of and that had never before been detected, also referred to as a "zero day". This attack was initiated through a random worker's USB drive. Although there have not been any official statements regarding the effects of Stuxnet, it is said that the malware was "designed to send Iran's nuclear centrifuges spinning wildly out of control" (Trautman 795). Stuxnet was the "first time anyone has seen a digital code in the wild being used to physically destroy something in the real world" (Trautman 795).

Another infamous cyber-attack was the Ukrainian power outage in 2015. Three Ukrainian electric power distribution companies were remotely attacked, which impacted approximately 225,000 customers. This was an attack on the Supervisor Control and Data Acquisition (SCADA) system that left citizens powerless for hours. During the attack,

hackers remotely switched breakers to cut the power. In addition, to prolong the power outage, hackers launched a telephone denial-of-service (DoS) against the utility's call center to prevent legitimate customers' call to get through and report the power outage (Department of Homeland Security). Eventually, though, the companies were able to restore power through manual operations. At any rate, this was the first successful blackout caused by cyber security. The reality that malicious attackers were able to get through the system of an electric distribution company to cause disruption to over 200,000 citizens is alarming and potentially represents a serious threat to the day-to-day running of nations.

Even in the wake of the Stuxnet attack, the critical infrastructure industry has shown little interest in implementing defense mechanisms in its evidently vulnerable systems (Trautman 797). In a global survey conducted by McAfee, a computer security giant, "two-fifths of all respondents, and nearly half of those in the electric industry, said that they had found Stuxnet on their systems" (Trautman 798). However, despite that alarming fact, the discovery of Stuxnet on their systems did not seem to galvanize companies into action.

The paradox of this problem is that critical infrastructure greatly relies on the newest interconnected and therefore vulnerable ICT technologies, while the control equipment at hand is typically outdated legacy software/hardware (Maglaras et al.). Many businesses believe that these cyber security issues can solely be resolved with technology. However, these problems are the result of the increased integration of technology. Like Einstein said, "no problem can be solved from the same level of consciousness that created it". Updating old software and hardware while having an underlying basic understanding of the systems in critical infrastructure will nonetheless improve situations where cyber-attacks occur. However, as our society becomes ever more complex with all things being connected, it is imperative that ordinary people call for a change in the mindset of institutions not merely limited to businesses and governments. IoT makes possible a wide assortment of wonderful benefits for daily life though the future of IoT will not all be rainbows and sunshine if we do not understand the consequences of it and initiate discussion on how to value security and build resilience in the cyber civilization.

References

"Critical Infrastructure Sectors." Department of Homeland Security, 22 Aug. 2018, www.dhs.gov/critical-infrastructure-sectors.

"Cyber-Attack Against Ukrainian Critical Infrastructure." *Siemens S7-1200 PLC Vulnerabilities | ICS-CERT*, 25 Feb. 2016, ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

Maglaras, Leandros A. "Editorial Board." *ICT Express*, vol. 4, no. 1, Mar. 2018, pp. 42–45. *Science Direct*, doi:10.1016/s2405-9595(15)30024-2.

Trautman, Lawrence J.1,2,3,4. J.Trautman@gmail.co., and PETER C.5,. ORMEROD. "Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things." *University of Miami Law Review*, vol. 72, no. 3, Spring 2018, pp. 761–826. *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&db=lpb&AN=129255039&lang=ja&site=ehost-live.