CONTROL ENGINEERING®

Reed Business Information.
RBI™

Vol. 56 No. 5

MAY 2009 Covering control, instrumentation, and automation systems worldwide

Addressing SIS Cyber Security: First or Last?

When considering integrated control and safety systems, building a strong defense is an investment in ensuring business continuity.

Bob Huba and Chuck Miller
Emerson Process Management

February 2008: A company that boasts it provides "total fire protection systems" went up in flames. Smoke was seen coming from the warehouse-like buildings that house Atlantica Mechanical of Dartmouth, Nova Scotia—a contracting business that oversees the design, installation and maintenance of fire protection systems. The local fire department struck the blaze, but the building and contents were lost.

Ask a diverse crowd of people to define the term "security" and the responses will likely include financial securities; fire protection; natural disaster protection; protection against unauthorized access to property, computers, and personal I.D.; protection against un-insured motorists; and many more similar concepts that tend to center on physical things.

> **"Workers need better training on managing backup systems in case of attack."**

Conduct a similar exercise with business executives and the responses will likely include cyber security; protection of intellectual properties; protection of critical business information; protection of personnel, facilities, assets, and the environment.

What these and the many other responses you hear illustrate is that most people consider security synonymous with defense—defense against unexpected interruptions to our daily activities.

Frequently, businesses will approach security using a domain-by-domain approach—protect the perimeter, protect the people, protect the intellectual property, protect the environment, and so forth. However, when you step back and look at it, security is really about ensuring business continuity and it is best achieved by designing a unified defense-in-depth strategy and architecture that can defend against myriad possible business interruptions.

Businesses have been aggressively engaged in establishing a strong defense against unauthorized access to their digital systems for about the last 20 years. Today we generally refer to these defensive efforts as cyber security, and while protecting against attackers that are using the Internet is an important consideration, cyber security represents only one part of a robust strategy that builds a larger sense of defense-in-depth.

It only takes one

In October 2007, about 1,100 employees at the Oak Ridge National Laboratory received versions of seven phishing e-mails which appeared legitimate. Rather than verify the messages' authenticity, eleven employees opened the emails' attachments, which enabled the hackers to infiltrate the Lab's system and remove data. Later DHS investigations reported that the hack originated in China.

Devil in the details

March 2008: "Workers operating networks supporting the nation's critical infrastructure, such as telecommunications and transportation, need better training on how to manage backup systems in case cyber-attacks take down main systems," said a top DHS (Department of Homeland Security) official. That's one lesson learned during Cyber Storm II, a DHS simulation of a large-scale coordinated cyber attack on the nation's infrastructure networks.

The underlying premise of a unified depth-in-defense strategy is simple—no single mechanism offers adequate protection against the variety of attackers and their evolving weapons. Therefore it is best to create a series of protection layers designed to impede attackers in hopes that they can be detected and repelled or simply give up and go elsewhere to seek less fortified installations.

That certainly seems simple enough but, as the saying goes, "the devil is in the details." Architecting a unified defense-in-depth strategy is not easy and, to be effective, its development and design demands full engagement and knowledgeable representation from every part of your business.

Later, this article will focus on the control- and safety-system domains but, as we just indicated, the most successful defense-in-depth strategies are those that encompass the entire business and include the following elements:

- Close and lock the doors: policies, practices and enforcement;
- Identify the "jewels" that must be protected—why and from whom;
- Use what you already know by conducting risk assessments, layer of protection analysis, and developing security assurance levels;
- Ensure that regular tests are conducted to exercise detection and alert systems, and the actions of persons responsible for responding to alerts;
- Establish and test disaster recovery implementation, including reloading saved software;
- Recognize and accept that there is no single protection mechanism;
- Create a torturous path for intruders;
- Understand your company's entire depth-in-defense architecture and leverage its infrastructure to protect the control and safety system domains;
- Apply appropriate protection, including industrial grade devices, in control and safety domains;
- Connect control- and safety-system domains using good engineering practices; and
- Accept that this is not a one-shot effort; that the sources, goals, and sophistication of attackers and the weapons they use continue to evolve, requiring that you continuously re-evaluate, and, when necessary, strengthen your protection layers.

Closing and locking the doors

April 2007: Lonnie Charles Denison, an employee of Science Application International Corp. in San Diego, was working as a contract Unix system administrator for the California Independent System Operator (ISO) Corp. Frustrated with an unresolved dispute with his employer, Denison tried to disrupt an ISO data center in Folsom, CA, by hammering the safety glass of an emergency power shut-off and pushing the button.

Even the youngest child understands the need to close and lock the doors to keep out the "bad guys," yet all around the world businesses essentially ignore this simple security measure and leave many of their doors open.

Following 9/11, process industries spent millions of dollars to install and upgrade perimeter fencing, dig ditches, add berms, reinforce guard gates and plant entrances, and install double-factor security technologies at employee entrances. To a person driving by one of these post-9/11 chemical, pharmaceutical, or refining facilities, it appears that they are nearly impenetrable.

However, looks can deceive, especially when you probe a plant's "back" doors. Vehicles with the correct markings—UPS, FedEx, caterer vans, and contractor buses—are often waved through the contractor's gate. Even if they are stopped, the check by security personnel, who are usually contractors themselves, is often very cursory.

A sound defense-in-depth strategy must include extensive policies, practices, and enforcements.

Certainly one part of such a collection must include what is required for visitors, contractor personnel, vendors, utility personnel, and others,

Troy's lesson

About 1200 BC, the Trojans protected Troy against an invasion by the Greek army for more than a decade. However, as the story goes, when traditional tactics failed, the Greeks penetrated Troy's defenses using a wooden horse that hid a handful of soldiers.

