



Sinclair Koelemij CISM
ENSASS – EMEA Network Solutions & Security Services

Industrial Control Systems and Cyber security



Honeywell → Honeywell.com

Why cyber security?

CNI Protection

Hackers For Hire


Faster Releases

Application Hacking

CyberCrime Increases

Increasing Incidents

**Why Is
CyberSecurity
More Important
Than Ever
Before**



**Why Are
Process
Control
Facilities At
Risk?**

Business Demands

Move To Open Systems

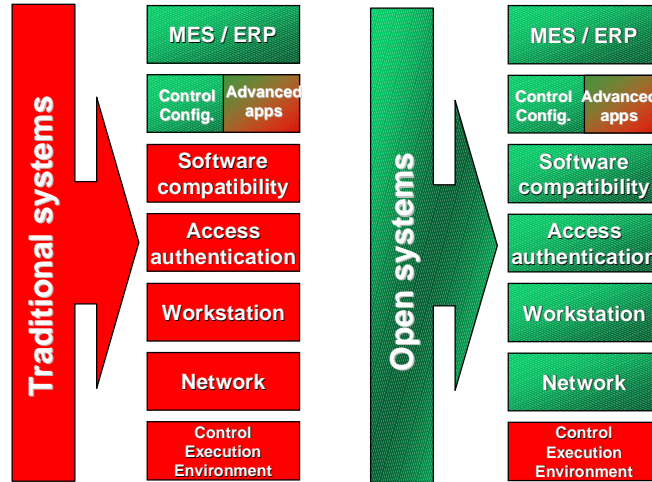
Outdated Security

Attractive Targets

The Risk Landscape Is Changing...

2
WIB April 2006 Honeywell Proprietary

Open systems



Transition from Proprietary to Open solutions

Just a few questions.....

- Does plant management know who is responsible for cyber security? Does the responsible individual know? Does everyone else know?
- How many staff had security training last year? How many of the management team received security training?
- What is industry best practice and how does your plant compare?
- Is plant management aware that serious security breaches could result in significant legal consequences for which management may be held responsible?
- When was the last time a cyber security audit was performed? Does management track progress on the recommendations?

Is security considered an afterthought or a prerequisite?

The security chain



Adversaries attack the weakest link, where is yours?

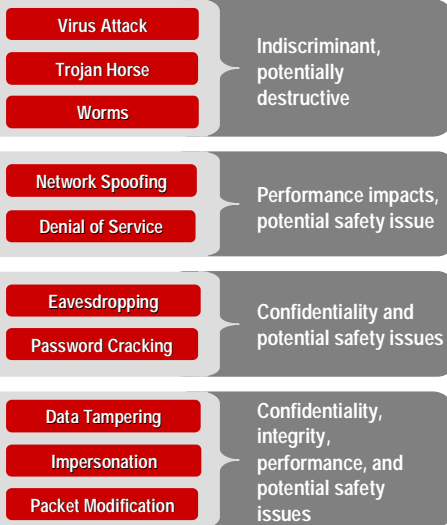
Links in the chain (non technology)

- ✓ Security policies and procedures
- ✓ Risk management
- ✓ Security planning
- ✓ Contingency planning
- ✓ Incident response planning
- ✓ Physical security
- ✓ Personnel security

Links in the chain (technology)

- ✓ Access control mechanisms
- ✓ Identification and authentication mechanisms
- ✓ Audit mechanisms
- ✓ Encryption mechanisms
- ✓ Firewalls

Examples of Cyber Security Attacks



Without a security strategy, you are taking **significant risks** with your business

What / Where are the vulnerabilities?

- Lack of Security Policies, Procedures, and Change Management
- Inadequate Physical Security
- Entry points into process control networks
- Lack of or out of Date Virus Software
- Lack of or out of Date Security Patches
- Inadequate Security Configuration
- Inadequate or Infrequent Backups



A vulnerability is something that enables a threat to reach / impact your asset

Cyber security for process control

Performance requirements	Real-time, critical response, modest throughput, no delay or jitter allowed
Availability requirements	Outages are not acceptable , fault tolerance, extensive pre-deployment testing
Security focus	Controllers, PLC's, field devices, stations, and servers
Time critical interaction	Response to human emergency action is critical
Resource constraints	Designed to support the intended industrial function
Communications	Many proprietary communication protocols, multiple media types
Software updates	Software changes must be thoroughly tested and deployed multi staged

Cyber security mission

- Ensure that the plant's requirements for: Availability, Integrity, and Confidentiality are met.
- Ensure that staff knows who does what relative to security – The dos and don'ts of security.
- Ensure that security is an integral part of the systems development life cycle process and is explicitly addressed during each phase of the process.
- Ensure that you are prepared when a security incident occurs.

