

Managing industrial control system security risks

Action is needed now to protect industrial process control and automation systems from cyber attack

RUSI Conference –

Trends in International Energy Security

5th April 2006

Justin Lowe



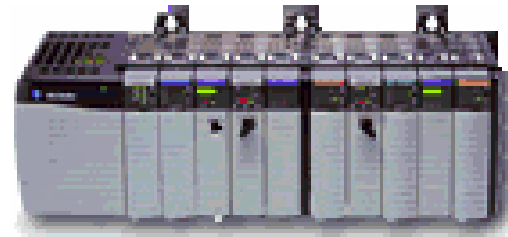
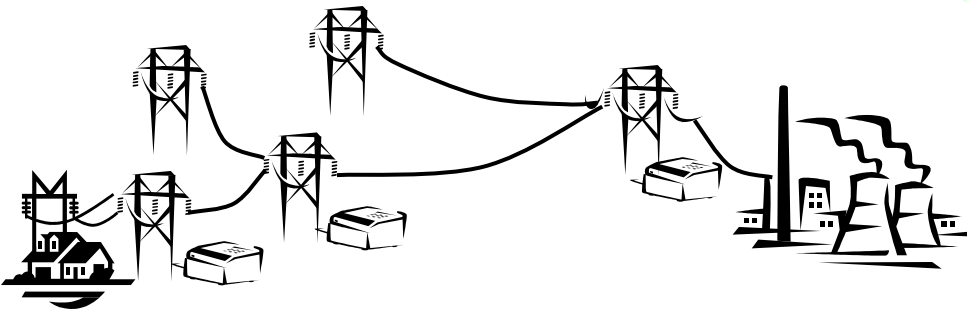
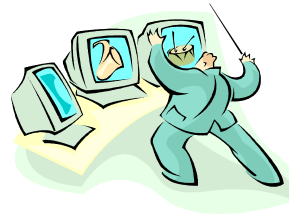
What are industrial control systems?

Involved in:

- Power generation and distribution
- Oil and gas refining and distribution
- Water and waste systems
- Chemical processing and transport
- Manufacturing
- Transportation

Also known as:

- Process Control Systems
- Supervisory Control and Data Acquisition (SCADA)
- Distributed Control Systems (DCS)
- Programmable Logic Controllers (PLC)
- Intelligent Electronic Device (IED)



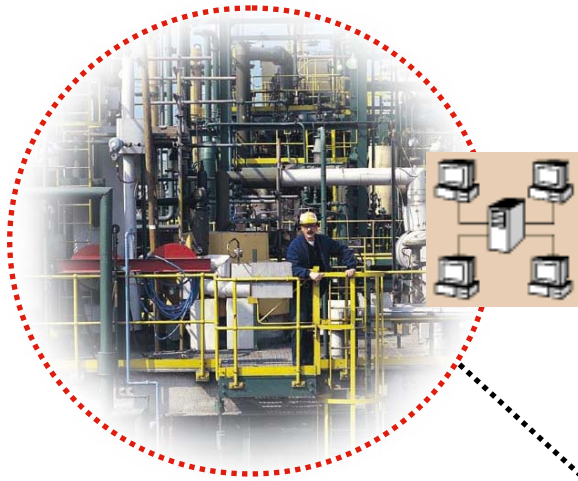
Process Control Systems are becoming increasingly vulnerable to cyber attack

- **Adoption of standard IT technologies**
 - Windows/Intel
 - TCP/IP
 - Web technologies
 - Wireless communications
- **Move from bespoke applications to packages & commercial off the shelf software**
- **However this has introduced all the standard vulnerabilities and security issues into the world of process control**

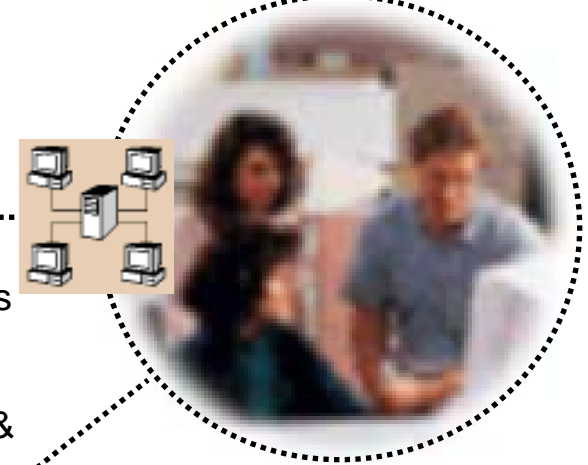


Vulnerable Process Control Systems are increasingly being exposed to the wider cyber world

