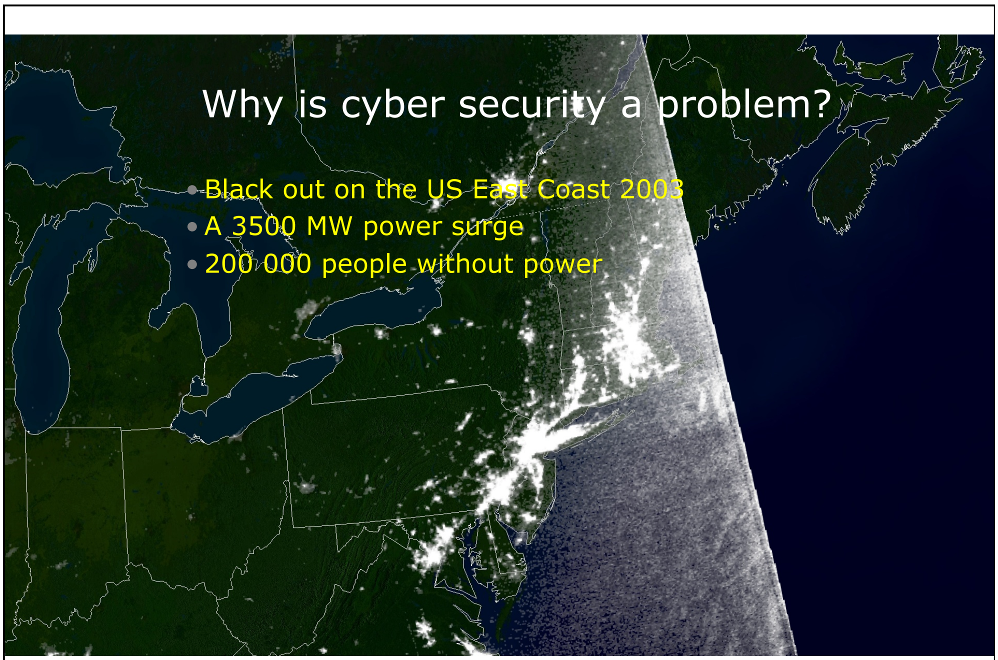
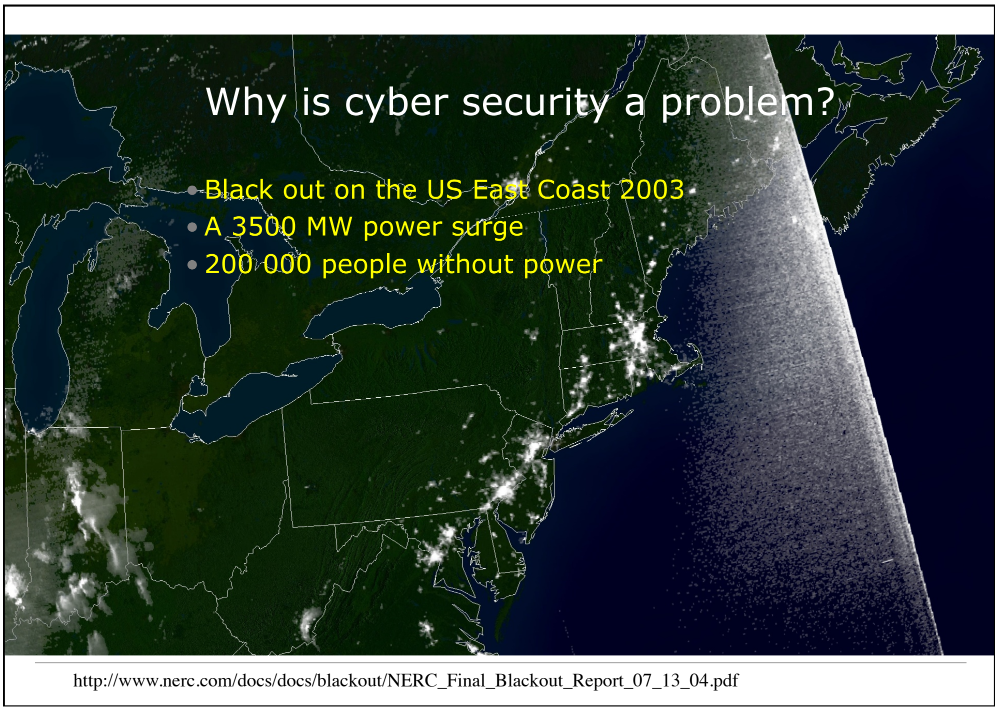
Cyber Security
a brief introduction



Why is cyber security a problem?

- Black out on the US East Coast 2003
- A 3500 MW power surge
- 200 000 people without power

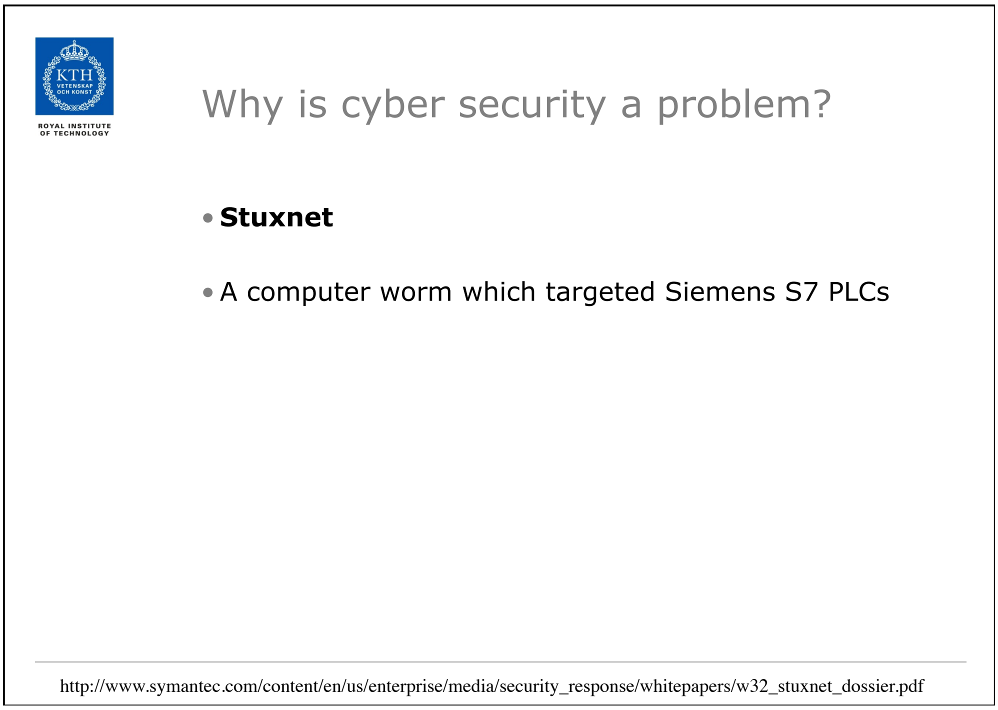
http://www.nerc.com/docs/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf



