Cyber Security in Manufacturing & Production

In today's competitive market, manufacturing and production facilities must improve the timeliness and effectiveness of their production decisions to stay competitive. This often involves the integration of real-time production systems with business applications to streamline the flow of information. However, security issues with Windows® & Internet-connected business networks have caused significant reliability issues for operations systems.

Some of the primary causes of lost production leading to financial loss are incorrectly configured firewalls, viruses and uninstalled or outdated system patches. To effectively address security; people, processes and technology must be considered. This presentation attempts to address security challenges by identifying vulnerabilities, applying pacesetter best-practices and sharing experiences and solutions.

Introduction

Market competition across different manufacturing and process industries has traditionally driven the evolution of production control systems. Over a decade ago, most systems were autonomous and built upon proprietary vendor technology and the solutions were geared towards access to data, speed, and functionality. Security features were not a high priority. However, due to the separation of the production systems from other networks, it permitted organizations to operate with confidence for several decades with the same system. But the demands on today's control systems have changed in today's the information age. To remain competitive, organizations need to respond quickly to the changes in their industry. Executives need to be in touch with the business and know when to make a decision, but they need to have timely and accurate information. Your production & control system must feed this information to the decision makers as soon as possible. This demand for information has forced the integration of production & control systems with business systems, and resulted in a number of new challenges for companies to deal with.

The use of open technologies has increased drastically in the last decade and presented many new challenges. In the early years of computer-based control systems used in many processing facilities, vendors built their solutions using their own designs, standards, and technology to achieve the reliability and capabilities needed. Everything from the hardware platform through to the software environment was all developed and sourced from the same vendor. Most of this technology did not exist, therefore the vendor had to design & engineer everything. Over time, public computer systems based on PC technology, Windows/UNIX operating systems, Ethernet networks, and TCP-IP communication evolved and their capabilities increased. Now vendors often develop their solutions based on commercial off the shelf (COTS) systems to maximize potential market share and to provide familiar platforms to the end users. This has resulted in the influx of open technologies like Windows, IP and Ethernet in current production systems. Benefits of leveraging existing standards and technology surpass the challenges of developing them internally.
# Table of Contents

- **Cyber Security in Manufacturing & Production** ................................................................. 1
- **Introduction** ......................................................................................................................... 1
- **Security Thinking: Risk Management Methodology** .......................................................... 5
- **Comparison: Pacesetter Activities** ..................................................................................... 7
- **Conclusion: Overcoming the Challenge** .............................................................................. 9
- **References** ......................................................................................................................... 10
**Table of Figures**

<table>
<thead>
<tr>
<th>Figure 1:</th>
<th>The Knowledge Gap</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 2:</td>
<td>Security Management Plan</td>
<td>6</td>
</tr>
<tr>
<td>Figure 3:</td>
<td>Recommended Secure Network Architecture</td>
<td>7</td>
</tr>
</tbody>
</table>
The danger is that software development is not perfect. Software companies test their software rigorously, yet even after it is sold to the customer there are still issues and bugs being identified. When the software is widely available like Windows, and therefore highly scrutinized, the likelihood of finding bugs is even higher and can affect significantly more people. Open technologies are a likely target for malicious activities because they are easily accessible, have a wide installation base and detailed information is available on the Internet. If an issue is discovered in an application, it does not take long for an exploit to be developed and a virus to be unleashed. In 2002, it took six (6) months for the Slammer virus to be developed for a SQL database server bug once the vulnerability was identified. It took one (1) month in 2003 for Blaster and three (3) weeks in 2004 for Sasser between identification and release of the worm. The latest viruses are being released just days after the exploit is discovered, making it difficult for vendors to find fixes and for companies to deploy them in time.

Deployment of a security patch should be subjected to internal testing to ensure it does not affect your systems. There have been situations when a new security patch caused systems to fail because it was incompatible with existing software, or the patch is not certified by the control system vendor, and its installation voided system support and warranty. It takes time for a vendor to certify patches, especially when their control system could be used in thousands of facilities, in different industries around the world. We have reached a point where vendors are unable to certify patches before the virus is developed. And while some vendors are putting serious efforts into minimizing the time lapse between Windows update releases and certified patches, the ‘bad-guys’ are moving towards a zero day attack.