Process Control Network

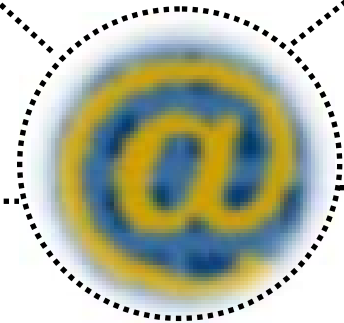


Corporate Network



Corporate connectivity provides access to production information that allows process optimisation & supply chain management

Connectivity for control system vendors to provide direct **support and maintenance** is increasingly common



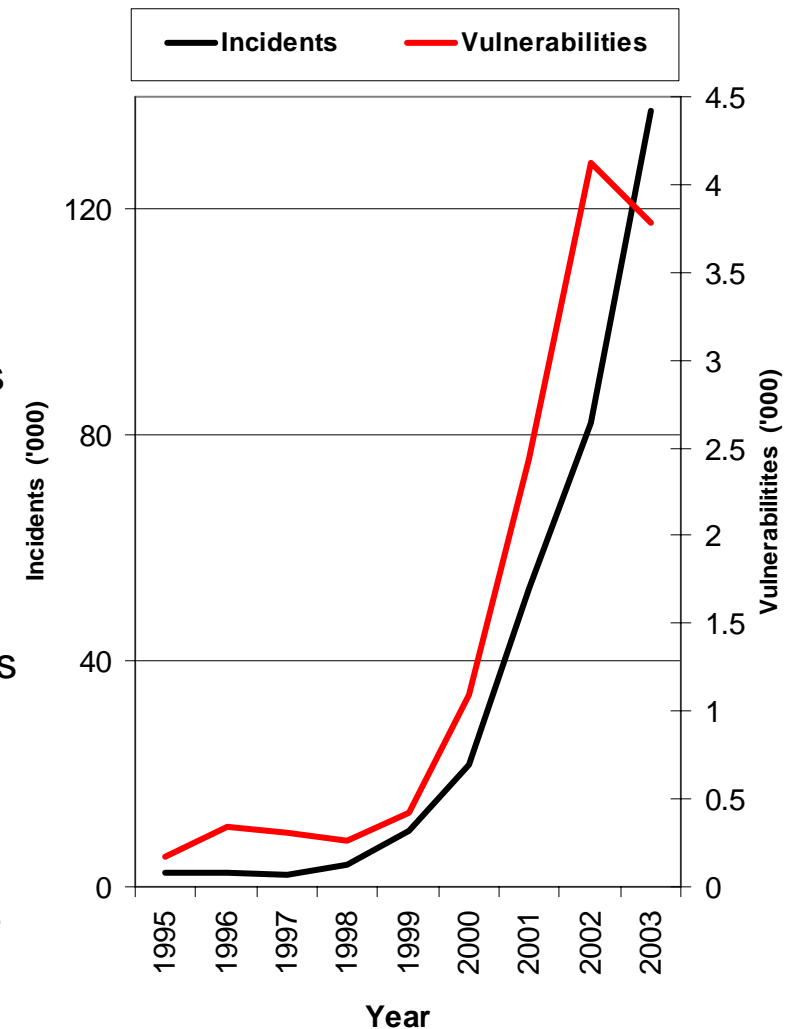
Almost all companies are now connected to the **world wide web**

Web enabled supply chain **B2B systems** are increasingly connecting corporate and process control networks



The wider cyber world is becoming increasingly hostile

- Vulnerabilities are being discovered at an ever increasing rate
- It is becoming increasingly difficult (and costly) to patch IT systems to fix these vulnerabilities
- These vulnerabilities are more quickly being exploited into attacks and self propagating worms
 - Code Red worm took around 6 months to be developed - Blaster took 26 days!
- Worms are becoming more frequent, capable of infecting global networks within minutes and are now attacking the core operating system functions
- Hackers are beginning to focus on embedded systems and SCADA/Process Control
- Hacking tools and information are freely available on the internet.