Why is cyber security a problem?

- Black out on the US East Coast 2003
- A 3500 MW power surge
- 200 000 people without power

http://www.nerc.com/docs/docs/blackout/NERC_Final_Blackout_Report_07_13_04.pdf



Why is cyber security a problem?

- **Stuxnet**
- A computer worm which targeted Siemens S7 PLCs

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

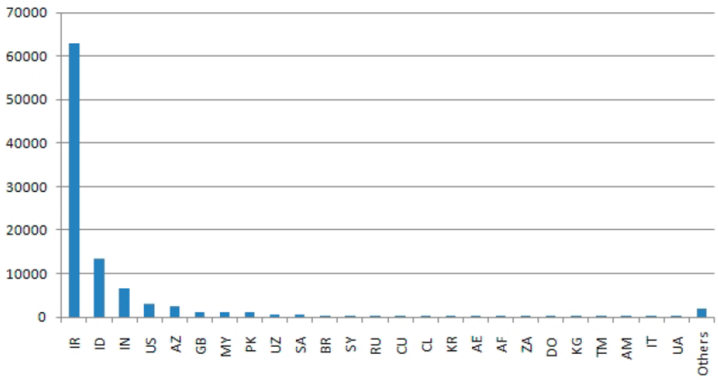
ROYAL INSTITUTE OF TECHNOLOGY

Why is cyber security a problem?

- **Stuxnet**

Figure 1

Infected Hosts



http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

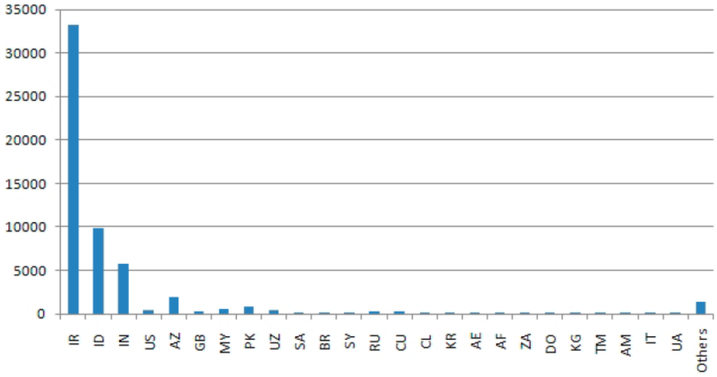
ROYAL INSTITUTE OF TECHNOLOGY

Why is cyber security a problem?

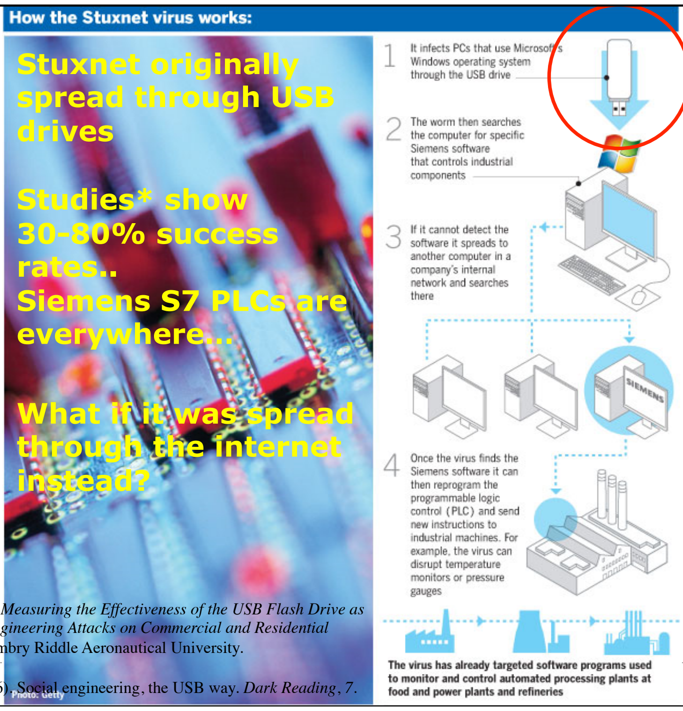
- **Stuxnet**

Figure 2

Infected Organizations (By WAN IP)



http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf



How the Stuxnet virus works:

1 It infects PCs that use Microsoft's Windows operating system through the USB drive

2 The worm then searches the computer for specific Siemens software that controls industrial components

3 If it cannot detect the software it spreads to another computer in a company's internal network and searches there

4 Once the virus finds the Siemens software it can then reprogram the programmable logic control (PLC) and send new instructions to industrial machines. For example, the virus can disrupt temperature monitors or pressure gauges

The virus has already targeted software programs used to monitor and control automated processing plants at food and power plants and refineries

Stuxnet originally spread through USB drives

Studies* show 30-80% success rates..

Siemens S7 PLCs are everywhere…

What if it was spread through the internet instead?

*Jacobs, J. R. (2011). *Measuring the Effectiveness of the USB Flash Drive as a Vector for Social Engineering Attacks on Commercial and Residential Computer Systems*. Embry Riddle Aeronautical University.

