

Security Flaws

Security has always been a big issue with manufacturers, especially following the Sept. 11, 2001 attacks, and it is gaining even more attention as Election Day nears with fears terrorists will try something big in the days leading up to November 7. This got me to thinking about security in general as it pertains to manufacturers. I've read several different studies and surveys and listened to discussions the past several



months on security issues facing manufacturing. At a Honeywell users conference a couple of months ago, for instance, one of the main topics of discussion was security. There, retired Adm.

James Plehal of the Dept. of Homeland Security talked about how businesses, particularly manufacturers that produce volatile products, should help be the ears and eyes in the fight against terrorism. Plehal calls this effort the "new normal" and what he means by this is that security efforts should be part of the normal routine on how companies conduct business on a daily basis.

Honeywell's Process Solutions group is among the technology companies championing the importance of security within manufacturing, whether it's helping to conduct security assessments or installing a fully integrated security system.

According to the folks at Honeywell, security is a big issue, particularly among chemical plants where some 4,000 facilities have volunteered to undergo an audit of their security procedures by the Dept. of Homeland Security. The audits are expected to be finished by the end of next year.

Security threats, of course, come from a variety of places, but according to experts the most common security threat comes from within. But no matter from where it emerges, executives, including manufacturers, view security as one of the top, if not the uppermost concern on their minds today. In a study conducted by AT&T, Bedminster, N.J., in cooperation with the Economist Intelligence Unit, London, England, reveals 78% of corporate executives view computer security is now the single most critical component of corporate networks, surpassing network reliability. Basically, if the network isn't safe, it doesn't matter how reliable it is.

This position by executives of placing a secure environment above a reliable one stems from businesses wanting to open their networks to partners, customers, suppliers, and even mobile workers. An open system, however, poses dangers, particularly from cyber attacks.

The good news is there are plenty of companies out there like Honeywell and Siemens, Munich, Germany, that are experts when it comes to security in manufacturing operations. There are other places as well executives can turn to for help starting with the Dept. of Homeland Security, which has an entire division devoted to the security efforts of the business community called The Private Sector Office. This office works directly with individual businesses, trade associations, and other professional and nongovernmental organizations to share department information, programs, and partnership opportunities.

In addition, the Dept. of Homeland Security has created a vendor information site at <https://vendors.dhs.gov> to invite businesses in the emerging homeland security industry to submit details about information technology (IT) products and services for enhancing the security of the homeland. The department is launching this site to invite the submission of

Security threats, of course, come from a variety of places, but according to experts the most common security threat comes from within. But no matter from where it emerges, executives, including manufacturers, view security as one of the top, if not the uppermost concern on their minds today.

IT product and service descriptions with the potential to broaden the invitation to include all products and services. Homeland Security is also working closely with the Small Business Admin. and numerous high-technology associations to alert small and disadvantaged businesses of this opportunity.

As you can see, there are plenty of places to begin when it comes to security. I also want to make mention that our news section the Buzz (p17) is focused solely on security. Executive Editor Mark Emond provides a more detailed look at security issues facing manufacturers and what some of the experts say are the important trends in this area.

BUZZ

Security and Protectionism	Protectionist “Red Herring”	p.18
Plant Security	Security from What?	p.19

Plant Protection

When it comes to making sure a facility is secure from a variety of threats, manufacturers have stepped up their efforts and are making great strides in protecting their plants.

Manufacturers have always put safety and security at the top of their priority list but as the November elections near and threats of terrorist attacks increase, each is an added element to push companies even further in their security efforts.

When you start looking around for what other manufacturers are doing in the way of plant security, you might find details scarce. For obvious reasons, companies don't want to share what security measures they have implemented. But examples are out there. Dow Chemical, Midland, Mich., for example, recently implemented technology from Honeywell Process Solutions, Phoenix, Ariz., that integrates its existing Honeywell security measures with its human resources (HR) system from PeopleSoft, Pleasanton, Calif.

How it works is that when an employee at Dow Chemical is let go, their access to secure locations throughout the plant is immediately denied. For

example, there is no lag time between when someone hands in their access card and when it officially gets entered into the HR system notifying all that need to know that this person no longer has access to secure areas. This process is now done in realtime because Dow's access card readers, which are from Honeywell, are linked to the HR system.