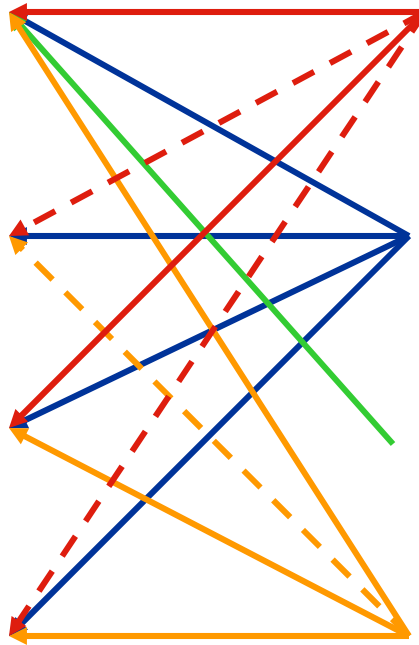
What are the threats?

Threat types

- Denial of Service
- Unauthorised Control
- Loss of Integrity
- Loss of Confidentiality

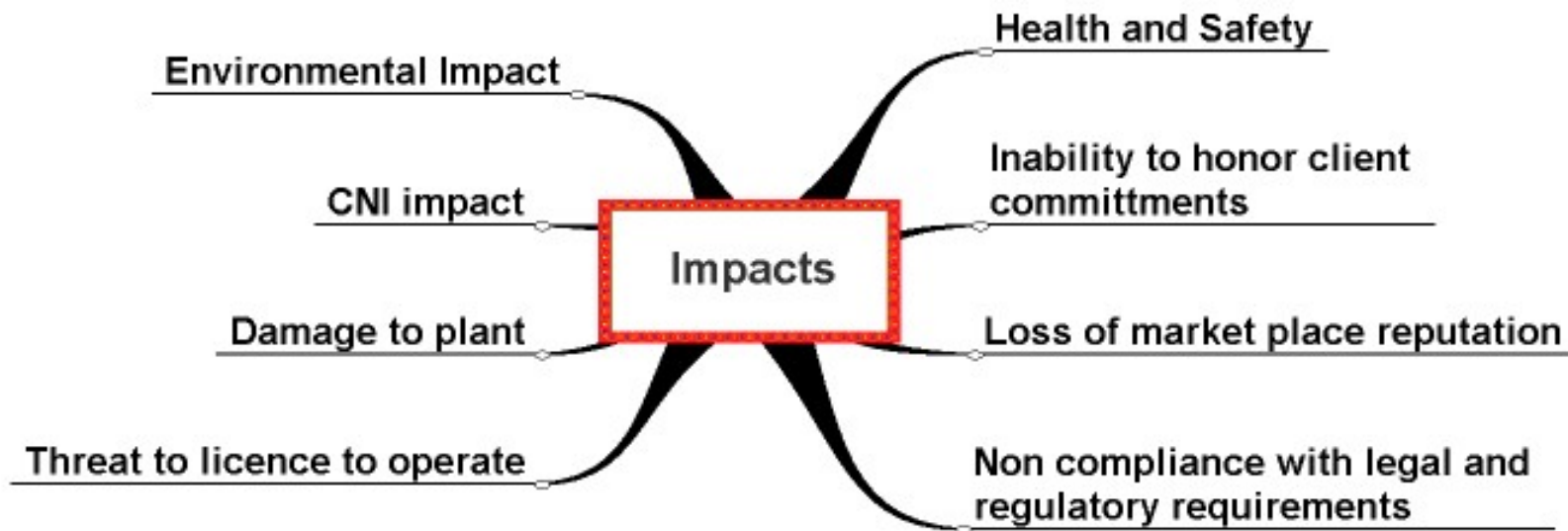
Threat Sources

- Worms
- Hackers
- Accidental Attacks