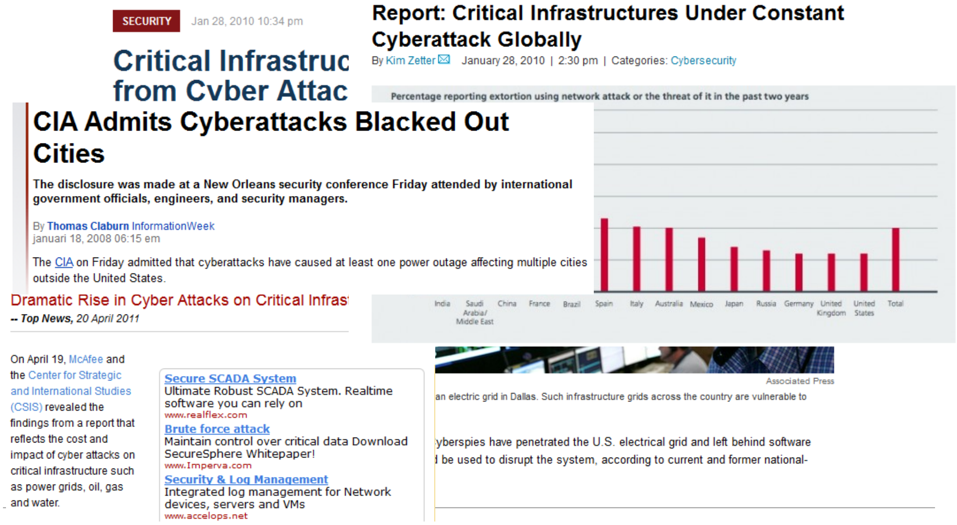
*Stasiukonis, S. (2006). Social engineering, the USB way. *Dark Reading*, 7.

Why is cyber security a problem?

- **Stuxnet**
- A Windows computer worm which targeted Siemens S7 PLCs
- Originally spread through USB-sticks, then peer-2-peer services (e.g. SMB - windows file sharing)
- Masked its presence
  - Only some attacks are identified…

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

Why is cyber security a problem?



SECURITY Jan 28, 2010 10:34 pm

Critical Infrastruc
from Cyber Attac

CIA Admits Cyberattacks Blacked Out Cities

The disclosure was made at a New Orleans security conference Friday attended by international government officials, engineers, and security managers.

By Thomas Claburn InformationWeek
januari 18, 2008 06:15 em

The CIA on Friday admitted that cyberattacks have caused at least one power outage affecting multiple cities outside the United States.

Dramatic Rise in Cyber Attacks on Critical Infras

***-- Top News,** 20 April 2011*

On April 19, McAfee and the Center for Strategic and International Studies (CSIS) revealed the findings from a report that reflects the cost and impact of cyber attacks on critical infrastructure such as power grids, oil, gas and water.

Report: Critical Infrastructures Under Constant Cyberattack Globally

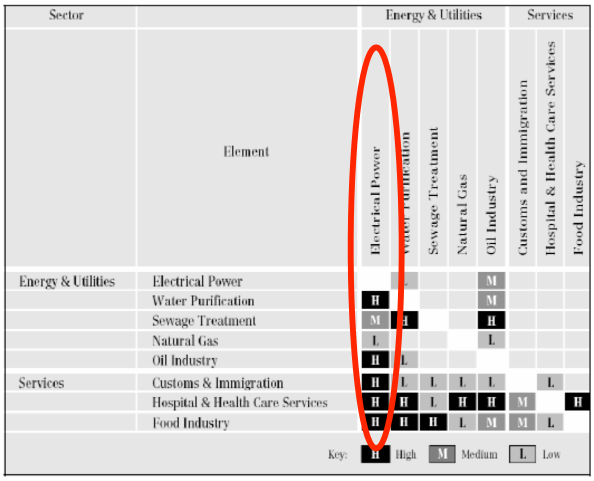
By Kim Zetter ✉ January 28, 2010 | 2:30 pm | Categories: Cybersecurity

Percentage reporting extortion using network attack or the threat of it in the past two years
India
Saudi Arabia/ Middle East
China
France
Brazil
Spain
Italy
Australia
Mexico
Japan
Russia
Germany
United Kingdom
United States
Total
Associated Press

an electric grid in Dallas. Such infrastructure grids across the country are vulnerable to

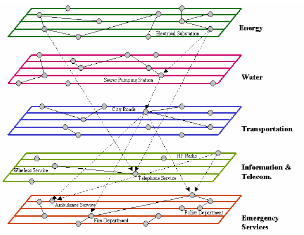
yberspies have penetrated the U.S. electrical grid and left behind software
l be used to disrupt the system, according to current and former national-

It is of national interest



Sector	Element	Energy & Utilities					Services		
		Electrical Power	Water Purification	Sewage Treatment	Natural Gas	Oil Industry	Customs and Immigration	Hospital & Health Care Services	Food Industry
Energy & Utilities	Electrical Power		L			M			
	Water Purification	H				M			
	Sewage Treatment	M	H			H			
	Natural Gas	L				L			
	Oil Industry	H	L						
Services	Customs & Immigration	H	L	L	L	L		L	
	Hospital & Health Care Services	H	H	L	H	H	M		H
	Food Industry	H	H	H	L	M	M	L	

Key: H High M Medium L Low



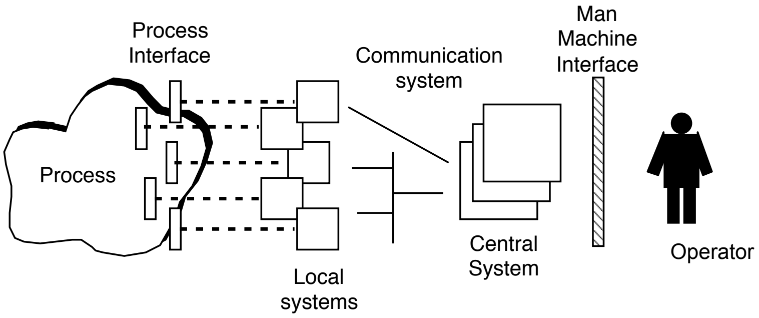
Pederson et al, Critical Infrastructure Interdependency modeling, 2006

