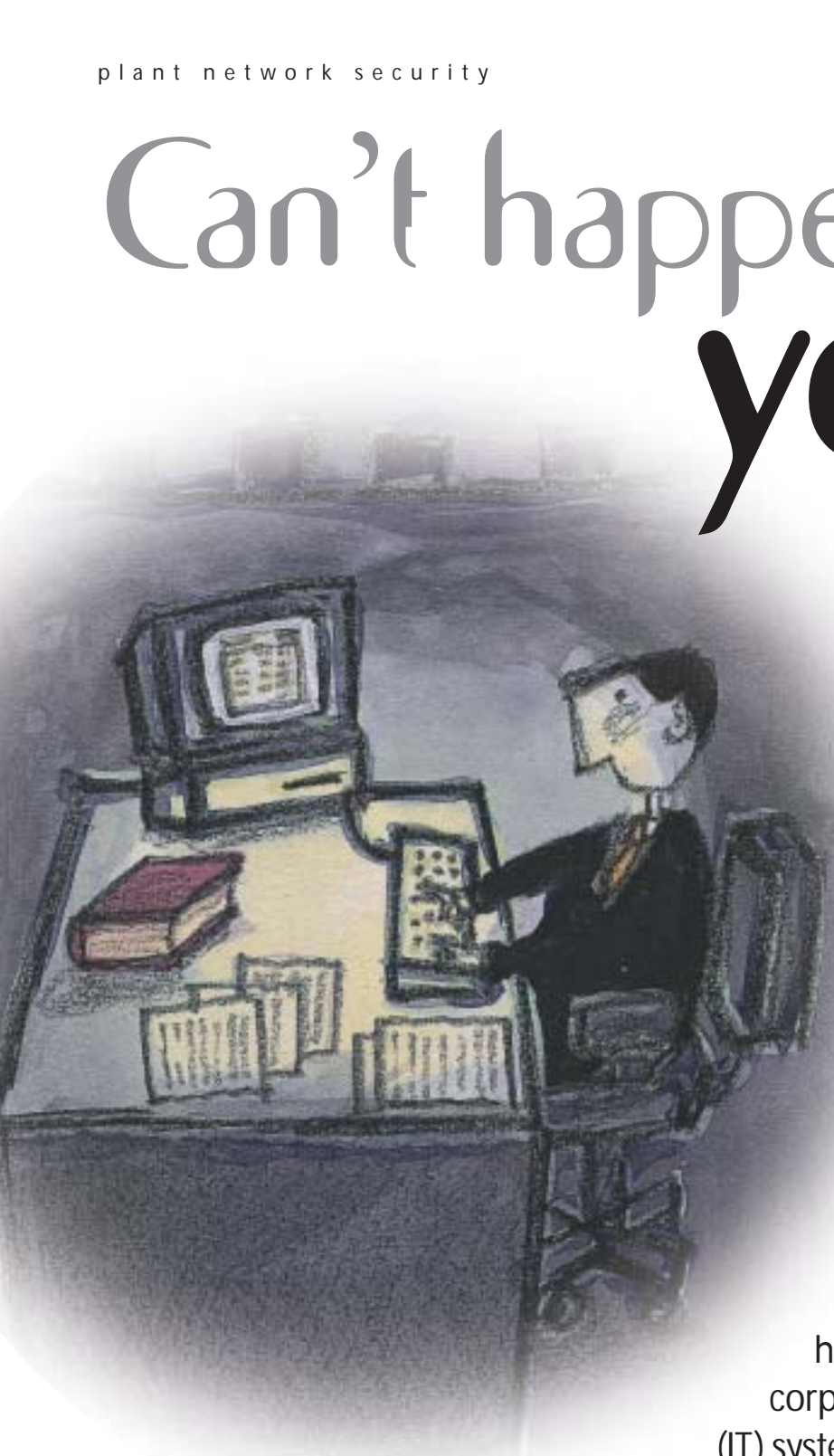


Can't happen at your site?

The black-hat community sees that as bluster and a challenge.

BY ERIC BYRES



Unless you've been hiding out on a desert island for the past year, you can't help but notice the serious impact hacking and viruses have had on corporate information technology (IT) systems.

At least once a month, a new hacker exploit or Trojan e-mail threatens to do considerable harm to the workings of a business network. If hackers can do that much damage to a desktop PC, what about that programmable logic controller (PLC) or human-machine interface sitting on the plant floor?