- Traditional Viruses



The business impacts of cyber attack cannot be ignored

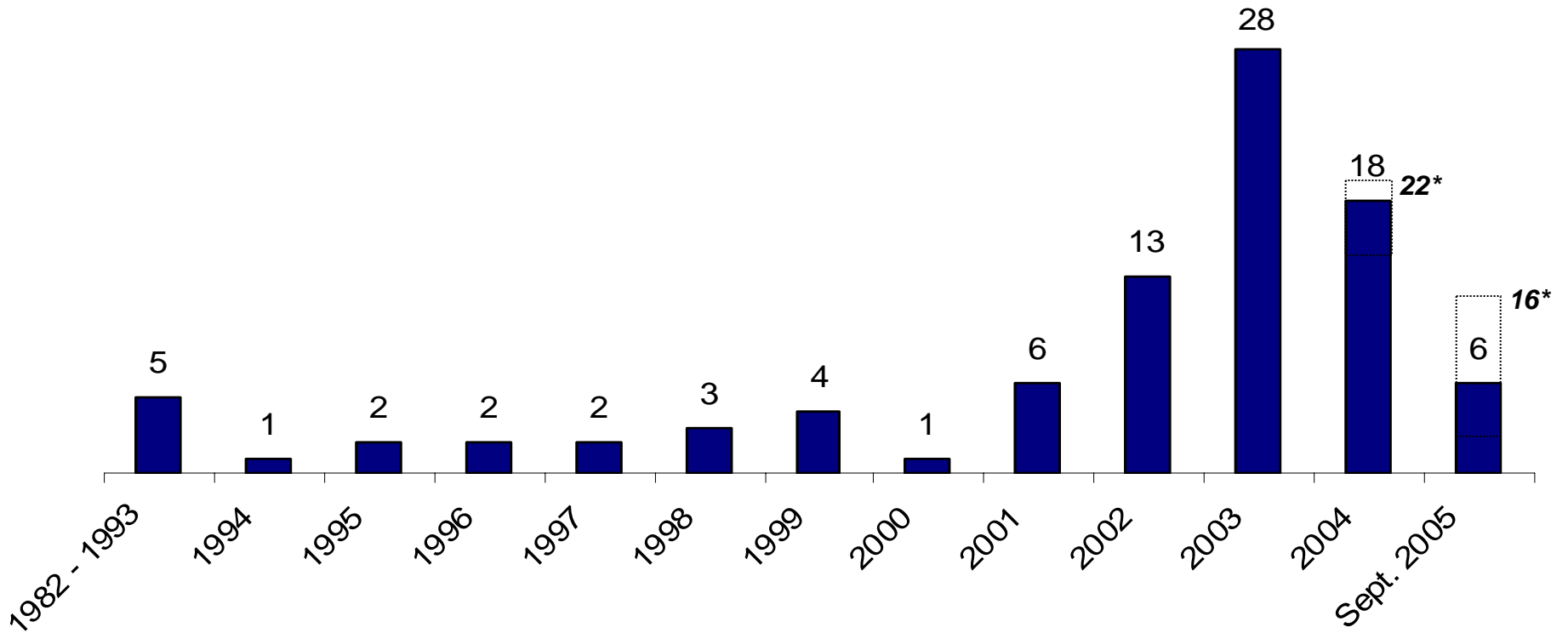
The obvious business impact is the financial consequences of disruption to production or operations. However there are other consequences of cyber attack.