Security is mandatory (in the US)

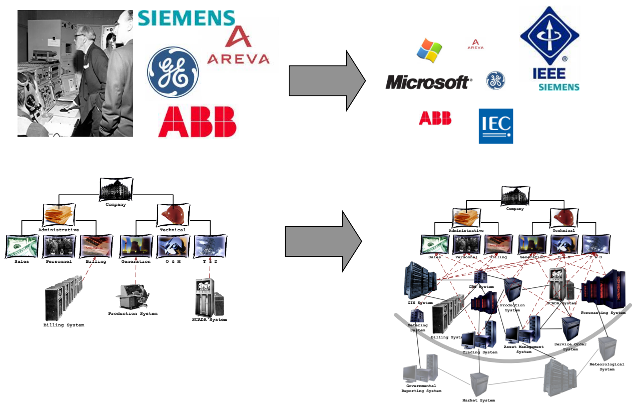
- NERC CIP 001-009 mandatory from 2007:
  - CIP-002 Critical Cyber Assets
  - CIP-003 Security Management Controls
  - CIP-004 Personnel & Training
  - CIP-005 Electronic Security
  - CIP-006 Physical Security of Critical Cyber Assets
  - CIP-007 Systems Security Management
  - CIP-008 Incident Reporting and Response Planning
  - CIP-009 Recovery Plans for Critical Cyber Assets
- Noncompliance = FINES

NERC - (North American Electrical Reliability Corporation)
CIP - (Critical Infrastructure Protection)

SCADA components

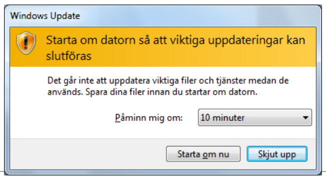


Evolution of SCADA systems



High performance demands!

- Leads to the SCADA system being "soft"
  - The scada system comprise of millions of lines of code
    - Security is not the focus when developing this code…
  - There are lots of third party components
  - Software are rarely updated
  - The operating systems are old and not patched
    - E.g. Windows 2000



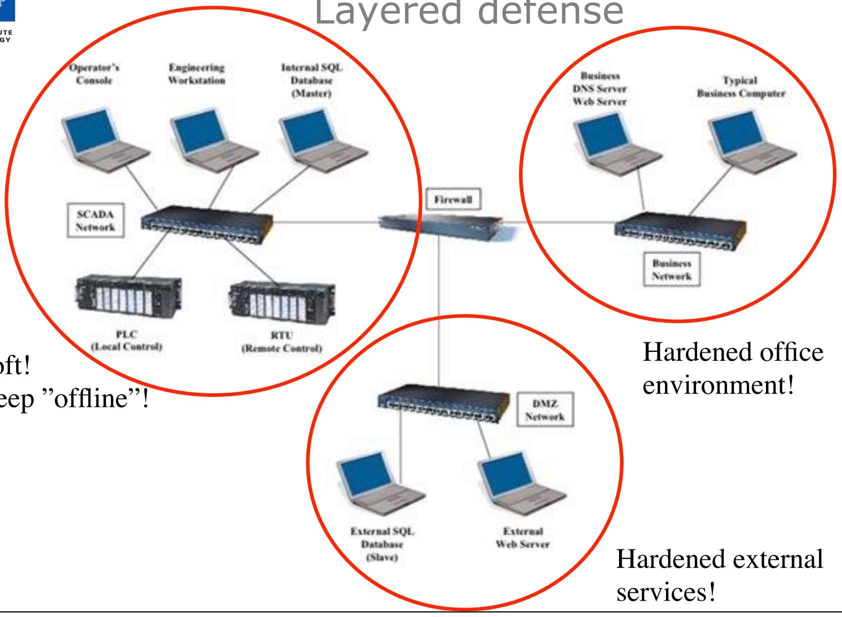
Windows Update

Starta om datorn så att viktiga uppdateringar kan slutföras

Det går inte att uppdatera viktiga filer och tjänster medan de används. Spara dina filer innan du startar om datorn.

Påminn mig om: 10 minuter

Layered defense



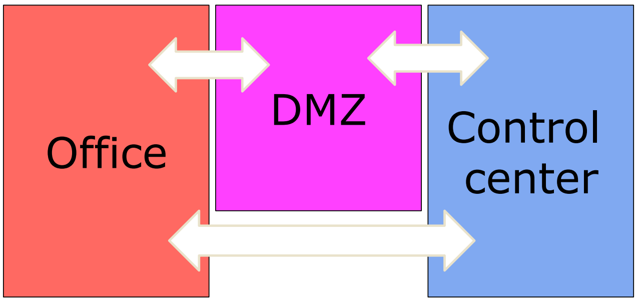
Soft!
Keep ”offline”!

Hardened office
environment!

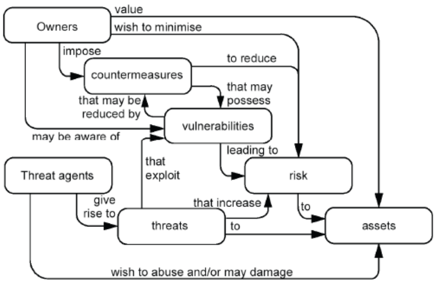
Hardened external
services!