Cyber security for Industrial Control Systems is common sense to design, build and maintain systems to be available, to ascertain that operators are in control and that the intellectual property of the plant is secured.

What is the impact?

- British Columbia Institute of Technology (BCIT) tracks security incidents at process control facilities
- BCIT reports the following customer impact experienced by those reporting incidents in 2003:



50% had losses > \$1M



29% had loss of view



41% had loss of production

Some examples

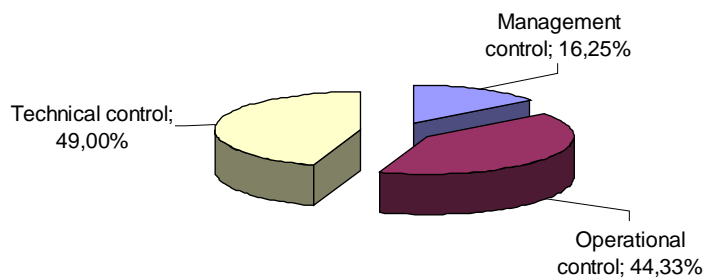


The list you want to keep out:

- o **Salt River Project** – Break into computer systems for water and power distribution
- o **Worcester Air Traffic Communications** – Disconnecting phone for control tower, airport security and airport fire department
- o **Maroochy Shire Sewage Spill** – Release of 264000 gallons of raw sewage into nearby rivers and parks
- o **CSX Train Signaling System** – Computer virus shuts down safety systems
- o **Davis-Besse** – Slammer network worm disabled safety monitoring systems nuclear power plant
- o **Daimler Chrysler** – Zotob network worm stopped 13 US production plants.

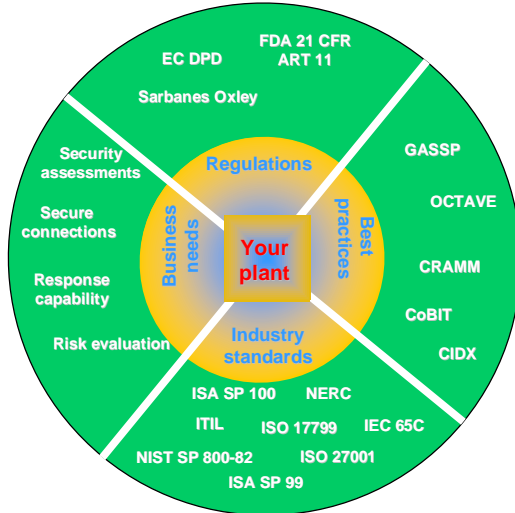
Source: ISA

How well are we protected?



Source: Honeywell PCN security assessments 2001-2006

The security field



**If you are caught today,
there is no one
to blame
but yourself?**

Honeywell PCN Security Services: Winner of Vaaler award



Recognizes the key roles that suppliers' innovations can play in helping plants achieve and maintain peak operating safety and efficiency

The awards, named for John C. Vaaler, long-time editor in chief of Chemical Processing magazine, were established more than 40 years ago specifically to honor products and services that have markedly improved the operations and economics of plants.

BCIT Security Testing

- BCIT Tests on C200 and C300
 - "The C300 and Control Firewall is the most secure control device combination that BCIT has tested to date. It is the only system that we were unable to disable in some manner." – Eric Byres, BCIT
 - "There were no critical notices uncovered in the C200, only the second time this has occurred in the history of industrial control device testing at BCIT." – BCIT Test Report
 - Both devices had minor notices due to Ethernet architecture
 - Broadcast and multicast storms
 - ARP floods
 - Emphasizes the need for a system approach to security
 - All vulnerabilities mitigated by either
 - Control Firewall; or
 - Switch QoS settings

Common sense

Cyber security is primarily common sense in protecting process control networks and systems

- **Protect against the obvious**
- **Be aware of the things that happen in your system**
- **Minimize the impact of device failure**
- **If an error event happens, contain the impact of the error**
- **Maintain performance**
- **Control access**
- **Make sure you can respond if the unavoidable happens**

And remember "No Safety without Security"

Honeywell

→ Honeywell.com

Honeywell

www.acs.honeywell.com