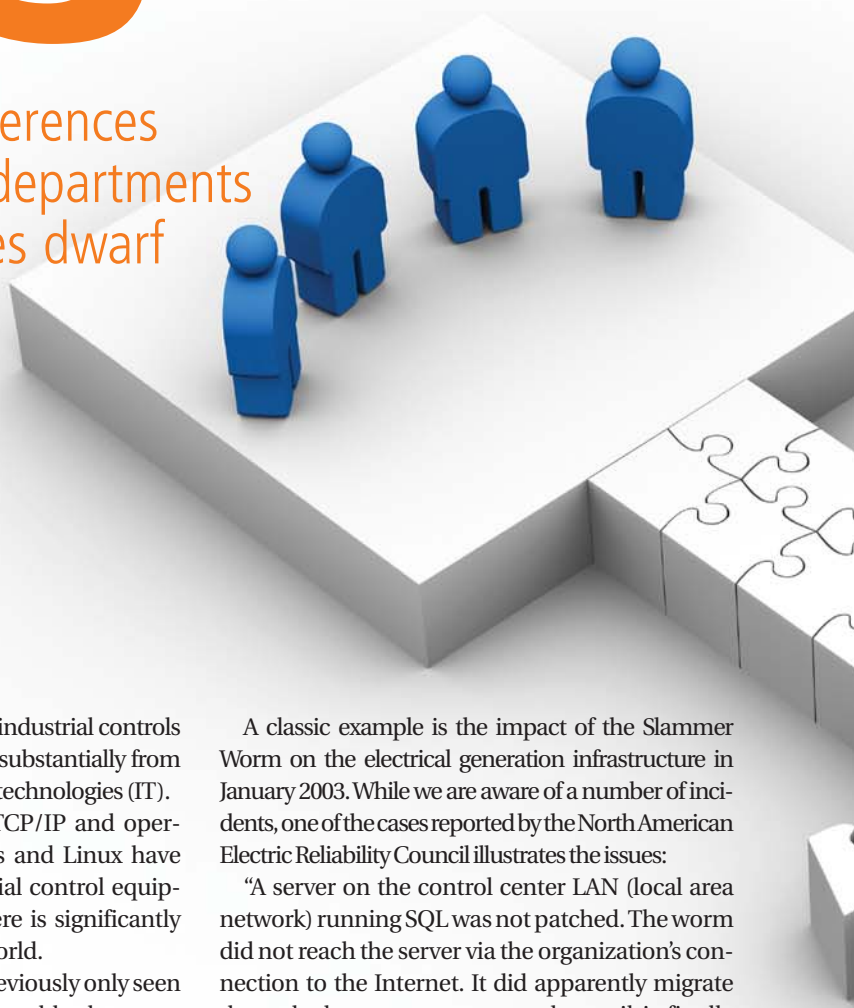
Forget the silos, build the Bridges

There are acknowledged differences between the IT and control departments but they are small; similarities dwarf differences

By Eric Byres, Jim Bauhs, and Brian Mason



Over the past 10 years, the industrial controls (IC) world has borrowed substantially from the world of information technologies (IT).

Protocols like Ethernet and TCP/IP and operating systems such as Windows and Linux have made the interfacing of industrial control equipment much easier, but now there is significantly less isolation from the outside world.

Network security problems previously only seen in the business network and the world at large can be passed onto process and supervisory control and data acquisition (SCADA) networks, putting industrial production and human safety at risk.

Similarly, network security incidents on the plant floor can travel back up into the corporate environment, creating the possibility of considerable business disruption.

At the same time, a core of our information infrastructure—the network—has come under increasing attack from a wide variety of sources, ranging from teenagers on a cyber joyride to professional hackers.

A classic example is the impact of the Slammer Worm on the electrical generation infrastructure in January 2003. While we are aware of a number of incidents, one of the cases reported by the North American Electric Reliability Council illustrates the issues:

"A server on the control center LAN (local area network) running SQL was not patched. The worm did not reach the server via the organization's connection to the Internet. It did apparently migrate through the corporate networks until it finally reached the critical SCADA network via a remote computer through a VPN (virtual private network) connection. The worm propagated, blocking SCADA traffic."

Here we have a worm designed to attack a business application (SQL-Server) and propagated over a non-control media (the Internet) impacting a critical SCADA system because:

a) IT products like SQL-Server have become an integral part of the plant floor.

b) A close coupling of Internet, business, and control networks now exists.