The DMZ

- A problem: There are often no real DMZ

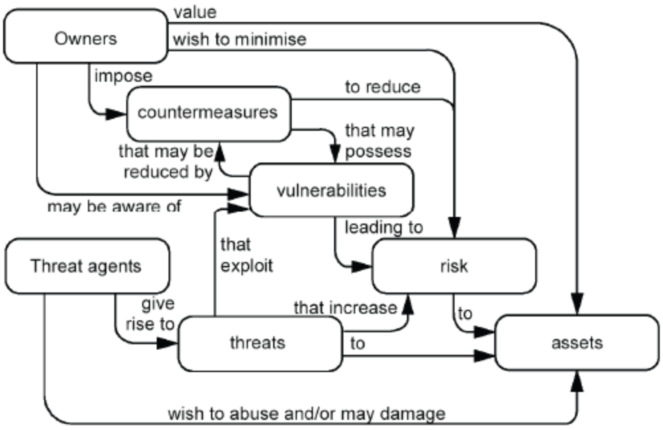


Today’s lecture – cyber security risk analysis

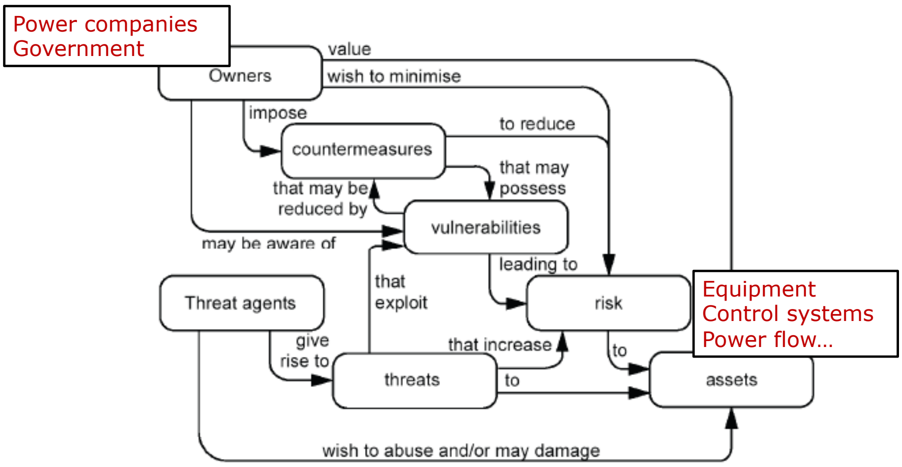


- Some basic preconditions
- We do a risk analysis
  - Threats
  - Consequences
  - Vulnerabilities
  - Countermeasures
- Summary

