SANS

September 9 2008

Gaining Support of Top Management for Investments In Improved Control Systems Security: What Works?

PRICEWATERHOUSECOOPERS

SANS

September 9 2008

Gaining Support of Top Management for Investments In Improved Control Systems Security: What Works?

Auditing works!

But hey, what other answer would you expect from an auditor?

PRICEWATERHOUSECOOPERS

ISO 27002/ISO 27001 audits

- We have conducted initial audits against ISO 27001/27002 at public utility companies, heavily based on SCADA systems
- ISO 27001/27002, also known as the Code of Information Security is the leading standard for information security:
  - ISO 27002 is a comprehensive list of security controls (133)
  - ISO 27001 describes a management system for the ISO 27002 control selection based on risk management

SANS

PRICEWATERHOUSECOOPERS

Some audit results

- Two worlds in one company: the ‘office’ and the ‘factory’
- Information security in the factory is still in its infancy
- Insufficient insight in the actual information security risks, let alone adequate management of them

SANS

PRICEWATERHOUSECOOPERS

Some audit results

- Security critical passwords shared by many employees (some of which even had left the company)
- No periodic review of user rights
- Default manufacturer passwords not changed
- No hardening of servers
- SCADA servers without virus protection

SANS

PRICEWATERHOUSECOOPERS

Some audit results

- Structural technical network security problems: SCADA components controllable from anywhere in the WAN without any authentication
- No firewalling
- WAN shared by office and factory networks

- Overall: an alarming message for management

SANS

PRICEWATERHOUSECOOPERS

Solutions

- Address structural, technical information security risks, most notably the lack of network security
- Discussion with manufacturers

SANS

PRICEWATERHOUSECOOPERS

Solutions

Get grip on SCADA information security through risk management (e.g., ISO 27001 or ISA-99 based):

- Create a (logical) inventory of the SCADA infrastructure
- Allocate security responsibilities for logical clusters
- Adopt and implement security baselines (ISO 27002, but also manufacturer specific)
- Perform business impact analysis to find critical clusters
- Conduct risk assessments to decide on additional controls
- And of course, let the PDCA cycle roll

SANS

PRICEWATERHOUSECOOPERS

Thank you