




By Eric Byres, Byres Security Inc.

---

# PROTECT YOUR PLANT

---

AVOID BASIC ERRORS IN  
CYBER SECURITY STRATEGIES



**PRODUCTION AT** a major U.S. chemical plant was unexpectedly shut down for two hours in March 2003, causing significant financial loss to the company. The root cause analysis indicated that the incident started when a control room operator's computer was restarted with a changed IP address. This new IP address duplicated an address already assigned to an analyzer used for continuous emissions monitoring and the analyzer locked up as a result of network error messages. While the individual responsible for altering the IP address was never officially identified, it was reported that the address was changed so that the operators could play computer games from the control room.

This is an example of a typical security incident in the chemical processing world. There were no evil hackers involved — only employees who, while probably violating company policy, weren't being malicious. Yet the impact from this insider threat was significant.

Interestingly, the company had a sophisticated firewall in place, based on a common strategy known as the Bastion model, where vulnerable systems are hidden behind a single firewall. Unfortunately, this design couldn't prevent the incident because the problem originated from inside the control system, completely bypassing the firewall.

#### IT LIMITATIONS

A number of security mistakes allowed this event to occur. First, there was an over-reliance on the Information Technology (IT) department to provide security for systems generally not in its area of expertise or under its control. IT departments are very good at providing security for systems they understand, such as Windows servers and accounts-receivable databases. Unfortunately, in most chemical companies, the critical control systems that run the processes day in and day out are strange and forbidding beasts to the IT professional.

Many process control systems have unusual operating systems and applications such as VxWorx or RSLogix that differ significantly from typical IT operating systems and applications. This means that many of the tried-and-true IT security solutions won't function correctly or, if they do run, will interfere with the process systems.

A good example of this was reported at an ISA Industrial Security Conference in Philadelphia a few years ago. When an emergency shutdown system on a boiler failed to correctly operate, investigators discovered that anti-virus software had been installed on the computer used to configure the safety system. This software blocked the proper operation of the safety system, putting the entire plant at risk. There was nothing wrong with the safety system or the anti-virus software on their own, but together they made a life-threatening combination.

At the core, the goals of IT security differ from those of the process control world. The IT security manager sees data confidentiality as paramount (don't let those credit card numbers be stolen) while the plant manager focuses first and foremost on human and plant safety. These differences in goals translate into huge differences in acceptable security practice. For example, using standard password lockout procedures just isn't acceptable for most operator stations in plant control rooms — the default needs to be access for the operator, not lockout, the opposite of the IT assumption. Imagine the impact if, during a chemical reactor emergency, the operator panics and misspells his password three times, causing the console to lock out all access for the next 10 minutes. Password lockout is considered good policy for protecting IT servers but certainly isn't going to work in the control room of the average chemical facility.

This isn't to say that IT security solutions are bad for chemical processing. In fact, studies at major oil companies have shown that 90% of all IT security policies and technologies work well for industrial process control. The answer lies in clearly understanding how chemical processing assumptions and

### Attack routes taken

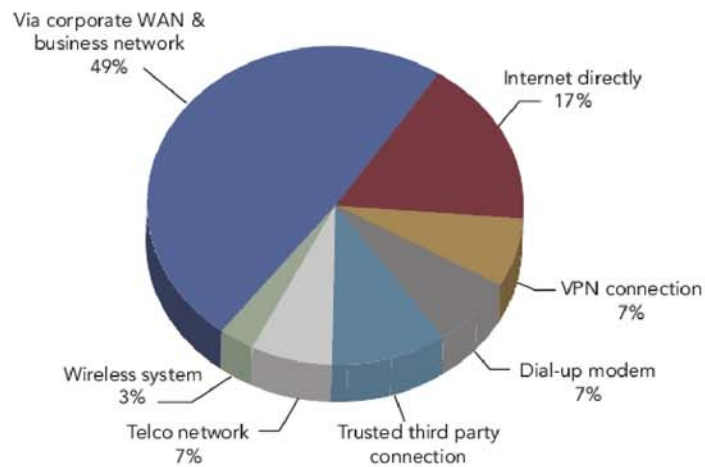


Figure 1. In 75 incidents from 2002 to 2006, attackers and viruses infiltrated via corporate networks most often but far from exclusively. Source: *Industrial Security Incident Database, June 2006.*