Cyber security in a live production system has several more challenges, and the technology to solve them is still in its infancy. Basic security practices like strong authentication, encryption, and others are not available in most systems. In many cases it is very difficult to implement security capability in low-speed and low-CPU devices. Customer requests for features and functionality have consumed vendor R&D efforts and low consumer priority has been placed on security capabilities. In the last few years security has become one of the most important items consumers are asking for, and few industry products are ready. In the meantime, the level of integration of corporate business systems with plant control systems continues to increase. Corporate IT security groups are demanding control system be more secure, have up-to-date patches, lock down their firewalls, and follow corporate IT policies. However well intentioned as this may be, it often does not work in the day-to-day production world.

Traditionally, corporate IT policies pressure control system engineers to manage their systems differently. In some cases IT groups have become deeply involved in the daily management of control systems, creating a situation where IT practices conflict with the priorities of a live production environment. For example, automated patch deployment, widespread antivirus software installation and computer security policies are not always feasible or appropriate.

In some corporations the level of cooperation between the corporate IT team and automation is lacking. There are many teams who detest the involvement of IT due to negative past experiences. In many organizations, conflicting priorities, a lack of trust, understanding, and limited technical knowledge about each other’s skill set and area of expertise, has produced an uncooperative environment between production & IT to create an efficient Industrial Security team both IT and production need to exhibit some empathy and patience.

The diagram below is a summary of the organizational and technical differences between production and IT that shows why these two groups have difficulty working together. It is necessary to create a team or involve a consultant that has the necessary knowledge of all areas and can help translate the technical and organizational differences.
The last challenge that even proactive and cooperative Industrial Security teams face is trying to justify security spending. Industrial Cyber Security is Powered by Matrikon, which represents vendor neutrality. This product works with third-party control systems and applications. In the current competitive landscape, only the project initiatives that produce the greatest results (i.e. improve the bottom line) get approved. Security helps to reduce the chance of an incident, but the monetary benefits are largely intangible. The probabilities of most security incidents are extremely low, but the impact is often devastating to the organization. In the worst scenarios, companies have experienced lost production, waste material, environmental fines, additional labor costs, and negative public exposure. Security is about risk management. Determine the likelihood and impact of an event and evaluate the risk to the organization. Every potential risk needs to be evaluated to determine the organization’s exposure and if it can be accepted or if it should be mitigated. Once the risk is determined it is easier to justify spending to rectify the situation. This is the same strategy that insurance companies use to justify their services, and we should consider security spending like buying insurance.

Major vertical industries like mining, utilities, petrochemicals, and forestry are at different stages in their security initiatives. After 9/11, the US Government passed a bill to address many of the security issues in the American critical infrastructure. Critical industries like electricity and chemicals were the first priority because their disruption could have terrible results. The Northeast Blackout in 2003 is a good example of the effects that a power disruption can have and how important this service is. North American Electric Reliability Council (NERC) is the regulatory body over the power industry. They are developing a set of security standards which is likely to be put into law, requiring all power companies in North America to follow these standards or face potential fines. Responsible Care is involved in the chemicals industry and is requesting chemical companies to perform security vulnerability assessments to identify and mitigate their security issues. The activities in industries like power and chemicals are positively affecting and the best-practices that are being developed. Many companies understand the importance of cyber security and are budgeting security spending with or without regulatory pressure.

There are so many challenges that organizations face when trying to secure their systems. Lack of industrial security technology, team cooperation challenges, difficulty justifying security spending, and uncertainty among competing regulatory initiatives make implementing security an overwhelming task. Increasing numbers of companies and consultants are overcoming the major hurdles and can assist both beginner and experienced companies with and control system security.

Security Thinking: Risk Management Methodology

The three most critical parts to a corporate security program are people, processes, and technology. If your security program does not consider all three parts, it will fail. The absence of one leg on a 3-legged stool will cause it to fall over!
When most people think about cyber security, technology such as firewalls and antivirus programs come immediately to mind. There is a common misunderstanding that a firewall and antivirus software will protect systems. Past experience and several audits have discovered that most firewalls are badly configured and are open to many serious threats. It is not only important to install firewalls correctly, but also to consider other critical systems such as backup and recovery. It is important to prepare for an incident and ensure that critical systems can be recovered quickly.

Technology is the foundation for security and it is necessary to have the right systems installed. Companies should ensure they have good firewalls, antivirus, patch management, tape backup, remote access, authentication, and physical security in place. In a past audit at a large mining organization in Eastern Canada, Honeywell identified a large number of technical shortcomings that could effectively shutdown their production. In another audit at a company in a southwestern mining company, we helped them realize the security risk of having their control system shared with the business network.