Troy's lesson is that committed attackers create their own rules of engagement and will apply innovative technologies to gain access to your business. Ensuring business continuity requires your defense-in-depth implementation provide timely detection, robust prevention, and appropriate and timely reaction/response.

to gain plant entrance. It should also address what contactor companies that provide on-site personnel must do before allowing their personnel to enter your plant—including background checks, safety training, muster station, evacuation training, personal communication, and so much more.

Hardware and policies

November 2006: Federal inspectors confirmed a security breach at the Oak Ridge Y-12 nuclear weapons plant when an unauthorized laptop computer was carried into a high-security area. Investigators confirmed that Y-12's cyber security personnel did not respond properly after the breach was discovered and did not report the incident to Department of Energy (DOE) headquarters in Washington until six days later. DOE policies require that such incidents be reported within 32 hours. The involved employees' access privileges have been revoked and they are awaiting future disciplinary action.

Eric Byers, CEO of Byres Security, says, "Policies and procedures are a quick win area. Managing something as simple as laptops and memory sticks is crucial. All the technology in the world won't help if you don't have these procedures in place."

Byers is correct, but even a vault full of policies and procedures won't protect you unless you are also willing to enforce them strictly. Until you are prepared to back your policies and procedures with immediate discharge of employees, contractors, vendors, etc., they are essentially worthless.

Policies and procedures help close the doors; tough enforcement locks those doors!

Identify the jewels

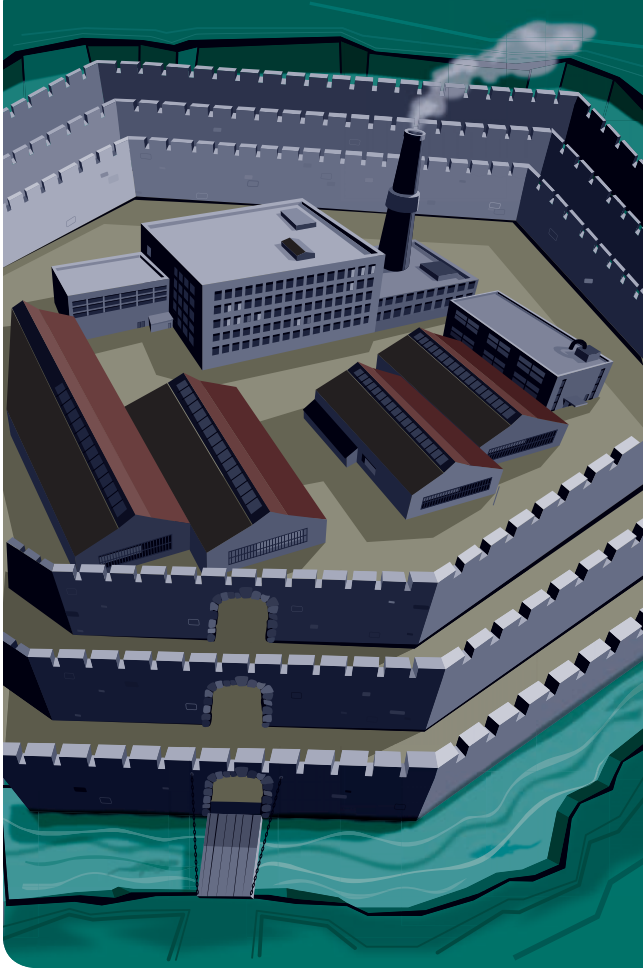
January 2008: A Polish teenager reportedly turned the city of Lodz's tram system into his own personal train set. Using a modified TV remote control, the 14-year-old was able to change switches and control signals that resulted in the injury of 12 people and the derailment of four tram vehicles.

Every company has physical assets and intellectual knowledge that must be guarded at all costs:

- Intellectual knowledge includes client information at stock brokers; research and clinical trial data at bio-techs; and fragrance ingredients and recipes at perfume manufacturers.
- Physical assets include generation, transmission, and distribution systems of electrical utilities; production process units for specialty chemicals and refineries; and pipelines and compressors at gas and oil transmission companies.

Alan Paller, the director of research at the SANS Institute, a cyber security education organization, recently revealed a CIA secret: "According to the CIA's top cyber security analyst Tom Donahue, computer hackers tried to infiltrate and disrupt the electric power grids in several foreign regions. And in some places, they succeeded."

Paller says he decided to break his secrecy agreement with Donahue and the CIA, "because the heads of utilities get lied to by their technical people. The technical people say 'oh, nobody can get in! We're not connected to the Internet.' But we had three people at that same meeting who, for a living, did penetration testing of utilities, and every one of them said they have never failed to get in, even when the organization claimed they weren't connected to the Internet. They just don't know all the connections they have."



Medieval concepts of defense-in-depth still apply in newer forms. ***Source:*** Control Engineering

Certainly the intent of a business continuity security system is to protect as many assets as possible, but common sense tells us that we simply can't protect everything equally. You must identify the "jewels," prioritize the value of each, and then erect the defense-in-depth architecture that provides the best solution to ensuring business continuity.

In part 2 (to appear in the July 2009 Inside Process section), we dig into implementation issues. **ce**

Bob Huba is a senior product manager for Emerson Process Management and coordinates security and cyber security initatives for DeltaV products. Chuck Miller is the business development manager for safety instrumented systems for Emerson Process Management.

ER-00119-May09