Over the past several years, there has been intense focus by governments and industry on the potential for cyber attacks on critical infrastructure. Recent events show us that the focus is essential.

What is “critical infrastructure?”

In his February 12, 2013, Executive Order—Improving Critical Infrastructure Cybersecurity, President Obama borrowed a definition from the USA Patriot Act of 2001, stating that it is “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.” This would include such things as telecommunications systems, public health systems, transportation systems, power generation and delivery, water supply, financial services, food production and distribution, government, and public safety.
Critical infrastructure businesses are attractive targets for cyber criminals. Many have valuable personal information about consumers and other confidential information. Like other businesses, they are vulnerable to attacks designed to cripple a company’s ability to conduct business. While those are significant concerns (just ask the Bundestag in Germany), perhaps the greatest risk facing some critical infrastructure companies is the possibility of cyber attacks on computerized industrial control systems.

This has happened. While the Stuxnet attack on Iranian nuclear centrifuges in 2010 may be the best known example of a cyber attack on industrial control systems, it certainly isn’t the only one, nor was it the first. Others have been launched against a water and sewage system in Australia, an oil pipeline in Turkey, a steel mill in Germany, and possibly a railway system in the US. Most recently, we’ve seen reports of a cyber attack on a small dam in the US by hackers in Iran, and of multiple attacks on the power grid in Ukraine.

How bad is the problem?

In a January 2016 report, the Industrial Control Systems Cybersecurity Emergency Response Team (ICS-CERT) of the US Department of Homeland Security noted that from October 2014 through September 2015, it monitored 295 cyber attacks in the US on industrial control systems. It seems certain that the number of attacks in the US and worldwide was much larger. Nearly half of the attacks were directed against the Critical Manufacturing and Energy sectors. While the vast majority (69 percent) were completely unsuccessful, the number of attacks that reached victims’ control system environments increased by 33 percent over the previous year.

What can critical infrastructure businesses do to address the risk of cyber attacks? As with all cyber risks, companies need to:

1. Identify what their risks are.
2. Manage the risks by implementing changes to equipment, practices, and procedures (including employee training) necessary to reduce the risks.
3. Consider managing the financial consequences of a cyber attack through cyber insurance.
Can cyber insurance really help? Yes.

The process of applying for and obtaining cyber insurance policies can help companies understand their risks better. Cyber insurance underwriters are very knowledgeable about risks companies face and increasingly rely on input from individuals with strong technical knowledge. This can lead to very illuminating discussions that help identify cyber risks and steps companies can take to address them. Also, good cyber-risk hygiene is becoming a prerequisite to obtaining cyber insurance and to getting it on favorable terms. That fact can be a strong incentive for companies to manage their cyber risks well.

While conscientious risk management can reduce the risk of severe consequences resulting from a cyber event, the risk cannot be eliminated completely. The availability of robust cyber insurance can take the financial sting out of such an event.

Cyber insurers are comfortable covering the economic consequences of attacks like the one against the German Bundestag that cause no physical damage. Those losses would include the cost of forensic investigators to determine what happened, legal costs, liabilities resulting from third-party claims, certain claims by regulators, loss of digital assets, and business interruption loss. While all of those losses can be covered, the scope of coverage varies widely from one policy to another.

The answer is murkier for attacks that do cause physical damage or bodily injury. With rare exceptions, cyber policies do not cover bodily injury or property damage resulting from a cyber attack. While general liability and property policies are designed to cover those types of losses, even they often do not cover cyber risks.

As a result, in the event such losses are caused by a cyber event, a company may have little or no insurance available. Insurers understand the problem, and some are starting to introduce new policies and changes to existing policies that can provide meaningful coverage. Companies that believe they have such risks should investigate that with their insurance broker.

One last point: Risk managers have cited the potential for reputational damage caused by a cyber event as one of the main reasons they buy cyber insurance. Unfortunately, cyber insurance policies typically do not cover such damage. The good news is that reputational harm can be covered under specialized policies.

Cyber attacks on critical infrastructure are the frightening new frontier of cyber risk. They deserve the full attention of businesses and governments that must manage that risk.

References


11. https://ics-cert.us-cert.gov/


Our Mission
To be the worldwide value and service leader in insurance brokerage, risk management, employee benefits, and retirement services

Our Goal
To be the best place to do business and to work