needs differ from those of the IT world and then modifying the IT security technologies and practices to properly use them in our world. This takes close cooperation and teamwork from both IT and process control staffs and not blind dependence on IT security procedures, a topic we'll explore in more detail later.

The other mistake the chemical company made was to assume that all security problems arise from outside the plant and those that do make it in come through obvious pathways that can be managed by a firewall. This assumption often means that companies base their entire plant-floor security solution on a single firewall between the business network and the control system network, believing that their firewall will be the ultimate security filter and will prevent anything evil from ever getting to the control system. Unfortunately as this chemical company discovered, nothing could be further from the truth.

This firm isn't unique. Many chemical companies make significant cyber-security mistakes. The sidebar summarizes the 10 most common errors.

#### MULTIPLE PATHS FOR ATTACK

To understand just how many pathways into a control system there can be, consider the security incidents caused by the Slammer Worm since its creation in 2003. This particular worm has resulted in more documented process disruptions than any other source, according to the Industrial Security Incident Database records. A few of its "achievements" include interrupting power-distribution supervisory control and data acquisition systems, infecting the safety parameter display system in a nuclear plant and curtailing oil operations in the Gulf of Mexico.

What's particularly interesting is that the Slammer Worm has used at least five different pathways to get to its control system victims. In one case, it

#### THE 10 MOST COMMON PLANT CYBER-SECURITY MISTAKES

1. Assuming that someone else (like the IT department) is looking after the security of control systems. It often turns out that everyone thinks it's someone else's job. (Upper management is especially prone to the mistake.)
2. No risk analysis for cyber incidents. Without a proper risk analysis that looks at vulnerabilities and consequences of cyber events, companies can't be sure they are spending their security dollars effectively.
3. A lack of policies and procedures to govern control system security. Security needs to be motivated from the top down by good corporate policies that are supported by upper management.
4. Assuming that IT security solutions will work on the plant floor. Security solutions need to fit the environment that they're to be used in or they either will get ignored or bypassed. Many IT solutions work well but some don't; it's important to recognize those that don't work and come up with alternatives.
5. Addressing security on a piecemeal basis. For security to be effective, it has to be deployed in a coordinated fashion across the whole plant or organization.
6. Forgetting the human aspects of security. Good security starts with ensuring that staff, management and contractors understand and follow appropriate practices.
7. Designing control system networks without sufficient defense-in-depth architectures. Depending on a single firewall between business and control systems is asking for trouble — security needs to be layered to be effective.
8. Poor patch management for applications on the plant floor. Many companies have good patching systems for the operating system but then forget to patch the software applications (like HMIs), which typically are far more vulnerable to software bugs.
9. Either no tools to detect inappropriate activity on the control system or no procedure to ensure that the tools are used regularly. I see many firewalls in plants whose logs never have been checked. This is like installing a burglar alarm but not turning it on.
10. Allowing remote access to the control system without creating and enforcing an appropriate access control system. Need I say more?

entered a petroleum control system via a maintenance laptop that was used at home, infected there and then brought into the plant. In another case, it contaminated a paper machine human/machine interface (HMI) via a dial-up modem for remote support. In a third case, it passed through a poorly configured firewall. In a fourth case, it took advantage of a temporary Internet connection set up by a contractor — involving a remote virtual private network for system maintenance — that bypassed the IT firewall. In all these

examples, firewalls were in use but the worm bypassed them or exploited a flaw in the firewall's deployment.