In themselves, these two conditions are not bad—the shared components, protocols, and manufacturers have created greater synergy, lower costs, and freer access to information for both IT and IC members. However, without improved security practices on all sides, the price for these gains may be unacceptability high.

Where does one start when attempting to improve the security of the plant floor from these threats from outside world? We believe the only technique with a high chance of success is a highly coordinated effort by both IT and IC, and this paper will look at techniques that can make this possible.

Blaming the wrong people

The ultimate goal of improved security is a shared goal, menace is a combined threat to all, and most of the technologies are common technologies. Thus, it is reasonable a harmonized IT/IC defense is appropriate.

Unfortunately, this is often the exception rather than the rule. As we have visited various companies around the world, we have seen a wide range in the attitudes and level of cooperation between IC and IT departments.

In a few exceptional companies, there was a spirit of cooperation and understanding between these departments. In other companies, we witnessed considerable animosity as each department saw the other as an adversary. Their attitude was there is an impending collision between IC and IT and one group would win and the other would lose.

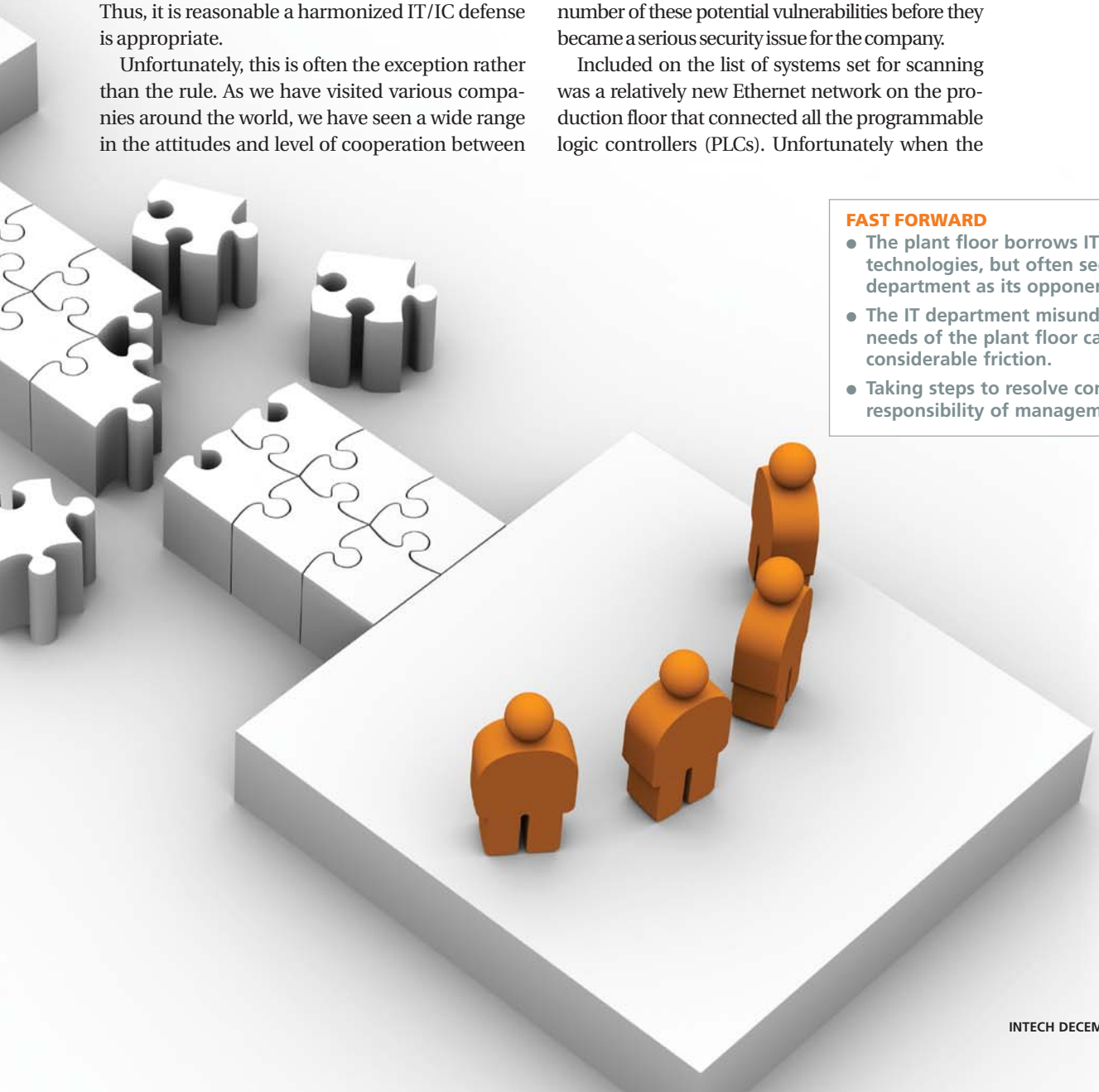
In most cases, there was a lack of communications between departments that impeded effective cooperation. The result of this lack of communication can be disastrous.