The security field



The SCADA security field



Power companies
Government

Owners

value

wish to minimise

impose

countermeasures

to reduce

that may possess

that may be reduced by

vulnerabilities

may be aware of

leading to

that exploit

Threat agents

risk

give rise to

that increase

to

threats

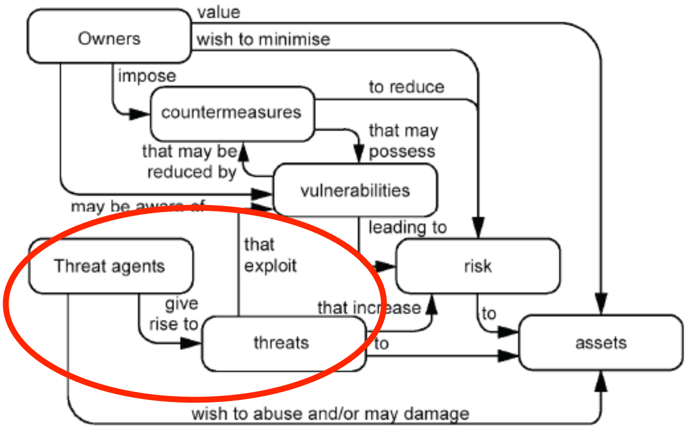
to

assets

wish to abuse and/or may damage

Equipment
Control systems
Power flow…

The threats



Owners

value

wish to minimise

impose

countermeasures

to reduce

that may possess

that may be reduced by

vulnerabilities

may be aware of

leading to

that exploit

Threat agents

risk

give rise to

that increase

to

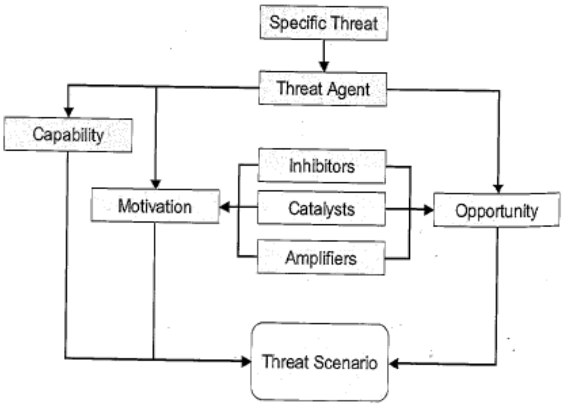
threats

to

assets

wish to abuse and/or may damage

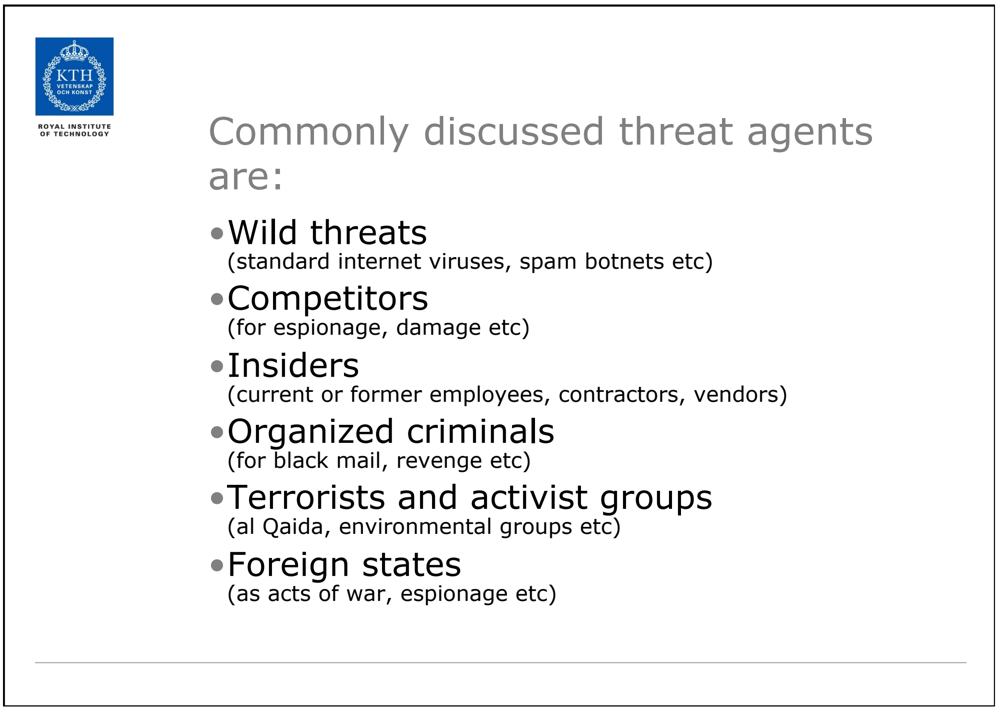
Components to consider



Source: Sherwood, Clark, Lynas, Enterprise security architecture

Bzzz…

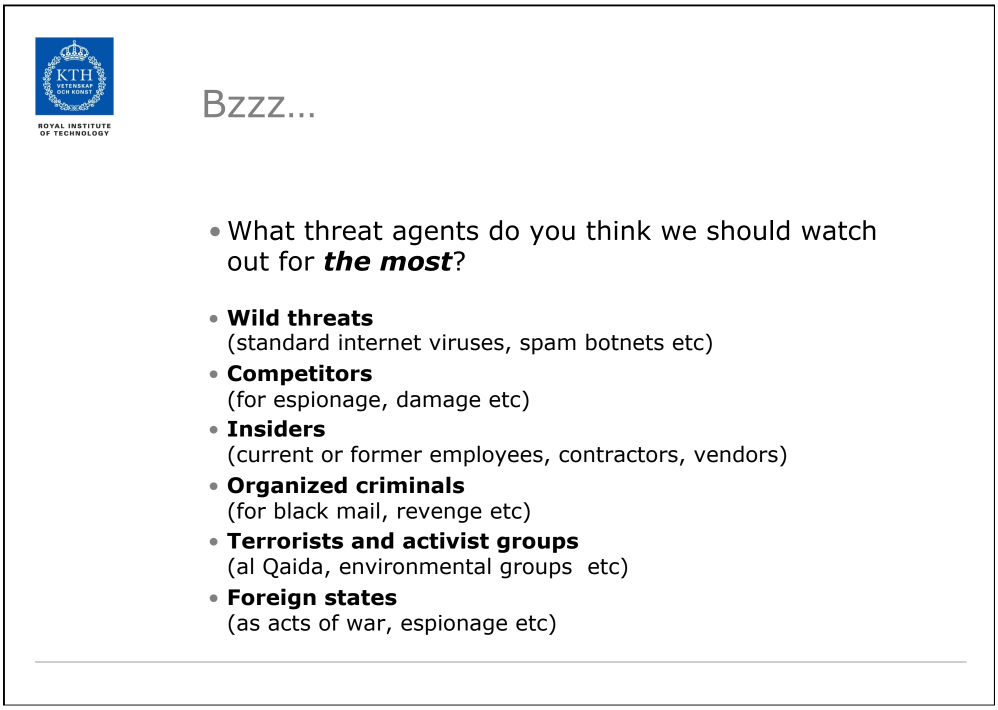
- What threat agents do you think we should watch out for?



ROYAL INSTITUTE OF TECHNOLOGY

Commonly discussed threat agents are:

- Wild threats
  (standard internet viruses, spam botnets etc)
- Competitors
  (for espionage, damage etc)
- Insiders
  (current or former employees, contractors, vendors)
- Organized criminals
  (for black mail, revenge etc)
- Terrorists and activist groups
  (al Qaida, environmental groups etc)
- Foreign states
  (as acts of war, espionage etc)

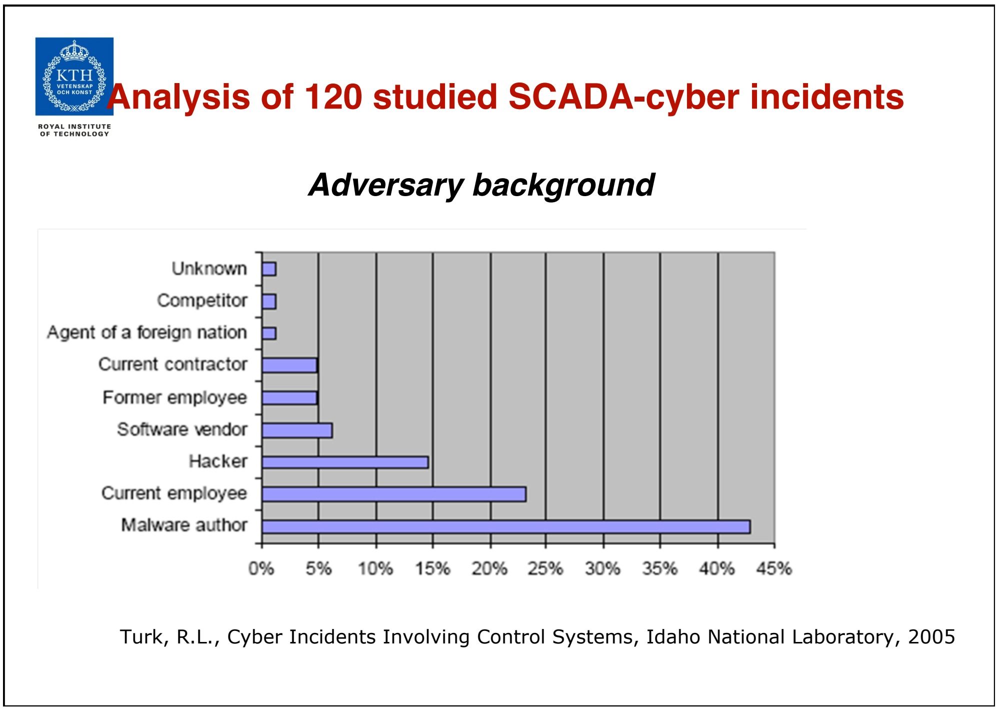


ROYAL INSTITUTE OF TECHNOLOGY

Bzzz…

- What threat agents do you think we should watch out for ***the most***?