Process Control Security incidents are real

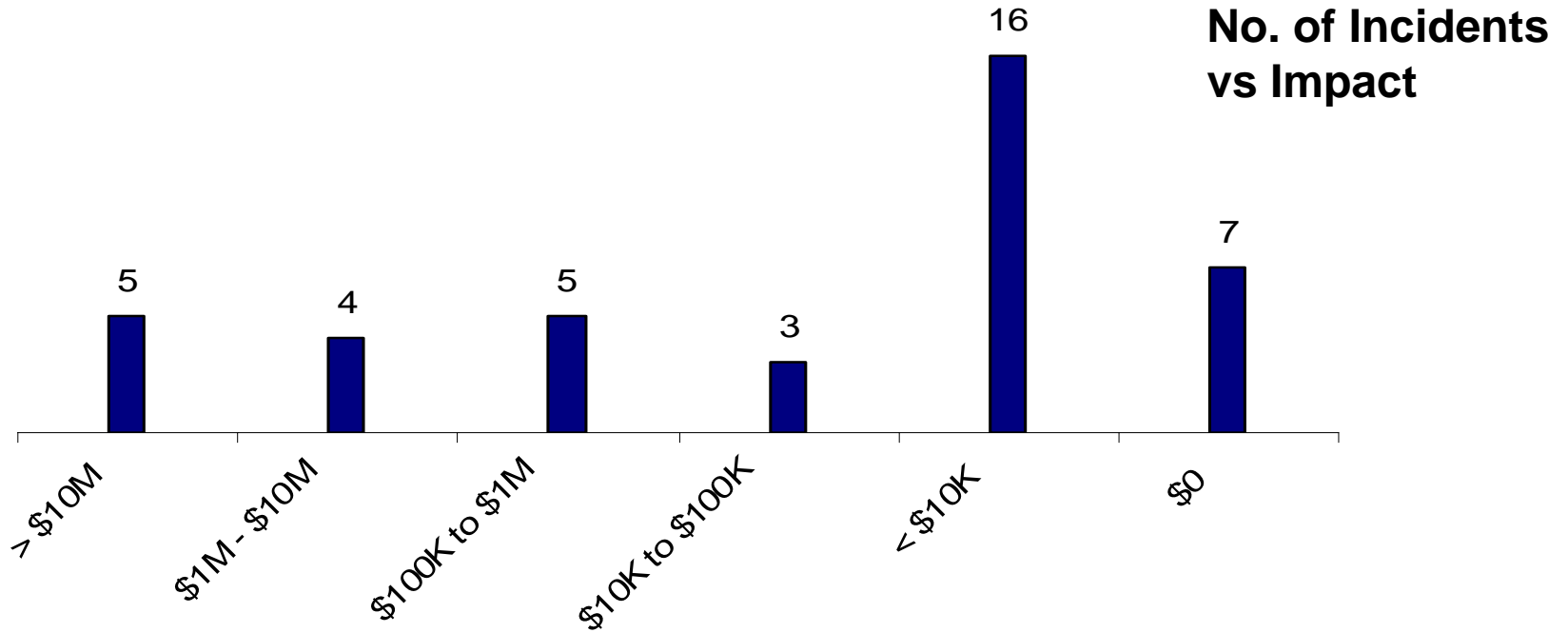
- A disgruntled ex employee attacks a sewage control system and releases millions of gallons of sewage into a river and hotel grounds.
- Hackers control Gazprom's pipeline for 24 hours
- SQL Slammer worm infects Davis Besse nuclear power station causing slowdown of control system
- Blaster worm contributes to US power outage
- Manufacturing plant grinds to a halt as security scan crashes hundreds of PLCs
- Control system infected by virus from contractor's laptop
- Manufacturers impacted by Sasser and Witty worms
- Vendor's update disk contained virus
- Hoover dam control system hacked by script kiddie
- Programme code written to incorrect PLC causes environmental incident

Incidents Appear to Peak in 2003



* Projected **PA**

Cyber Incidents can be Expensive



- Wide range of costs from 0 to >\$10M
- Average cost per incident is \$1.8M
- However the data sample where impact is quantified is still very small (40)

Looking to the Future - The Hackers are Waking Up

Brum2600 Blackhat Conference:



“Things started to get a little more interesting... The talk was titled ‘How safe is a glass of water.’ It was a detailed breakdown of the RF systems that are used by water management authorities in the UK and how these systems can be abused, interfered with and generally messed.”

Source: The Register, October 20, 2003

Talk #16: SCADA Exposed



“Cyber-attacks on these systems and subsystems can be targeted from remote locations to multiple locations simultaneously... This talk focuses on the assessment of the SCADA infrastructure and attack analysis of the more common SCADA protocols in use today.”

