IT security and the plant floor

A few months ago, while attending a conference on "Cybersecurity for Process Control," we heard a question from a very smart network engineer at Cisco that got us thinking. He asked:

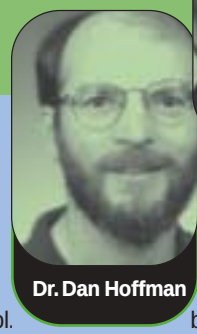
"Why not just apply the already developed practices and technologies from information technology security to plant floor security—isn't that good enough to solve the problem?"

A week later, an IT security specialist said:

"None of this would be a problem if those plant floor people just used proper security policies. What's wrong with them?"

Both of these questions are valid. In the dozens of industrial cybersecurity incidents we've investigated over the past five years, had the facility followed good IT security practices in network design, password handling, and access controls, virtually none of the problems would have occurred. So why don't we just deploy the standard IT practices for our process control systems and stop making such a big deal of plant floor security? Are process engineers so stupid, lazy, or stubborn that they won't just do what IT says?

Process engineers are certainly not stupid, lazy, or stubborn (OK, there are a few exceptions). Certainly some don't deploy the proper IT security measures because they don't understand them, but most hesitate because they sense that somehow many IT practices don't mix well with the plant floor environment. And they're correct, for four very good reasons.



Dr. Dan Hoffman

Eric J. Byres

DIFFERENT EYES

First of all, the goals of IT are different from those of process control. The IT world sees performance and data integrity as paramount, while the industrial world sees human and plant safety as its primary responsibility. These differences in goals mean huge differences in acceptable security practice.

For example, using standard password lockout procedures just isn't acceptable for most HMI stations—the default needs to let the operator in, not lock him out, which is the opposite of the IT assumption. Imagine how popular the security manager would be if, during a reactor meltdown, the operator panicked and misspelled his password three times, causing the HMI to lock out all access for the next 10 minutes.

Second, the assumptions regarding what to protect on the IT network and process control network are different. In the IT world, the primary focus is to protect the central server and not the edge client. In process control, the edge device is far more important than a central host. Thus, standard architecture of commercial network security—namely, the firewall protecting the server—may not be appropriate to industrial applications. Unless we put a firewall in front of every controller, our most important assets are largely undefended.

Clearly industry needs some economical technology that gives us the protection of firewalls while at the same time being widely distributed to protect our critical edge devices.

It is worth noting that this server-centric security mentality permeates many of the IT communications documents, such as the wireless Ethernet standard, IEEE 802.11. In the current version of this standard, the authentication procedures validate only that the workstation signing in to the central access point is the authorized device. The access point never has to prove it is valid and authorized to the edge device.

This protects the central access point from rogue workstations signing on to the system, but it certainly does not stop rogue access points from fooling workstations into joining the wrong network. Maybe the IT world considers workstations expendable, but a PLC on the edge of a wireless network is not.

PROCESS POINTS

Third, many processes require real-time performance and continuous operation that is rare in IT applications. As a recent National Institute of Standards and Technology document stated:

"Real-time computer systems used in process control applications have many characteristics that are different from traditional information processing systems used in business applications. Foremost among these is design for efficiency and time-critical response."

The process control industry needs to evaluate the performance impacts and tradeoffs of using many information security technologies before they deploy in industrial real-time control systems.

Finally, the nature of process control systems, with their reliance on unusual operating systems and applications, means that many of the software-based security solutions will not run, or if they do run, they will interfere with the process systems.

A good example of this came at an ISA Industrial Security Conference in Philadelphia. When an emergency shutdown system on a boiler failed to operate correctly, investigators discovered antivirus software installed on the computer used to configure the safety system. This software blocked the correct operation of the safety system.

What is the solution? It certainly isn't to just throw out all IT security technologies and practices and start from scratch. The IT department is not the enemy.

The answer lies in understanding that the industrial control world has already borrowed heavily from the IT world, making technologies such as Windows, TCP/IP, and Ethernet our own. Now we need to borrow their security technologies and practices but modify them and learn how to use them in our world.

We need to press forward to make plant floor cybersecurity as universal as plant floor safety. IT

Eric J. Byres, P.E., is a faculty member and research manger of the Internet Engineering Lab at the British Columbia Institute of Technology. **Dr. Dan Hoffman** is a professor at the University of Victoria, where he researches network and security testing methodologies.