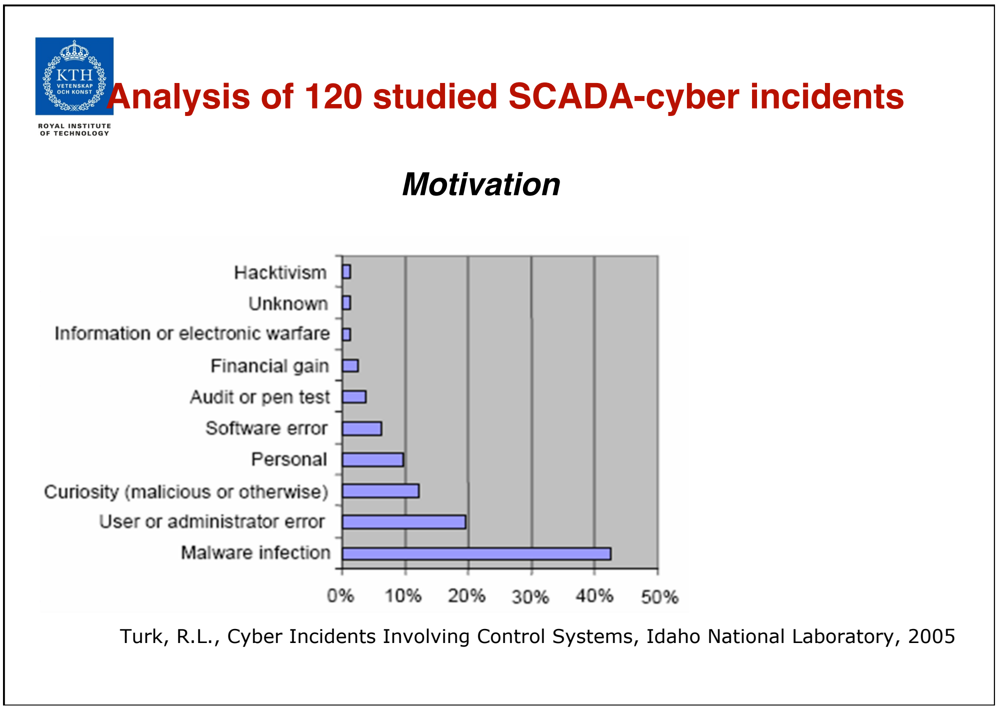
- **Wild threats**
  (standard internet viruses, spam botnets etc)
- **Competitors**
  (for espionage, damage etc)
- **Insiders**
  (current or former employees, contractors, vendors)
- **Organized criminals**
  (for black mail, revenge etc)
- **Terrorists and activist groups**
  (al Qaida, environmental groups etc)
- **Foreign states**
  (as acts of war, espionage etc)



Analysis of 120 studied SCADA-cyber incidents

Adversary background

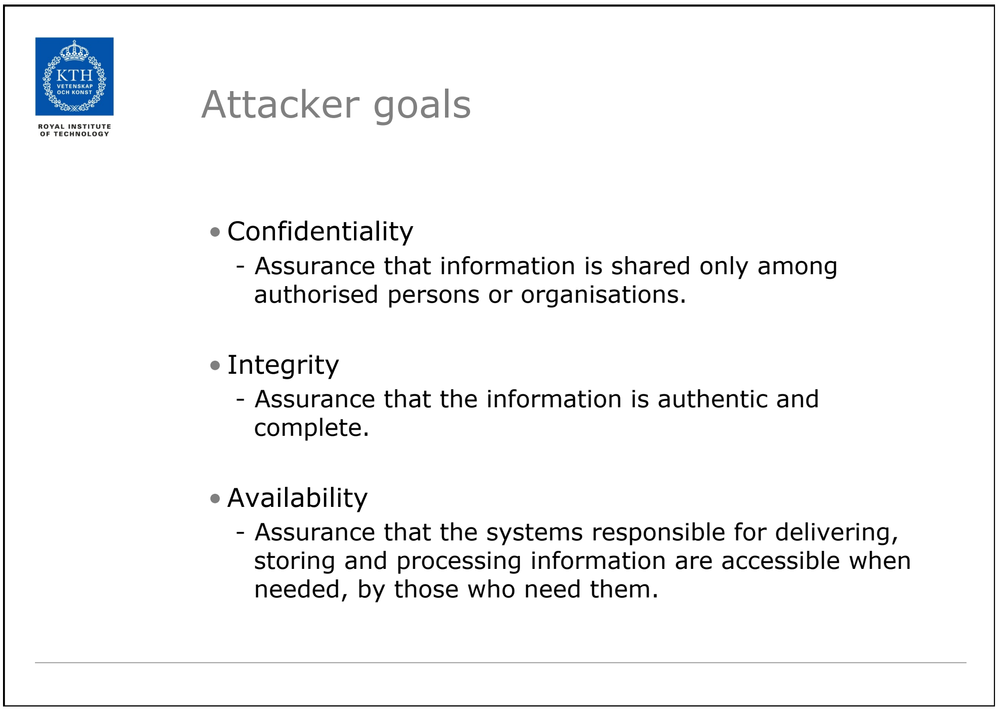
Turk, R.L., Cyber Incidents Involving Control Systems, Idaho National Laboratory, 2005



