**The rise of cyberattacks on critical public infrastructures and how to prevent them**

In an episode of the TV show “Sherlock,” a pair of bad guys die in a crash after a hacker takes complete control of their car. In an episode of “Homeland,” the vice president is assassinated with his own pacemaker when a cyberattacker takes control remotely and stops his heart. On “CSI: Cyber,” a hacker infiltrates a navigation app, directing victims to areas where they get robbed.

These scenarios are no longer just the stuff of Hollywood writers’ overimagination. As our lives become increasingly digitized and connected through the Internet of Things (IoT), those kinds of hacks are becoming more and more plausible. Especially with Gartner estimating the number of connected devices in the consumer and business sectors to reach [20.8 billion by 2020](http://www.gartner.com/newsroom/id/3165317) — and many of those devices not necessarily being designed with security in mind.

But even more troubling is the reality of attacks on critical public infrastructure — the possibility of a hacker disabling a city’s entire 911 system or plunging an entire region into darkness by taking out the power grid.

As former U.S. Secretary of Defense Leon Panetta has been frequently quoted, “The most destructive scenarios involve cyber actors launching several attacks on our critical infrastructure at one time, in combination with a physical attack on our country.” Combined with the disabling of critical military systems and communication networks, these kinds of actions would result in what [he described as a cyber Pearl Harbor](http://archive.defense.gov/speeches/speech.aspx?speechid=1728).

Security experts have warned that several state actors have the capability of compromising U.S. critical infrastructure — including the Islamic State in Iraq and Syria (ISIS), which reportedly is [creating a centralized hierarchy that would be capable of forming a cyberattack group](http://www.iar-gwu.org/content/isis-has-capacity-strike-us-critical-infrastructure).

**Public infrastructure an increased target**

The [Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)](http://ics-cert.us-cert.gov/), part of U.S. Department of Homeland Security, responded to 295 incidents related to critical infrastructure in fiscal year 2015, 50 more incidents than the previous year. Many incidents go unreported, ICS-CERT said. Even if the number seems small compared to data breaches in the private sector, the potential consequences are far more devastating.

According TrendMicro’s 2015 “ [Report on Cybersecurity and Critical Infrastructure in the Americas,](http://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/the-state-of-cybersecurity-and-critical-infrastructure-in-the-americas)” of the 575 respondents — heads of security and CIOs of major critical infrastructure from 26 members of the Organization of American States — 43 percent indicated they had experienced an attack while 31 percent weren’t sure. And about half of the respondents noted an increase in computer systems incidents from the previous year, with another 40 noting steady levels.

In another 2015 [survey of 625 critical infrastructure organizations](http://www.mcafee.com/ca/about/news/2015/q3/20150720-01.aspx) from around the globe, the Aspen Institute and Intel Security found that nearly half of the respondents thought it was either likely or extremely likely that “a successful cyberattack will take down critical infrastructure and cause loss of human life within the next three years.” Respondents in the United States were more concerned than those in Europe.

Just the last few months saw several critical-infrastructure attacks around the world. In December, about 225,000 customers of several Ukrainian power companies lost power for hours. [Malware was found on the companies’ computer networks](http://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01), and Russian hackers were blamed.

More recently, [Israel’s power authority was hit with ransomware](http://www.computerworld.com/article/3026609/security/no-israels-power-grid-wasnt-hacked-but-ransomware-hit-israels-electric-authority.html) via a phishing attack. Although the grid itself wasn’t afffected, this was yet another example of a particularly vile type of attack. And as we saw in February when [the Hollywood Presbyterian Medical Center was crippled by ransomware](http://arstechnica.com/security/2016/02/la-hospital-latest-victim-of-targeted-crypto-ransomware-attack/), this kind of threat may not only cost organizations a lot of money but could also completely cripple critical operations — in this case, access to patient data and ability to perform tasks that impact patient health, such as lab work and scans.

The NSA’s director [reportedly told a House intelligence committee](http://www.ciodive.com/news/why-ukraines-blackout-matters-to-the-us/411758/) that several governments have already breached energy, water and fuel-distribution systems in the United States. One known incident that surfaced last year was [the infiltration of a New York dam control system](http://www.thetower.org/2722-iranian-cyber-attackers-hacked-new-york-dam-control-system-in-2013/) by Iranian cybercriminals in 2013.

**‘Detection and response’ as the new normal**

Various security experts expect to see [attacks on critical infrastructure to grow this year](http://www.inc.com/will-yakowicz/5-cybersecurity-predictions-for-2016.html). Both Symantec and McAfee listed this among their [top predictions of threats for 2016](http://www.symantec.com/connect/blogs/symantec-predictions-2016-looking-ahead), with McAfee noting a new trend of cybercriminals selling direct access to critical infrastructure systems.

According to McAfee’s survey, 76 percent of respondents think those threats are escalating, while [48 percent think an attack will take down critical infrastructure with potential life loss](http://www.mcafee.com/us/resources/misc/infographic-threats-predictions-2016.pdf). Nation-state actors are likely to be the culprits.

CrowdStrike’s [2015 “Global Threat Report”](http://www.crowdstrike.com/global-threat-report-2015/) also predicts that in 2016, specific nation-state actors will likely target agriculture, healthcare and alternative energy sectors “not just for intellectual property, but also for know-how such as building native supply chains and administrative expertise.”

The ramifications of the security incidents on critical infrastructure don’t just include disruption of critical operations and critical business applications. An ESG survey found that 32 percent of organizations also [experienced data breaches](http://www.networkworld.com/article/2987290/security/u-s-critical-infrastructure-under-cyber-attack.html) of confidential information. The fallout for an organization may lead to increased regulatory scrutiny and government penalties because of laws such as [HIPAA, to use healthcare sector as an example](https://www.skyhighnetworks.com/cloud-compliance/hipaa-encryption-compliance-requirements/).

Many of the attacks happen because of the lack of analytical security systems. In a SANS Institute survey of critical infrastructure organizations, less than a third felt they had excellent or very good visibility into their networks’ threats while 40 percent rated their visibility as OK, poor or very poor.

Traditional, signature-based security solutions no longer hold up to today’s sophisticated threats, especially as more data moves to the cloud. That means organizations needs to get serious about advanced analytical systems that can correlate various processes and policies — and help provide the kind of detection and response that antimalware and other single-layer technologies simply can’t handle.

The increased targeting of critical infrastructure should be a wake-up call. It’s only a matter of time before a disastrous attack wreaks havoc. Organizations need to up the ante on their cybersecurity and shift the focus on detecting all security breaches and bringing situational awareness to incidents — especially those that may pose incredible harm.

*Sekhar Sarukkai is a co-founder and the chief scientist at*[*Skyhigh Networks*](http://www.skyhighnetworks.com/)*, driving the future of innovation and technology. He has more than 20 years of experience in enterprise networking, security and cloud services development.*