Many chemical industry managers find the number and variety of pathways into their control systems hard to believe. However, this information has been corroborated by the 2006 Process Control Security Forum (PCSF) keynote presentation and a 2007 ARC Advisory Group survey. The PCSF paper reported that at a large oil company 80% to 90% of all control networks were connected to the enterprise network, which, in turn, was hooked up to the Internet. ARC canvassed control engineers about the types of connections that their automation networks had to the outside world. Only 17.5% reported no connection. Indeed, ARC found an extensive number of hookups:

- 47.5% to a company intranet/business network;
- 42.5% directly to the Internet;
- 35% to direct dial-up;
- 20% to wireless modems; and
- 8% with other connections.

Notice the percentages add up to far more than

100%, indicating that many control-system networks had multiple connections.

These secondary pathways can have a huge impact on plant security. An analysis of 75 control-system security incidents between 2002 and 2007 showed that more than half of the attacks came through secondary pathways such as dial-up connections, wireless systems and mobile devices (Figure 1).

This indicates that chemical companies are missing or at least failing to adequately secure numerous pathways into their control systems (Figure 2). Many are human pathways such as contractors' laptops, USB drives and inappropriate employee behavior. Others are communications systems that aren't based on the typical local area network technologies — e.g., serial and telephone connections to remote process equipment, modems and wireless systems.

The only solution is to conduct a thorough analysis of all pathways into the chemical process systems. Often this can result in some big surprises. A 2005 survey of a U.S. refinery that I directed uncovered 17 different pathways — site management had believed there was only



Emergency • Planned • Supplemental • Turnaround • Pilot Plant

# Rental Cooling.

For Chemical Process Applications

## Rental Cooling



Chillers • Cooling Towers  
Pumps • Heat Exchangers  
Tanks • Air Conditioners  
Air Handlers • Dehumidifiers  
Heaters • Boilers • Generators

800-586-8336

CarrierRentals.com

**We keep process lines running at peak capacity.**

Our engineers speak your technical language and can help you solve your temperature control problem.



