THE BUSINESS CASE FOR CYBER SECURITY

What's this about in a nutshell? The importance of cyber security for manufacturing and computer control systems has only recently been recognized and therefore has not yet been addressed by industrial companies. Appropriate security measures must be taken to avoid events which could have impacts as tragic as those of September 11, 2001. Lesser cyber attacks have already occurred. Action is needed now to deal with this threat.

What's the issue? The process industries have invested considerable effort in managing the risks of terrorism and other deliberate criminal acts against facilities since the events of September 11, 2001. However, these efforts have focused primarily on physical security and have not dealt with attacks on facilities through their computer systems. While few deliberately focused attacks on manufacturing systems have been reported, random attacks of worms, trojans, viruses, etc. have occurred and they have adversely impacted computer systems including those operating manufacturing facilities.

Hasn't the IT department already dealt with this issue? No. While cyber security is an established discipline for computer systems used for business management, it deals with the protection of valuable information stored on those systems from adversaries who want to obtain, corrupt, damage, destroy or prohibit access to it.

Cyber security for process plants includes protection against cyber or physical attack on computer systems and their support systems by adversaries who wish to disable or manipulate them to cause harm. Examples of manipulation include opening/closing valves, starting/stopping equipment, and overriding alarm and trip settings. Traditional IT cyber security countermeasures are not adequate to protect against attacks on control systems. Furthermore, such countermeasures may compromise the safety or operability of the process.

Safety and security are simply good business.

Why can computer control systems be attacked? Historically, computer control systems have been kept separate from business and enterprise computer systems but increasingly they are being connected through networks, driven by the need to communicate process information to business groups and the opportunity to intervene in manufacturing processes through an intranet or the Internet.

Process control systems are exposed to penetration when they are connected to other networks or when there are provisions for remote access. Existing control systems were not designed with public access in mind, often have poor security, and are vulnerable to

attack. Furthermore, much of the technical information needed to penetrate these systems is readily available.

Any link to a site on the Internet is a potential two-way street. Connecting control systems to networks or providing dial-up access without protection is like leaving the doors of your house unlocked. There may not be a problem immediately, but eventually the house will be burglarized or vandalized. These issues also affect other types of computer systems including communications, access control, inventory control, power, transportation, and financial systems, all of which are increasingly interlinked.

What are the consequences of cyber attacks? They can include:

- Release, diversion or theft of hazardous materials
- Employee and public fatalities, injuries and health effects
- Environmental impacts
- Violation of regulatory requirements
- Loss of proprietary or confidential information
- Process upsets
- Product quality problems
- Contamination of products
- Loss of production capacity
- Interruption of production
- Process shutdown
- Equipment damage
- Economic loss
- Societal impacts
- Loss of public confidence
- Impact on national security

Undesirable incidents of any sort detract from the value of a business, but safety and security incidents have negative impacts on all stakeholders - employees, shareholders, customers, and the communities in which a plant operates.

Is the risk real? In January, 2003, hackers released the Slammer worm. It penetrated a computer network at Ohio's Davis-Besse nuclear power plant and disabled a safety monitoring system for nearly five hours, despite a belief by plant personnel that the network was protected by a firewall. This event occurred due to an unprotected interconnection between plant and corporate networks. The Slammer worm had significant impacts on other companies. It downed one utility's critical SCADA network after moving from a corporate network to the control center LAN. Another utility lost its Frame Relay Network used for communications and some petrochemical plants lost HMIs and data historians. A 911 call center was taken offline, airline flights were delayed and canceled, and bank ATMs were disabled. These were the effects of the release of one *unintelligent* piece of malicious software. No specific facility was targeted.

In 2001, a cyber attack on a computerized waste treatment system by a disgruntled contractor in Queensland, Australia caused the diversion of millions of gallons of raw sewage into local parks and rivers. There is evidence that al Qaeda terrorists have investigated the availability of software and programming information for systems that run power, water, transport and communications in the US.

In September, 2001, a teenager hacked into a computer server at the Port of Houston, Texas in order to target a female chat room user following an argument. The attack bombarded computer systems used for scheduling at the world's eighth largest port. The port's Web service, which contained crucial data for shipping pilots, mooring companies and support firms responsible for helping ships navigate in and out of the harbor, was left inaccessible.