W We can no longer delude ourselves into thinking hackers won't bother with our distributed control systems and PLC systems.

The bad news is that recent studies indicate hackers can do a lot of damage to process equipment—and in some cases are doing so. In May 2001, hackers took advantage of security lapses in the systems of the California Independent System Operator and the California power grid narrowly avoided shutdown.

In October, an Australian man was sent to prison for two years after he was found guilty of hacking into a waste management system and causing millions of liters of raw sewage to spill out into local parks, rivers, and even the grounds of a Hyatt Regency hotel.

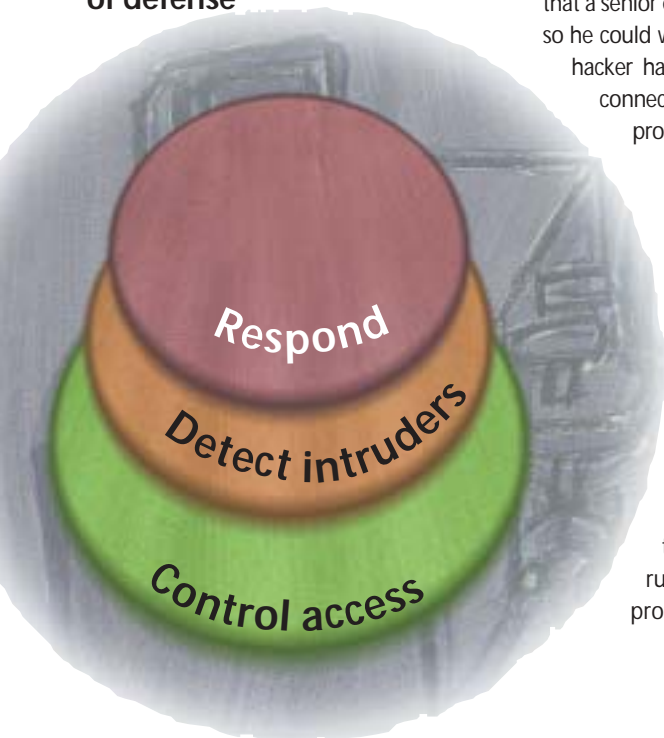
He exacted this revenge after the area's council rejected his job application to work as a control engineer at the treatment plant.

It appears that the problem may be more widespread than most process engineers believe. The incident database maintained by the British Columbia Institute of Technology Internet Engineering Lab now contains more than a dozen cyberattacks involving process control process systems in all sectors of manufacturing.

CYBERPUNK ON A JOYRIDE

We can no longer delude ourselves into thinking hackers won't bother with our distributed control systems (DCSs) and PLC systems. Ten

Intrusion detection systems are the second layer of defense



years ago, that might have been a reasonable assumption because process networks were awkward, proprietary systems that were isolated from most corporate systems.

Today, that has changed because we are building sensor-to-boardroom integrated systems that use open standards such as Ethernet, TCP/IP, and Web technologies.

Depending on the corporate firewall to protect the process is not the answer. That ignores the well-documented fact that more than 70% of all corporate hacking is from inside the firewall. In other words, most of the security risks to a control network may not be an Internet teenager on a joyride but rather a disgruntled employee.

In fact, one of the first reported cases of plant-floor hacking occurred in 1988 on an Allen-Bradley DH+. An angry worker used it to modify a different department's PLC-5. He changed the password to something obscene, blocking all maintenance access to the system (apparently he had found the original password on a Post-It note).

To make matters worst, firewalls don't always protect you. Recently, a large manufacturer in Cleveland started to notice PINGs (small messages used to probe which computers are attached to a network) appearing on the PLC research/testing network.

Investigation led to a modem attached to a desktop in the finance department. It seemed that a senior executive had added the modem so he could work from home. Unfortunately a hacker had located it and was using the connection to bypass the firewall and probe the network for security holes.

CREATING ITS OWN SECURITY

There are a number of reasons why standard IT security standards can't directly apply to the plant floor. First, the nature of process control systems, with their reliance on unusual operating systems and applications, means many of the software-based security solutions will not run, or if they do run, they will interfere with the process systems.

Secondly, traditional IT security techniques focus on threats from outside the organization. As we noted earlier, this is not the primary risk for process control security. In effect, the process control world faces the task of creating its own security standards.