In 1995, the IT department at a major food products manufacturer decided to hire a consultant to scan all the corporate computer systems for possible security vulnerabilities. This was a commendable and forward-looking decision as the risks from software bugs and misconfigured systems were just beginning to hit in the IT world. The scan would likely identify a number of these potential vulnerabilities before they became a serious security issue for the company.

Included on the list of systems set for scanning was a relatively new Ethernet network on the production floor that connected all the programmable logic controllers (PLCs). Unfortunately when the

FAST FORWARD

- The plant floor borrows IT technologies, but often sees the IT department as its opponent.
- The IT department misunderstands the needs of the plant floor causing considerable friction.
- Taking steps to resolve conflict is the responsibility of management.



scanner software sent out a certain class of ICMP Redirect messages all the PLCs crashed, resulting in reported production losses exceeding $1 million dollars.

One can easily imagine the animosity an event of this nature might have created between departments. IT's actions were well intended and did highlight a serious vulnerability in the PLC system, one that could have been exploited later by an attacker with malicious intent.

Unfortunately, because of poor understanding of the environment and needs of IC department, this useful information sank in sea of acrimony. Equally important, the IC department failed to educate the IT department to the needs and conditions of the plant floor.

The common enemy

Blaming each other for security issues is missing the point—the enemy is not the other department, but the hacker or virus attempting to infiltrate the company systems.

It is easy to point the finger at the other business unit for security issues, but it is certainly not helpful in reducing the risk. The existence of numerous common technologies means the enemy is not unique to either the IC or IT environments; it is a common and shared adversary.

For example, a Denial of Service (DoS) attack against a business server is likely to be just as devastating against data historian server on the plant floor.

Similarly, a poorly configured modem is a security risk whether it links to the president's laptop or the desktop computer of an instrument mechanic.

Furthermore, regardless if security incidents are the result of ignorance or intentional acts, the basic outcome is the same—potential loss to the company that can affect everyone.

The severity and nature of the loss may vary between IT and IC. For example, a DoS attack launched against a key business network may result in loss of sales, while the same DoS attack against a process network may result in loss of production. The result, however, is the viability of the company and livelihood of its employees are at stake.

This is especially true as companies require more cooperation and information sharing between departments. The integration of IC and IT has joined environments that in the past enjoyed the benefits of separation and insulation from each other. Not only did this insulation separate the two environments from each other, it also provided a physical barrier (i.e. air gap) from the distinct threats previously unique to each. The very organizations we support are at greater risk with this increased integration.

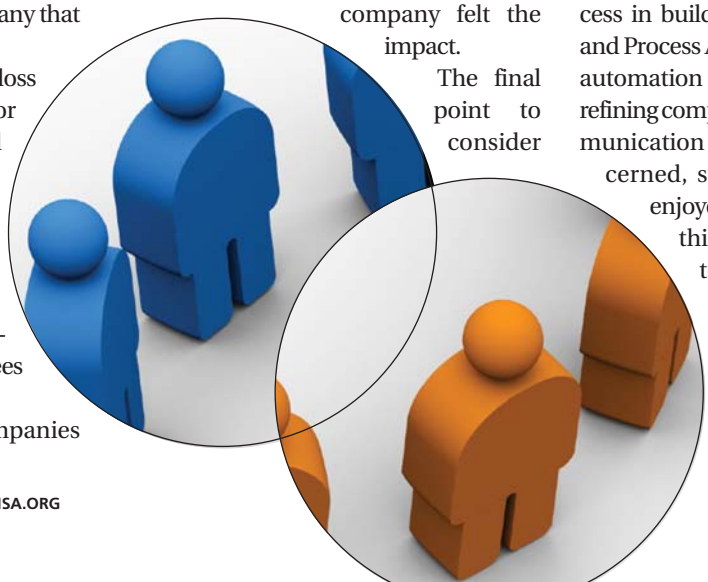
It is easy to point the finger at the other business unit for security issues, but it is certainly not helpful in reducing the risk.