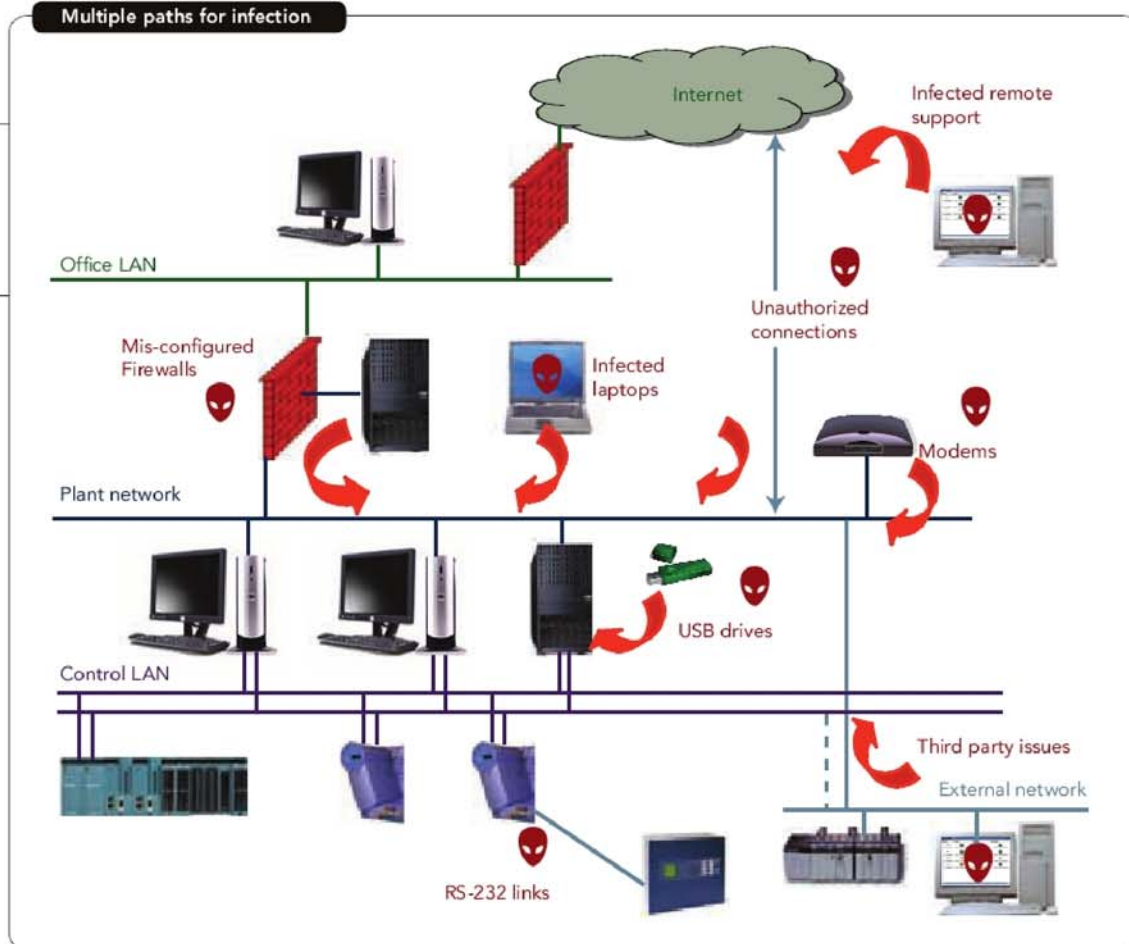
**Rental Systems**

We are the rental cooling, heating and dehumidification experts.



### Multiple paths for infection

Figure 2. Most chemical plants suffer from a wide variety of vulnerabilities.



one control-system-to-business link. Once a complete list has been compiled, each pathway should be analyzed for its potential security impact. Assuming “no hacker would use that pathway” isn’t a route to good security.

#### EASY TARGETS

Once a misguided employee, virus or hacker does get past the main business or control-system firewall, the typical control system is an easy target for attack. Poorly patched Windows-based computers abound and anti-virus software is the exception rather than the rule. For example, during a security survey conducted at a major refinery we discovered that only 55% of the Windows 2000/XP machines in control rooms had the patch that prevented Blaster infections and even fewer, 38%, had the patch for the Sasser Worm installed. Yet both of these patches had been available for more than two years and were approved by the control system vendor at the time of the survey. Even the most inexperienced hacker could have taken over this control system in a matter of hours.

A typical plant’s actual control devices such as the programmable logic controller (PLC) or distributed control system (DCS) are even softer targets than unpatched PCs. In a study by CERN, Europe’s laboratory for high energy physics, 25 industrial control devices (mostly

PLCs) were tested using standard IT security tools (such as Nessus and Netwox) that are available to the average attacker. Almost half of the devices failed the tests, usually due to communications breakdowns, system crashes and unprotected services. For experts in the field these results weren’t all that surprising — the majority of PLCs and DCSs currently in use offer no authentication, integrity or confidentiality mechanisms and can be controlled by anyone who can “ping” the device. Nor can they be easily updated or have security features added to them.

#### DEFENSE IN DEPTH

Sound strategy, regardless of whether it’s for military, physical or cyber security, relies on “defense in depth.” Effective security is created by layering multiple security solutions, so that if one is bypassed, another will provide the defense. This means not over-relying on any single technology such as a firewall. Firewalls aren’t bad technology — in fact they’re a fantastic tool in the security tool box — but industry has misused them by believing they will solve all security ills.

Defense in depth begins by creating a proper electronic perimeter around the control system and then hardening the devices within. The security perimeter for the control system is defined both by policy and

technology. First, policy sets out what truly belongs on the control system network and what's outside. Next, a primary control-system firewall acts as the choke point for all traffic between the outside world and the control system devices.