ARC Advisory Group, Dedham, Mass., recently came out with a report on the types of areas manufacturers are addressing when it comes to security. Analyst Dick Hill writes, “What we found was that the full range of security aspects is indeed being taken with extreme seriousness. In some cases, the serious nature of the manufacturers' activities are being closely guarded for fear that the knowledge of exactly what they are doing could actually breach their security measures.”

Some general observations:

For most respondents, physical security measures are further ahead of their plans for cyber security.

For more than 60% of the respondents, fire and safety measures are considered completed.



Also considered complete or nearly complete are perimeter security and access control.

Surveillance measures are planned for most respondents, with about one-third indicating they have completed all sites, and another third indicating they have completed some of their sites.

About one-third of respondents indicated they saw no requirement to integrate plant security with plant automation systems, but about 40% said they have either completed this for all or some of their plants, indicating that it was important to them.

Many other observations are too detailed to report here. A couple of recommendations are:

- Developing a central point of responsibility for all security issues should be a high priority.
- Seek out firms specializing in security.

—Mark Emond

Protectionist ‘Red Herring’

All manufacturers will likely have heard by now arguments against the U.S. Dept. of Homeland Security (DHS) awarding contracts to offshore companies. Some of the opposition comes from companies opposed to U.S. com-

and a research assistant, have taken issue with the opposition. They contend, “Applying protectionist policies to homeland security would only work to compromise America’s security. DHS’s goal when awarding contracts should be

“This robust performance—particularly when compared to the economic stagnation and high unemployment rate in Europe—can be attributed to U.S. reliance on the free market to allocate resources.”

“Applying protectionist policies to homeland security would only work to compromise America’s security. DHS’s goal when awarding contracts should be to obtain the best security for the dollars invested.”

—The Heritage Foundation

panies that relocate offshore, particularly in the Caribbean, to escape high U.S. tax burdens. This is called inversion or expatriation.

Opponents express fear that the foreign company could be secretly working against U.S. interests, but the real reason is that the expatriated companies are avoiding taxes that other businesses and the people have to pay, and thereby gaining an unfair competitive advantage in the marketplace.

Some companies that have inverted are Ingersoll-Rand, Accenture, Tyco, Cooper Industries, McDermott Intl., Nabors Industries, the Noble Corp., and Foster-Wheeler. They have dissolved their U.S. charters and reincorporated in low-tax jurisdictions like Bermuda and the Cayman Islands.

The issue came to a head when Accenture LLP, New York, N.Y., the U.S. subsidiary of Accenture, Hamilton, Bermuda, was awarded a DHS contract to implement a new U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT). Cable network CNN devoted a program or two, “Exporting America,” to the subject. The fear generated by the subject is amplified by high-light job losses to overseas companies.

Four analysts of The Heritage Foundation, Washington, D.C., three PhDs

to obtain the best security for the dollars invested.”

They point out that Accenture is not expatriated, but rather is a set of foreign partnerships that chose Bermuda as a home base for purposes of incorporation. The American company, Accenture LLP, which received the contract, will do all the work, and the dollars and tax revenues generated will remain in the United States.

Further, “Accenture LLP met all of DHS’s legal requirements for the US-VISIT bid and was awarded the contract based on its ability to do the job.”

The authors argue that the ability to contract outside the United States benefits the American economy and national security. They say more Americans are employed today than ever before—a record high of 139 million workers, as reported by the U.S. Bureau of Labor Statistics.

The unemployment rate has dropped for one year and is steady at a low 5.6%—“all the more impressive because the American workforce has grown by 2.84 million people since late 2001.

The authors state, however, that the U.S. high corporate tax rate and the taxation policies worldwide simply make it difficult for corporations chartered in the United States to compete overseas. The federal government imposes a 35% tax on corporate income and states take another 5% (on average)—the second highest total in the industrialized world.

Additionally, U.S.-chartered firms must pay tax to the Internal Revenue Service on income earned in other countries, in addition to the local corporate tax. Worldwide “territorial taxation,”

taxing only income earned inside their borders, puts American companies at a tax disadvantage.