The cyber sabotage of a prominent manufacturer of measurement and control devices is a fine example. This leading manufacturer suffered losses of over $10 million when a terminated network manager detonated a software time bomb he had previously planted in the network he helped create. The bomb paralyzed the company by destroying the programs and code generators used by the manufacturing equipment to produce the company's 25,000 different products.

The incident led to 80 staff losing their jobs, while the company lost its competitive footing in the instrument and measurement market.

The lesson from this incident is while the culprit was a disgruntled ex-staff member from the IT department, his target was the plant floor, and employees throughout the company felt the impact.

The final point to consider is the threats to security do not acknowledge the boundaries that exist from a corporate viewpoint. A hacker looking for a weakly secured workstation inside a company will not care whether it sits on a business or a process network, as long as it provides a foothold into the corporate systems. A piece of malware (i.e. a virus or worm) does not know about the political or departmental divisions inside a company; it simply seeks a suitable target for infection.



Building bridges, not silos

There are plenty of examples of what can go wrong in IT/IC security cooperation and of the subsequent consequences.

However, in preparation for putting this piece together, we also saw many organizations where healthy bridges between groups existed and security was clearly improved.

What was it that made the difference between an open bridge versus two silos in terms of IC/IT security cooperation?

To help answer this question, we conducted interviews with experts representing process control industries that included chemical, electric, oil and gas, utilities, and others. The roles of the people we talked to ranged from trades people to executive directors working in both IT and Process Control departments.

Several companies operating in both Canada and the U.S. spoke about the involvement of their senior leadership team and how this has been instrumental in creating trust between people and departments.

Over time, this has had the effect of creating unique cultures that have contributed to producing positive bottom-line results.

One company has had significant success in building bridges between the IT and Process Automation groups. A former automation group supervisor at a large refining company noted that as far as communication and cooperation was concerned, staff at the local levels had enjoyed a relatively good level of this because they worked together daily. People knew each other, and there was a trust built up between them. Unfortunately, at the corporate level, getting the same degree of interaction

between different departments was more difficult.

Top management recognized the need for better communication and cooperation at the corporate level between IT and process control groups in order to protect the business. With that important goal in mind, they launched a pilot meeting to bring the two groups together in the same room, at the same time, to focus on this single important issue.

However, while the subject matter was the main focus for the meeting, he stated, "We took time to learn about each other's needs and to also get to know each other. We could put a face to a name or a voice. Once we had this, we were able to sit down to educate and influence each other. There was a tremendous amount of positive discussion as we started to see each other's world."

One of the tangible outcomes from that meeting was a commitment by the groups to collaborate to improve the business. The first project was jointly developing policies and standards. Because of the first meeting, a culture of cooperation between the groups has continued to develop.

At The Dow Chemical Company, there has been a long history of IT and Engineering working together, said Eric Cosman, Engineering Solutions Architect.

Five years ago a group of managers went to a meeting called by the CIO and the VP of Engineering. The purpose of the meeting was to identify opportunities to improve the way the two departments worked together.

As Cosman said, "It was clear that we had to work together, and so we started to talk to each other." From there, with the top-level support in place, the partnership resulted in a trickle down effect.

There were more joint meetings and collaborative efforts between the departments. Cosman said there was a greater appreciation that the groups were in it together.

He quipped, "We have an informal saying here. There is no hole in just your end of the boat."

To make the partnership between Engineering and IT work, senior leaders recognized there was a need to invest in relationship building. They looked for solutions that would create the framework for sustaining their culture of cooperation.

Dow offers an internal course called "Creating Strategic Partnerships." This is a two-day course offered by Human Resources and delivered by line managers. All members of the Engineering function take the course. Many of those in IT take it as well.

There are three foundational values that create the platform for working between the two groups. There must be shared vision, shared power, and shared accountability.

Cosman said the workshop "… is an example of not only talking about the partnership but also about living it." He also said, "There is no formal way of measuring success, but it is easily seen in the behaviors of the people here. The real problems between IT and Engineering groups are not about re-assigning people or re-structuring but about culture, behaviors, and people's individual points of view."

"Not all disconnects between IT and Process Control are the result of conflict and tension. They can also come from 'innocent' mistakes," noted a well-known control systems engineer who works for a large chemical company.

The engineer reported an incident

TERMINOLOGY

Malware: Malicious software is a program or files that damage or disrupt a system, such as a virus, worm, or a Trojan horse.