These events are just the beginning. Cyber attacks can be mounted with few resources other than brain power. Primarily, they require information, knowledge and the ingenuity to identify and exploit vulnerabilities. These resources are the principal weapons of many potential assailants and their numbers around the world are staggering. The failure susceptibility of PLC control systems due to simple, relatively low-volume denial of service attacks is well recognized. It is not a question of whether they will be attacked, only when. Some have dismissed such cyber attacks as defacing web sites, limiting access to popular sites, etc. as pranksterism or “weapons of mass annoyance”, but these attacks demonstrate the “proof of concept” for much more serious attacks.

Who will attack? Computer systems can be attacked from within a facility or externally, including attacks from outside the country. Data on cyber attacks indicate that about 70% of actual attacks are made by insiders. Attackers include:

- Thrill-seeking, hobbyist or alienated hackers who gain a sense of power, control, self-importance, and pleasure through successful penetration of computer systems to steal or destroy information or disrupt an organization's activities.

- Disgruntled employees, contractors or other insiders who damage systems or steal information for revenge or profit.

- Terrorists for whom hacking offers the potential for low cost, low risk, but high gain attacks.

- Professional thieves who steal information for sale.

- Adversary nations or groups who use the Internet as a military weapon for cyber warfare, a discipline the US has already engaged in itself. This threat is changing the nature of conflict as fundamentally as other technologies have in the past including gunpowder and nuclear weapons.

A strong safety and security management system is fundamental to a sustainable business model.

How will they attack? Insiders usually have legitimate reasons to use computer systems but they may misuse their privileges or impersonate higher-privilege users. Outsiders may use the Internet, dial-up lines, partner networks linked to your network, or physical break-ins to access a computer system.

Attackers may have specific objectives or they may simply want to penetrate a system. In the latter case they may cause harm deliberately or inadvertently as they explore the system.

Attackers exploit vulnerabilities using a variety of techniques and tools. Hackers originally were individuals with highly specialized and esoteric knowledge of computer systems. Consequently, they were few in number. However, some of these early hackers decided to make their knowledge available to others through the development and distribution of software packages that provide hacking tools. Some of these packages rival commercial software in their design and are essentially point-and-click applications. A number of them provide suites of hacking tools. Their availability has significantly increased the number of people capable of performing sophisticated hacking. The hacking community spends considerable time probing computer networks for vulnerabilities and will actually publicize them, for example, through chat rooms on the Internet.

What computer systems are at risk? Those used for manufacturing and process control, safety systems operation, facility access, information storage, and networks. Locations that need to be protected from physical and cyber attacks include computer rooms, server rooms, control rooms, motor control centers, rack rooms, and telecommunications rooms.

Safety and security performance is both a pathway to financial success and your license to operate.

What are the benefits and costs of cyber security? Responsible risk management mandates that this threat should be managed to protect the interests of employees, the public, the company, shareholders, customers, vendors, and our society. The potential costs of inaction dwarf the costs of action. Risk analysis enables costs and benefits to be weighed so that informed decisions can be made on protective actions. In addition to reducing risks, displaying responsibility helps companies in many ways:

- Increases employee morale, loyalty and retention
- Reduces community concerns
- Increases investor confidence
- Reduces legal liabilities
- Enhances your corporate image and reputation
- Helps with insurance coverage
- Assists investor and banking relations

Proactive measures by companies can also help forestall new and more prescriptive regulations that increase costs and impede business flexibility.

Can I afford to wait? No. Presently, it is likely there are more people trying to break into computer systems than trying to prevent intrusions. Fortunately, most potential intruders have not yet targeted manufacturing and process control systems. However, that is likely to change quickly.

Some organizations are already moving on the issue. ACC's Responsible Care Management System requires that member companies address cyber security. The Chemical Industry Data Exchange has reviewed a number of cyber security vulnerability analysis methods and made recommendations for their use. ISA is working on a standard for integrating cyber security into manufacturing and control systems.

DuPont reported that firewalls recently installed to separate manufacturing and process control systems from the business network successfully stopped the rounds of virus attacks that were prevalent in the Fall of 2003. No process control systems protected by a process control firewall became infected by the viruses that were common on Dupont's business network.

What can be done? Do the following:

- Add cyber security to your company's values.

- Ensure someone takes ownership of cyber security and hold them accountable.

- Immediately conduct a review or audit of your current cyber security measures. Implement obvious fixes.

- Follow up with a cyber security vulnerability analysis for a more complete identification of your vulnerabilities and recommendations on further corrective actions.

- Implement a cyber security management program, ideally by integrating it into your existing management systems for safety, quality, etc.

“As long as we turn off the computer, we’ll be protected from hackers.”