When we talk about people in the context of security it refers to the employees, contractors and any visitor to the organization. Humans are the single biggest security risk! In order for a security program to be successful, it is necessary for the participants and stakeholders to have the necessary awareness, training, documentation and roles. Everyone needs to understand appropriate system use and why it is important, and technical people also need to know how to identify and address security risks. It is recommended from an organizational perspective to have a dedicated security group with the authority and executive support to enforce security violations. But, it is more important to have a security awareness program for employees to share the importance of security and how they can participate. If organizations do not focus on their people, security policies will not be followed, staff will not understand security issues, and technical staff will not manage systems effectively. In our past experience, we typically find a strong corporate security program, but rarely have we found an organization that proactively includes their production systems in their training and cyber security awareness programs.

The third aspect of security is process. When discussed in the context of security, process refers to the policies, procedures and action plans. Effective planning and processes minimize incident impact! Regardless how hard you try, there will always be residual security risks and potential incidents. The measure of your preparedness and the validity of your security program will determine how well you contain the incident and how quickly you recover from it. It is necessary to have documents in place like an appropriate use policy, backup policy, and wireless policy to define how company assets should be used and deployed. Policies determine the rules of using a system; define procedural countermeasures for potential security risks, and any best practices. Procedures are step-by-step instructions on how to perform or execute a plan without being the expert on the system. Both policies and procedures are required for a good security program. Processes or procedures are also vital in outlining the overall security mentality and approach your organization wishes to implement. As your business evolves, so too will your environment. By having clearly defined expectations of future programs and applications you can evolve your business while maintaining the highest possible level of security.

To summarize, security must focus on people, processes and technology to be effective. A shortcoming in any of these areas will severely weaken your efforts and ultimately your security program will fail. Honeywell has created the Security Management Plan above.
as an outline of the critical parts of a security program. It helps to visualize the requirements of industrial security, and ensure the preliminary framework is in place.

**Comparison: Pacesetter Activities**

A decade ago when most systems and business networks were isolated from one another security was relatively simple. However, over time the two networks have become interconnected. The first method of integration was usually a server with a network interface into both the business and production networks, commonly called bridging. For several years this was an effective way to control the flow of data from one network to the other. But with recent worms that have the ability to infect one computer and become a launching point to find more, viruses easily propagate through bridged network servers. Bridging servers is not a secure computing practice. Another common practice is to install a firewall between production and business networks, but this still allows a computer on the inside network to be compromised and propagate the virus through to the critical systems within. Unfortunately, there have been several companies that have suffered operational losses through technical shortcomings with bridged servers or poorly configured firewalls.

The best way to control security between two networks such as production and business networks is to use multiple firewalls and a DMZ (de-militarized zone). This creates a middle-tier network that can be used for the safe transfer of information. Devices and applications on the DMZ become security agents or brokers to ensure that malicious threats are contained and not permitted to propagate.

![Recommended Secure Network Architecture](image)
The drawing above demonstrates a model network architecture which is based on the common DMZ model, but with Honeywell’s experience it is often enhanced to meet the unique requirements of today’s production system. The purpose of the DMZ network is to allow the structured flow of information between the business and production networks while maintaining a high level of security. This can include production, lab, maintenance, haulage information, and reports. It also allows incoming connections for administrators, file transfers, antivirus and security updates. With designs like this, the system can operate safely but also permit the flow of information into higher-level business systems. If a security incident or change occurs on the business network, the critical systems are isolated from the threat.

Once the correct network design is in place, the next step is to install the supporting systems to help maintain its operation. From a maintenance perspective, it is recommended to have active monitoring systems to identify when a fault occurs so that it can be repaired quickly. From a security perspective, it is important to identify inappropriate uses and intrusions to ensure they are stopped before an incident occurs. From a legal forensic perspective, it is important to log, audit, trace and identify who is using the system and determine who may have been involved in malicious activity. If a security incident occurs, good trace logs help to identify how the intruder got into the system and how to get out of the situation. Without appropriate logging information, it is very difficult to correctly identify a security issue and to mitigate or resolve the situation. What may appear as a failed operator console may be the result of a hacker or virus. And in light of the increasing pressure from many different compliance efforts (such as Sarbanes-Oxley), logging and audit-ability is becoming more and more important to many organizations.

Industrial security pacesetters are also writing, reviewing and deploying extensive policies and procedures. Every organization has security policies in place to define the appropriate use of corporate IT computers, but rarely do they consider the unique requirements of a live production environment. Pacesetters understand the differences, and are writing documents that are unique to their systems. For example, they have policies and procedures in place to guarantee all critical systems are backed up regularly and verified and tested to ensure they are prepared to recover the system quickly. Typical IT infrastructure like tape backups cannot be used to recover all production systems. The recovery policies for a live production system are unique and must be documented and regularly practiced. Pacesetters also have strict remote access policies to define how vendors access their systems for support and administration in both safe and auditable ways.