Once the electronic perimeter of the control system is secured, it's necessary to build the secondary layers of defense on the control system itself. Control components like HMIs and data historians that are based on traditional IT operating systems such as Windows and Linux should take advantage of the proven IT strategies of patch and anti-virus management. However, this requires prior testing and care.

For devices like PLCs and DCS controllers where patching or anti-virus solutions aren't readily available, I suggest an industrial security appliance. This rapidly evolving security solution deploys low-cost security modules directly in front of each control device(s) needing protection (Figure 3).

#### PEOPLE FIRST, NOT TECHNOLOGY

Despite the razzle-dazzle of these technological solutions, it's important to consider the human aspects of security such as developing policy, assigning responsibility and training staff. It's this human part of the equation — not the technology — that's most critical to the success of any security program.

Three factors are critical for the successful implementation of a security program within a chemical facility:

1. security policy, objectives and activities that reflect business goals;
2. an approach and framework for implementing, maintaining, monitoring and improving information security that's consistent with the organizational culture; and
3. management's visible support and commitment.

If any of these are missing, then the security program will likely fail.

Finally, IT managers and plant managers face a common enemy attacking related technologies in what has become a highly interconnected environment. This demands developing a coordinated defense. It can be valuable to:

- establish cross-department training programs that focus on values and behaviors expected, to foster a culture of co-operation and communication;
- create cross-functional teams to develop policies, standards and projects for process security; and
- encourage informal networks. These are important. When a real problem arises, provide opportunities for people from both the process and IT departments to liaise and work together.

Local security appliance



Figure 3. Low-cost modules are designed to protect individual control devices. Source: MTL Instruments.

#### ADDRESS THE THREATS

These are just a few of the most important steps that the chemical industry needs to take to effectively protect itself from cyber attack. Failure to adapt to changing threats and vulnerabilities will leave companies exposed to increasing numbers of cyber incidents. The consequences unfortunately could include a marred reputation, environmental releases, production and financial loss, and even human injury or death. ●

**ERIC BYRES, P.E.**, is chief technical officer of Byres Security Inc., Lantzville, B.C. E-mail him at [eric@byressecurity.com](mailto:eric@byressecurity.com).

#### RELATED SECURITY RESOURCES ON CHEMICALPROCESSING.COM

- Feel Secure about Vulnerability Assessments, [www.ChemicalProcessing.com/articles/2008/042.html](http://www.ChemicalProcessing.com/articles/2008/042.html)
- Become a Cyber Security Pacesetter, [www.ChemicalProcessing.com/articles/2007/186.html](http://www.ChemicalProcessing.com/articles/2007/186.html)
- Plug Cyber Security Gaps, [www.ChemicalProcessing.com/articles/2007/152.html](http://www.ChemicalProcessing.com/articles/2007/152.html)
- Properly Protect Control Systems, [www.ChemicalProcessing.com/articles/2007/104.html](http://www.ChemicalProcessing.com/articles/2007/104.html)
- Get Ready to Comply with New Security Mandates, [www.ChemicalProcessing.com/articles/2007/095.html](http://www.ChemicalProcessing.com/articles/2007/095.html)

#### OTHER ARTICLES BY ERIC BYRES:

- Wolves at the Door(s) of the House of Straw, [www.ControlGlobal.com/articles/2007/449.html](http://www.ControlGlobal.com/articles/2007/449.html)
- Wolves at the Security House Door(s), Part 2, [www.ControlGlobal.com/articles/2008/017.html](http://www.ControlGlobal.com/articles/2008/017.html)
- Making Cyber Security Work in the Refinery, [www.isa.org/Template.cfm?Section=Technical\\_Information\\_and\\_Communities&template=/ContentManagement/ContentDisplay.cfm&ContentID=64756](http://www.isa.org/Template.cfm?Section=Technical_Information_and_Communities&template=/ContentManagement/ContentDisplay.cfm&ContentID=64756)