CRITICAL INFRASTRUCTURE **DOOMSDAY:** Not "If," but "When"

James Arbuthnot, former chairman of the UK Defense Select Committee, said it best: "Our national grid is coming under cyberattack not just day by day, but minute by minute."[11] **In fact, nearly 70 percent of critical infrastructure (CI) companies suffered a security breach over the last year.**[12] One attack during 2014, by a group of Russian hackers called Energetic Bear, launched a campaign that targeted oil and gas companies. Through infection of industrial control software that those companies relied on, attackers embedded malware that automatically downloaded and installed when the victim organizations updated their software. This gave attackers visibility into—and potential control of—the targeted networks.

In a separate incident, a German steel mill was targeted, causing major damage to a blast furnace. According to the German Federal office of Information Security, BSI, attackers deployed a socially engineered spear phishing campaign to trick specific individuals into opening messages. From there, the cybercriminals were able to capture login names and passwords, which helped them access the mill's production network. Once in, they went after the control systems, causing elements to fail, which prevented the furnace from shutting down normally. As a result, the whole system was impaired.

Why is this happening?

When we look at the causes of CI incidents, we see a few things going on. To begin with, the supervisory control and data acquisition (SCADA) system, commonly used by CI, was not designed for security. Not only are its devices vulnerable, its networks are old and outdated. Plus, SCADA systems embed Windows and Linux operating systems, which are also vulnerable. A second cause is that, too often, the view of security is short-sighted, with an emphasis only on the electronic perimeter. This falls short because it leaves the production systems at risk. Finally, a third problem that we see is the mistaken belief that good physical security means good network security. Not recognizing the difference can lead to severe consequences.

Securing critical infrastructure: What to do

Just as we see three causes of CI incidents, we also see three key paths to preventing such occurrences. Below are steps to safeguard critical infrastructures.

1. Security Architecture: First and foremost, protect the corporate network to block infiltration of the production network. Then, segment and protect your production network with specialized security. For perimeter security, use proper tools such as firewall, intrusion prevention, anti-virus, anti-bot, and threat emulation.

2. Security Products with Granular SCADA Support: Always use products specifically designed for SCADA systems. Remember, CI industries rely on dedicated systems on specialized networks with unique protocols. Solutions like Check Point SCADA security solutions include SCADA logging, firewall, app control, intrusion prevention, and SCADA workstation endpoint security.

3. Threat Intelligence: Be sure to independently log all SCADA activity by using in-depth SCADA traffic monitoring and analysis for threats.