To ensure that the infrastructure critical to your system stays running, it is important to assess how they are managed and the training that their staff possess. This is a simple statement, but many systems are installed and allowed to operate unattended for years until an event occurs. This is the worst situation because the support team is unprepared, not practiced and often not familiar with the system after years of inattention. This results in system troubleshooting and recovery that could take several days of additional cost when it should only be hours!

The leading pacesetters for industrial cyber security have already upgraded their systems and have extensive policies, procedures, training programs, and support teams in place. Pacesetters are also actively involved in industry activities to increase awareness and knowledge of others. There are many workgroups, committees, forums, and regulatory bodies that are actively trying to improve control system security across all industries. They include:

- **National Institute of Standards & Technology (NIST)** – Computer Security Resource Center (CSRC) and the SP800-series of guidelines.
- **North American Electric Reliability Council (NERC)** – Critical Infrastructure Plan (CIP) standards 002 through 009.
- **Chemical Industry Data Exchange (CIDX) and Responsible Care**
- **National Petrochemical & Refiners Association (NPRA) and American Petroleum Institute (API)**
- **Process Control Security Forum (PCSF)**
- **Department of Energy (DoE) and Department of Homeland Security (DHS)**
  
  All of these groups develop documents, guidelines, checklists, and other useful information. These are great venues to learn from others who have been faced with similar issues and how they have overcome them.

  One of the most important topics that you will find across various information sources is the need for greater security awareness among the corporation as a whole. To move ahead with any security initiative, it is necessary to value and weight all options before proceeding with any changes. In order for the security initiative to be successful, a very fine line between securing data and access to that data must be decided upon. Further to that is the issue of user burden. As the complexity of any system or access to it increases, there is an inevitable increase in the tasks and expectations placed upon the users of that system. In order to have success in any security project, a multi-disciplinary team should be included in the decision making process. This team will likely include someone from operations, IT, engineering, users and the project execution team. This team could also include any administrative representation the project may affect, any compliance team or executive level presence where applicable (SOX or NERC). One of the most important functions of a multi-disciplinary approach is the awareness level that is instantly brought back to each of the departments represented at the meetings. In cases of major projects, specific awareness campaigns are recommended because your security initiative is only going to be successful if your end-users use the new procedures and systems properly. Without widespread ‘buy-in’ you will eventually fail.

  True pacesetters in the area of user buy-in and company-wide security campaigns have multidisciplinary teams that review all IT/Security related projects from the bid phase through completion and testing. This serves multiple purposes from sharing information across teams and departments, garnering support for various initiatives and to streamlining specific projects when they are off-track. Most of all it raises the awareness of any single project to the consciousness of the entire company.

**Conclusion: Overcoming the Challenge**

The importance of industrial security and compliance is new and has seen significant growth in the last five years. This is largely due to the integration of and business systems, but also the exponential growth of viruses and increasing maliciousness of people. As systems migrate to open systems like Windows and TCP-IP, the security risks are greatly increasing. Even with the assistance of corporate IT groups, companies have challenges mitigating security issues.

To effectively manage industrial security requires a focus on three elements – people, processes and technology. This helps maintain an awareness of all security factors and ensures there are no weak links in your strategy. They must also ensure they implement the correct security architecture design and systems to support their security efforts. Guidance on how to address many industrial cyber security challenges is available from many security committees and professional consultants.

The primary differentiator of pacesetters with respect to industrial security is the fundamental thinking and cultural change in the organization. It is not just a checklist, but an environment that adopts new ideas, evolves, and promotes participation & sharing. They see the benefit in security initiatives and are able to achieve full participation and ownership from all employees, contractors and visitors.
References


Donovan Tindill, BAIST-NM
Rick Kaun, CCIT
November 2007

© 2011 Honeywell International Inc.

For more information:
For more information about Industrial Cyber Security, visit our website
www.honeywell.com/ps or contact your Honeywell account manager.
www.matrikon.com
security@matrikon.com

Honeywell Process Solutions
1250 West Sam Houston Parkway South
Houston, TX 77042
Lovlace Road, Southern Industrial Estate
Bracknell, Berkshire, England RG12 8WD
Shanghai City Centre, 100 Junyi Road
Shanghai, China 20051

Windows® is a registered trademark of Microsoft Corporation in the United States and other countries. UNIX is a registered trademark of the Open Group