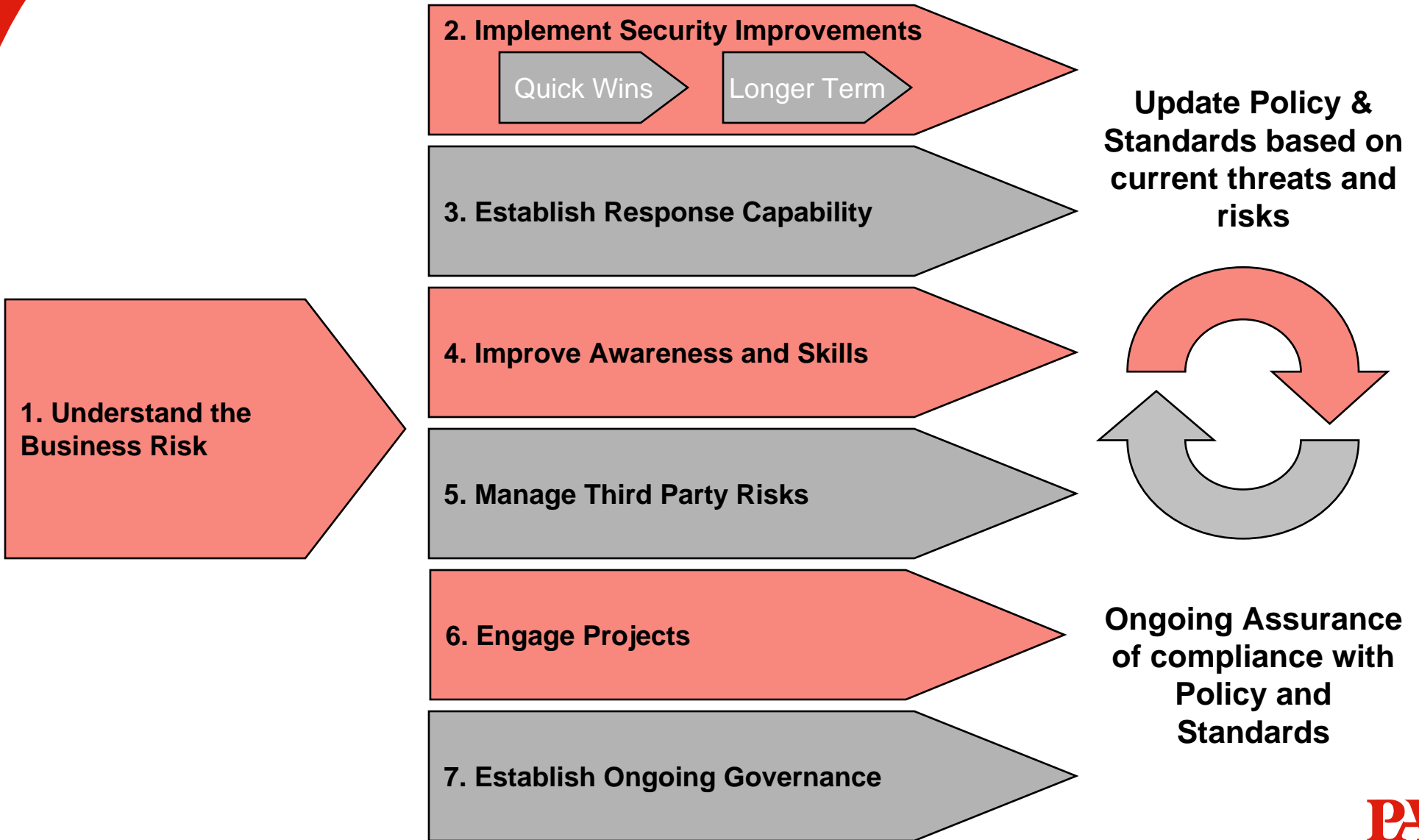
Source: Toorcon 2005 Website

It isn't just a matter of simply extending the IT Department's security policy

The process control IT environment and the 'standard' corporate IT environment have some significant differences. This means that some of the standard approaches don't work or aren't applicable.

Topic	Corporate IT	Process Control
<i>Anti Virus</i>	<i>Widely used</i>	<i>Often difficult/impossible to deploy</i>
<i>Lifetime</i>	<i>3-5 years</i>	<i>5-20 years</i>
<i>Outsourcing</i>	<i>Widely used</i>	<i>Rarely used for Operations</i>
<i>Patching</i>	<i>Frequent (daily?)</i>	<i>Slow (requires vendor approval)</i>
<i>Change</i>	<i>Frequent</i>	<i>Rare</i>
<i>Time Critical</i>	<i>Delays OK</i>	<i>Often safety dependent</i>
<i>Availability</i>	<i>Outages OK (overnight)</i>	<i>24/7/365 for years</i>
<i>Security Skills & Awareness</i>	<i>Pretty good</i>	<i>Poor</i>
<i>Security Testing</i>	<i>Widely used</i>	<i>Use with care!</i>
<i>Physical Security</i>	<i>Usually secure and manned</i>	<i>Often remote and unmanned</i>

Good practice guide for process control and SCADA security





PA Consulting Group



PA Consulting
Group

Justin Lowe

IT Management

123 Buckingham Palace Road
London
SW1W 9SR
United Kingdom

Direct Dial: +44 20 7333 5852
Direct Fax: +44 20 7333 5457
Mobile: +44 79 7362 7196
Switchboard: +44 20 7730 9000

www.paconsulting.com
justin.lowe@paconsulting.com

http://www.paconsulting.com/process_control_security

<http://www.niscc.gov.uk/niscc/docs/re-20051025-00940.pdf?lang=en>