A Community-Based Platform for Critical Infrastructure Cyber Resilience

A Working Paper of the EastWest Institute Breakthrough Group
"Strengthening Critical Infrastructure Resilience and Preparedness"

August 24, 2015

Summary

The growing digitization and interconnection of society, and in particular critical infrastructures, increases the risk of accidental or deliberate cyber disruptions. Significant attention is being given to reducing cyber-related risk in many countries. However, a lack of awareness of the importance of cyber risk management, particularly among the owners and operators of small- and medium-sized critical infrastructure facilities and organizations, creates unacceptable risks across national economies.

The EWI Breakthrough Group on "Strengthening Critical Infrastructure Resilience and Preparedness (CIRP)" proposes to develop an action-oriented, interactive, community-based platform where critical infrastructure owners and operators can share stories related to cyber incidents and increase their awareness of cyber risk management.

The platform will feature two elements:

- Stories and case studies of critical infrastructure cyber risks and responses, contributed by community members.
- Risk assessment and management questions and techniques.

Definition

For the purposes of this work, the term "critical infrastructure" means the assets, systems and networks so vital that their incapacitation or destruction would have a debilitating national or regional effect on security, the economy, public health, safety or quality of life.

Stories and Case Studies

We included the following story as an initial example for discussion:

A report[1] of the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik (BSI)) released just before Christmas indicated that hackers had attacked an unnamed steel mill in Germany. They were able to compromise the control system and disable a blast furnace's ability to be properly shut down. This resulted in "massive," but unspecified damage.

The security and industrial control systems (ICS) community has given significant attention to Stuxnet, launched late 2007 or early 2008, and the weapons-grade malware attack that sabotaged centrifuges at an Iranian uranium enrichment facility. Since that attack, discovered in 2010, the security community has predicted that more

[1] "The State of IT Security in Germany 2014," English version available at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014_pdf.pdf?__blob=publicationFile.

"destructive" attacks were on the horizon. With the nature of ICS and the management processes typically surrounding them, critical infrastructure (such as power and energy) if similarly attacked, could have a much wider degree of human and societal impact than what resulted at a single steel plant.

What has been disclosed about the steel mill attack indicates that the attackers came in through the business network via spear-phishing[2] then successfully worked down through the production network to the controllers that operate the plant. Through sending targeted email messages that were cloaked as legitimate correspondences, the attackers were able to inject malware into key systems to gain multiple points of entry and exploration. The attackers were credited with the exploration of a "multitude" of systems including the ICS portion of the network.

The report states, "Failures accumulated in individual control components or entire systems." As a result, the plant was "unable to shut down a blast furnace in a regulated manner," which resulted in "massive damage to the system."

The report also states the attackers appeared to possess advanced knowledge of industrial control systems: "The know-how of the attacker was very pronounced not only in conventional IT security but extended to detailed knowledge of applied industrial controls and production processes."

There is no indication as to how long the attackers were in the systems or if the disablement of the shutdown procedure was intentional or just an accident. The report does, however, give us a stark wakeup call that while expertly crafted weaponized malware like Stuxnet can most certainly cause physical damage to ICS systems, even an inexperienced or tool-driven hacker can do severe damage to an accessible critical infrastructure system.

Risk Assessment and Management Questions and Techniques

The following text is drawn from another EWI work in progress, "Cybersecurity Risks and Rewards," available as an accompaniment of this working paper for this CIRP Breakthrough Group:

The CEO should start by finding out how well his risk management team understands the cybersecurity risk landscape. One way to get there is to ask five key cybersecurity risk questions. These questions are not much different than the questions one might ask about other common business risks, and that is the point. As these questions confirm, managing cybersecurity risk is like managing other risks. It requires a common sense approach and reliance on technical expertise that the CEO may not have.

Experience teaches that most companies are unable to provide convincing answers to questions 3, 4 or 5. The cybersecurity risk landscape is very complex, and new risks arise regularly. Residual risk is thus somewhat open-ended. But known residual risks are identifiable. Similarly, prioritization of investments in cybersecurity is difficult because of the relative immaturity of the field. There is little data to support a quantitative tradeoff between, for example, training employees about malicious attachments versus purchasing a better firewall.

The most important thing to remember is that the answer to question 1, "What are we trying to protect?" defines the answers to all the other questions!

1. What key information and technology assets are we trying to protect?
2. What are the major cybersecurity risks that could affect our business operations and profitability?
3. What techniques are we using to mitigate those risks?
4. What residual risks remain after we have applied those techniques?
5. How did we decide where to prioritize our risk management expenditures and efforts

[2] Spear phishing is an email that appears to be from an individual or business that you know; but, it isn't. The victims are asked to click on a link inside the email that allows the attacker to insert himself inside the enterprise's systems.

Discussion Questions

What are the critical success factors for the platform?
Towards what infrastructures should outreach focus first? Toward which countries?
What other organizations should EWI leverage to ensure rapid progress?
How will we know whether the platform is successful?