DoS: Denial of service is an attack on a site or service that overwhelms a web site's servers with requests or messages thereby preventing users from making legitimate requests and effectively disabling the site.

SQL: Structured Query Language is syntax for defining and manipulating data from a relational database. Developed by IBM in the 1970s, it has become an industry standard for query languages in most relational database management systems.

VPN: A virtual private network is a form of communication over networks that are public in ownership, but emulate a private network in terms of security.

where an IT employee attended a vendor seminar and came back eager to implement a wireless solution to extend wireless services to conference rooms in a plant location so people could use their laptops wirelessly. What the IT employee did not know was there was already an existing wireless instrumentation application in place on the plant floor. The good news was the employee's action came from a place of wanting to give good customer service to the people on the plant floor. The bad news was his execution had flaws within since there were serious channel conflicts and bandwidth limitations between the IT wireless system and the wireless instrumentation application.

Do we need senior leadership?

While having top down approval at the corporate level both makes sense and allows for implementation, there have been other successes without this level of support.

A Fortune 10 telecommunications company did this when three regional leaders representing National Operations, Network Operations, and Network Engineering decided to come together. These regional leaders had been given conflicting objectives by corporate with little or no room to negotiate.

The three groups were distinct, and yet their successes were not independent of one another and, indeed, depended on each other's performance. As in many other companies, there was little room to negotiate with upper management's expectations, and so they were stuck with each other. Normally there might be the usual turf wars. However, these three leaders decided they would do the unusual: They would look for ways to cooperate with each other.

Their leadership and commitment culminated in what they informally referred to as the two-day Back Scratching session. Fifty-five second level supervisors, directors, and executive directors came together to listen to each other, vent their frustrations, and eventually create solutions. The ground rules were simple: For each department to win, each of the departments had to be willing to give something or give up something in order to get something in return.

There was a critical moment in the meeting late in the afternoon of the first day. The three leaders realized their people were sitting on the surface and they were not discussing the real issues. If they did not get busy with the real issues, the meeting would be a waste of time, and they would be no further ahead in addressing their business needs. With the aid of a skilled facilitator, the leaders called the group on their concerns and over the next two hours invited people to get things off their chests. Tempers came to the surfaces, people challenged assumptions, and folks began to listen and understand the other side's problems. This venting and the encouraging handling of it created a safe place for the conflicted groups to talk and then start

working together on developing solutions that were within the control of the people in the room.

For organizations looking to make headway, there are several suggestions to consider:

- Conduct annual staff surveys that measure elements of cooperation between the groups such as utilization of resources, trust and conflict, clarity of goals and objectives, controls and procedures, and the like.
- Develop cross-department training programs that focus on values and behaviors expected in order to foster a culture of co-operation and communication.
- As part of a formal talent management program, place high talent performers in the various departments. Most successful leaders are those who have worked both sides of the fence. This can also be a design element for a college graduate after entering the organization.
- Create cross-functional teams to work on developing policies, standards, projects, etc. Imbedded in this is metrics for both completing projects and for the quality of collaboration used to develop and execute the project.
- Informal networks are important. In the context of a real problem, create opportunities for people from the different departments to network and work together.
- Finally, there is something each person can do to improve and maintain effective relationships. Be willing to make the effort to reach out to the other side and be willing to walk in their shoes.

In conducting the interviews, there was one thing that virtually everyone agreed on: Trust is ultimately the crucial factor in creating great working relationships.

Conflict and misunderstandings are a part of life and a part of working together. Taking the first steps to resolving conflict is ultimately the responsibility of leadership.

It is clear IT and IC face a common enemy attacking similar technologies in what has become a highly interconnected environment. The key is to develop a coordinated defense involving both IT and IC.

The solutions to address a specific risk are far more likely to have a common approach rather than two completely different technologies or techniques for the two settings.

As well, the increasing dependence and connectivity between IC and IT means there are numerous opportunities to both collaborate and learn from each other.

RESOURCES

Uncovering Cyber Flaws
http://www.isa.org/intech/060002

Can't happen at your site?
www.isa.org/link/BlkHat0202

ABCs of Industrial Network Security
www.isa.org/link/ABC_Sands

ABOUT THE AUTHORS

Eric Byres (eric@byressecurity.com), **Jim Bauhs** (jim_bauhs@cargill.com) and **Brian Mason** (brian.mason@masoncg.com) spoke about security, networks, and hacking defense strategies at ISA EXPO 2007 in Houston.

View the online version at www.isa.org/intech/20071205.