Where do you start if you want to build a solid cyberdefense for your control system? At the present time, there are few best-practices guides or standards to guide process engineers, so the challenge is considerable. However, it is not insurmountable if one follows an organized implementation strategy.

The first stage is to develop a security policy for the control systems. This is a statement of the goals, responsibilities, and accepted behaviors required to maintain a secure process environment.

This defines the direction, gives broad guidance, and demonstrates senior management support for security-related facilities and actions across the organization.

A security policy should be technology and architecture independent and should not include the implementing procedures and processes. In other words, the security policy outlines what you want to achieve—not how you'll do it.

BYTE POINT OF TRAFFIC CONTROL

Once the security goals are clear, overall network architecture development can start. This usually involves creating a multilevel network with firewalls between the layers.

For example, a simple architecture might be to divide the plant into two levels: a business network level and a process control network level. At the process level, there might be two or more networks divided either by function (e.g., brew plant network vs. bottling network) or by manufacturer (e.g., PLC network vs. DCS network).

Regardless, all internetwork and interlayer traffic flows through the firewall, giving the system a single point of control to manage all network traffic.

For firewalls, there are a number of options from which to choose. The simplest and fastest is usually a packet inspection firewall that checks each network packet against a filter list to determine whether the packet should be forwarded.

These can often implement directly using an Ethernet switch. More complex firewalls include proxy firewalls and air-gap systems. Regardless of which style you select, it is usually best to make it a different brand name than the one used for the corporate Internet firewall.

USE INTRUDER TRAFFIC PATTERNS

While the firewall is the lock on the door to the process network, it is not the burglar alarm. You need some method of monitoring traffic and identifying malicious activity on the network.

This tool is known as an intrusion detection system (IDS) and ranges from a simple scan detector to a heuristic engine that profiles user behavior to an action-oriented system that reaches out and takes action against the suspected intruder.

In the process world, traffic patterns tend to be very consistent, so even simple traffic matrices that show who is talking to whom can be a big help.

For example, if a PC in the accounting department suddenly starts chatting up a

storm to a PLC, it might be time to take a closer look.

An IDS also helps configure firewall filters by identifying which traffic patterns are normal and which patterns need to be blocked.

The layered security model is very strong if it is implemented as designed and without exceptions. Unfortunately, as we all know, there will be exceptions.

For example, a control vendor may need to connect into a PLC via a modem to offer technical support. As tempting as it might sound, banning nonstandard connections outright is not usually a solution because the No. 1 goal is to facilitate production, not enhance security.

The solution is to systematically record exceptions to the model and to ensure that means other than the standard firewall securely deal with the exceptions.

For example, a configuration policy and tracking system of all modem connections might be a first step.

A more advanced solution might be to set up a secured remote access server attached to the firewall as a dial-in point for all vendors.

EXIT PROPRIETARY HIGHWAYS

The final stage of the security strategy is to develop an incident response plan. Oftentimes companies know they are being hacked, but they don't know how to handle the problem.

Rather than waiting until they are in trouble, these firms should have an established security response team and a process to deal with incidents in advance. The team would monitor events and act quickly in the event of a serious incident.

There is no easy fix to the issues faced by automation specialists when it comes to network security.

For example, many current corporate security solutions are too complex for most controls technologists to implement without additional training or assistance.

Certainly we can't turn our backs on Ethernet, Web-enabled equipment, and open systems and return to the days of slow, proprietary data highways. The benefits of open network architectures are too great to ignore.

But we can't ignore network security either.

Automation engineers need to start taking an active interest in how their process is going to weather hackers and slackers from the outside world. There are now a number of excellent courses every automation specialist should consider taking that teach networking from a plant floor perspective.

These courses may not teach enough to build a firewall, but one will learn what questions to ask when considering an interface between business and the plant floor. In the same vein, companies need to appoint a team member that will tackle industrial network security as a primary focus.

Finally, it is time we start putting pressure on vendors and on organizations such as ISA—The Instrumentation, Systems, and Automation Society to develop standards for process network security. IT

See related story about standards, page 50.

 **Behind the byline**
Eric Byres is a professional engineer and the research team leader of the Internet Engineering Lab at the British Columbia Institute of Technology. He has published numerous papers and articles. Byres is a regular speaker at ISA, IEEE, and other conferences. He is the chair of the ISA Industrial Ethernet Conference and a board member of the Industrial Automation Open Networking Association. Contact him at Eric_Byres@bcit.ca.