The Heritage Foundation study concludes that protectionist policies should not be applied in investments in homeland security,

but DHS should ensure that its contracts outline stringent security and data-protection requirements.

DHS should also insist that contract work is conducted in countries that have a cooperative relationship with the United States across a broad spectrum of security initiatives.

The authors conclude that the homeland-security argument against outsourcing is a red herring that implements protectionism and would harm the economy and impair national security.

THE HERITAGE FOUNDATION STUDY CONCLUDES THAT PROTECTIONIST POLICIES SHOULD NOT BE APPLIED IN INVESTMENTS IN HOMELAND SECURITY, BUT DHS SHOULD ENSURE THAT ITS CONTRACTS OUTLINE STRINGENT SECURITY AND DATA-PROTECTION REQUIREMENTS.

Security from **What?**

The attacks of Sept. 11, 2001, were a wakeup call for industrial security, no doubt about it, but the wakeup extended further than the physical threat of terrorism to the plants. It caused manufacturers and others to take a closer look at the whole security picture.

As a result, physical security of manufacturing plants is not alone in management concerns about security. In the complex of threats are perhaps five: physical intruders, cyber intruders, clients, supply partners, and employees. There has always been the threat of theft.

Currently elevated security concerns come from basically two directions: physical and cyber. Analysts who have dealt with manufacturing security over the years believe the uppermost security should be in cyber security and physical security, in that order.

ARC Advisory Group, Dedham, Mass., in a study entitled “The New World of Manufacturing Security,” says, “Many point to 9/11 as the wakeup call for security, particularly for the critical manufacturing infrastructure of the industrialized nations.

“The threat of terrorism is not the primary driver behind the need for an enhanced level of security at all levels of the manufacturing enterprise. In ARC’s view, a coherent security strategy should address both information-based (cyber) security and physical security.”

According to a recent ARC security server, manufacturers are taking security threats very seriously, and most say their physical security efforts are ahead of their cyber security efforts. Therefore ARC focused this report mostly on cyber security.

“Modern manufacturing cannot thrive without current information from its manufacturing processes being fed to its business systems,” says the ARC study.

Collaborative activities connect a manufacturer’s production systems to other manufacturing systems outside the corporate structure. The plant floor is connected to the business enterprise.

“The enterprise includes the business partner on both the supply side and the customer side. The Internet is the pipeline that facilitates this business collaboration, resulting in the dramatic increase of Internet connections to the plant floor and increased vulnerability to the outside world.”

ARC Advisory Group discusses multiple cyber threats, some of which most of us haven’t thought about. Networking is widely accessible to many security threats, such as overwhelming an open port with requests for service, viruses, worms, packet modification, network spoofing. The authors—Bill Moore, Dick Slansky, and Dick Hill—provide abundant examples.

They conclude, however, “While the inherent open nature of the Internet can potentially expose internal systems and processes, there are a number of security tools, methods, and procedures that are currently providing more than adequate levels of security.”

Cyber attacks are being analyzed by numerous governmental bodies as well as international private-sector organizations. In the United States, most governmental activities regarding cyber security have moved to the Dept. of Homeland Security (DHS), notably the Critical Infrastructure Assurance Office (CIAO).

One of the key activities is to facilitate information sharing and analysis for the many critical-infrastructure industries. These centers, when fully operational, will quickly disseminate critical information regarding any cyber attacks to alert the industry to the threats before damage can be done, the authors explain.

ARC Advisory Group describes many cyber security activities taking place worldwide, most of which manufacturers should find out about to know what’s being done to help. For instance, the National Institute of Standards and Technology (NIST) is heavily involved in researching technology for cyber security on the manufacturing floor.

ARC lists specific automation suppliers that can provide some of the security-solution mix and others that are broad-based security specialists. It discusses best practices in manufacturing security for emulation by others. It discusses budgeting and who should be in charge of security.



Much more is available in the study, too lengthy to detail here.

Among many recommendations, one is develop a holistic security policy. Empower your risk assessment and analysis group to establish policy and procedures to protect your physical assets, networks, and automation systems from attacks.

Remember that cyber security is not implemented once and done but is an ongoing task to stay ahead of those that wish to breach your security.

Do not ignore the internal security threat that can be either malicious or unintentional.