Analysis of 120 studied SCADA-cyber incidents

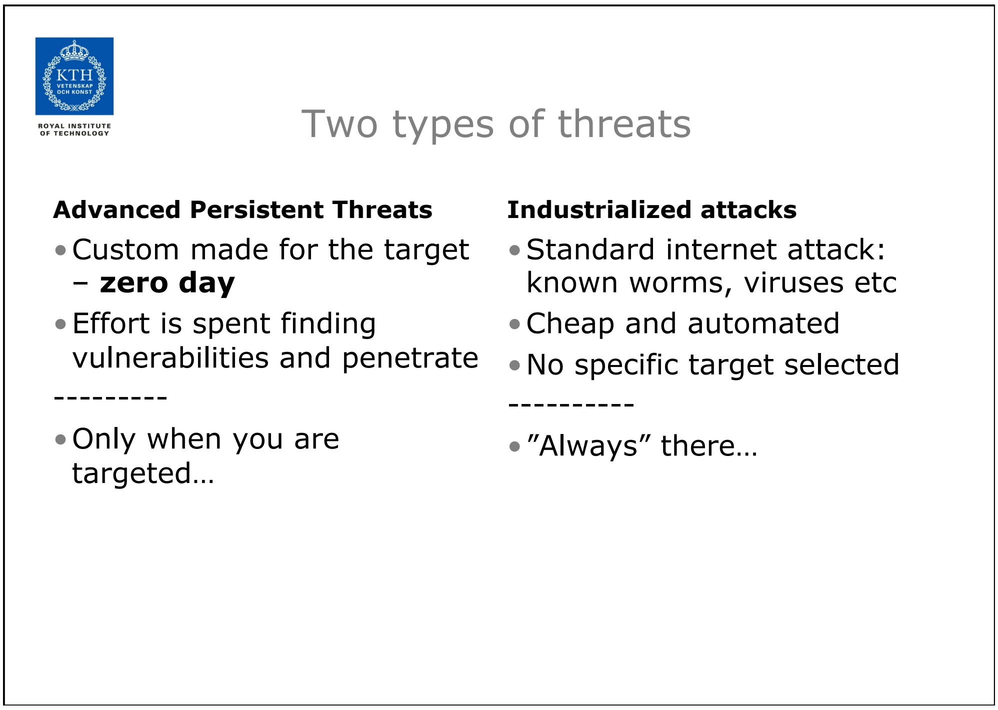
Motivation

Turk, R.L., Cyber Incidents Involving Control Systems, Idaho National Laboratory, 2005



Attacker goals

- Confidentiality
  - Assurance that information is shared only among authorised persons or organisations.
- Integrity
  - Assurance that the information is authentic and complete.
- Availability
  - Assurance that the systems responsible for delivering, storing and processing information are accessible when needed, by those who need them.



Two types of threats

Advanced Persistent Threats

- Custom made for the target – **zero day**
- Effort is spent finding vulnerabilities and penetrate

- Only when you are targeted…

Industrialized attacks

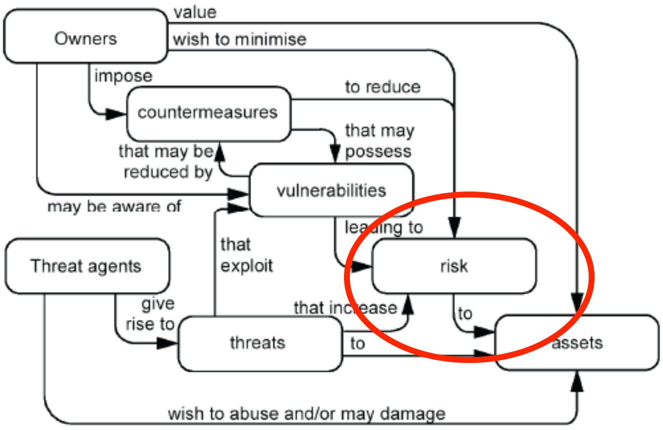
- Standard internet attack: known worms, viruses etc
- Cheap and automated
- No specific target selected

- ”Always” there…

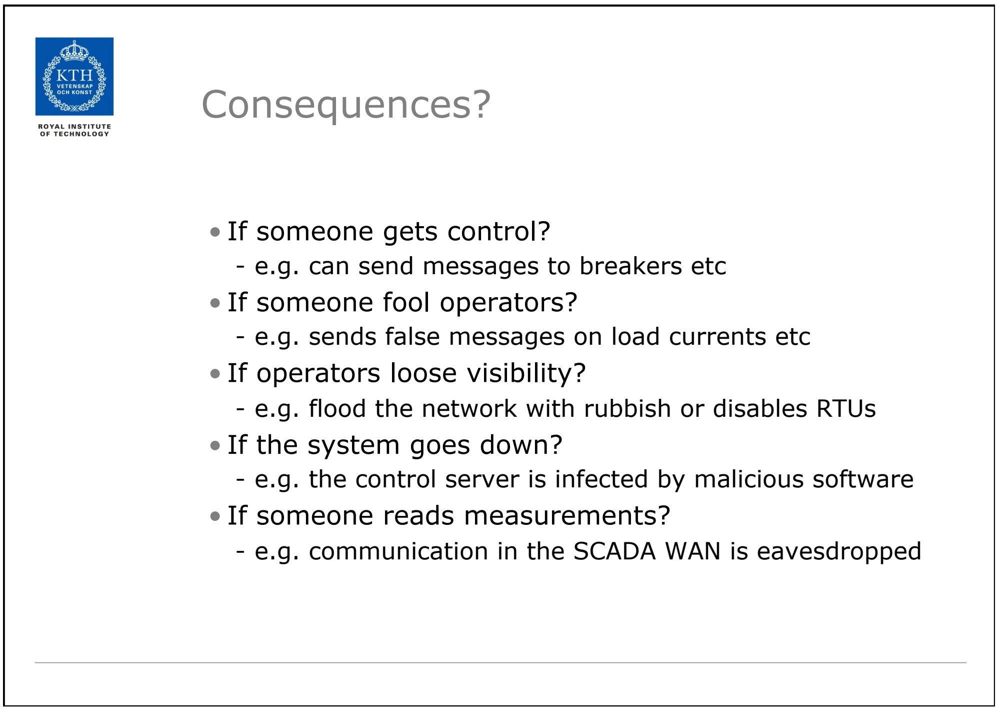
Advanced and persistent?

- Wild threats
  (standard internet viruses, spam botnets etc)
- Competitors
  (for espionage, damage etc)
- Insiders
  (current or former employees, contractors, vendors)
- Organized criminals
  (for black mail, revenge etc)
- Terrorists and activist groups
  (al Qaida, environmental groups etc)
- Foreign states
  (as acts of war, espionage etc)

The consequences

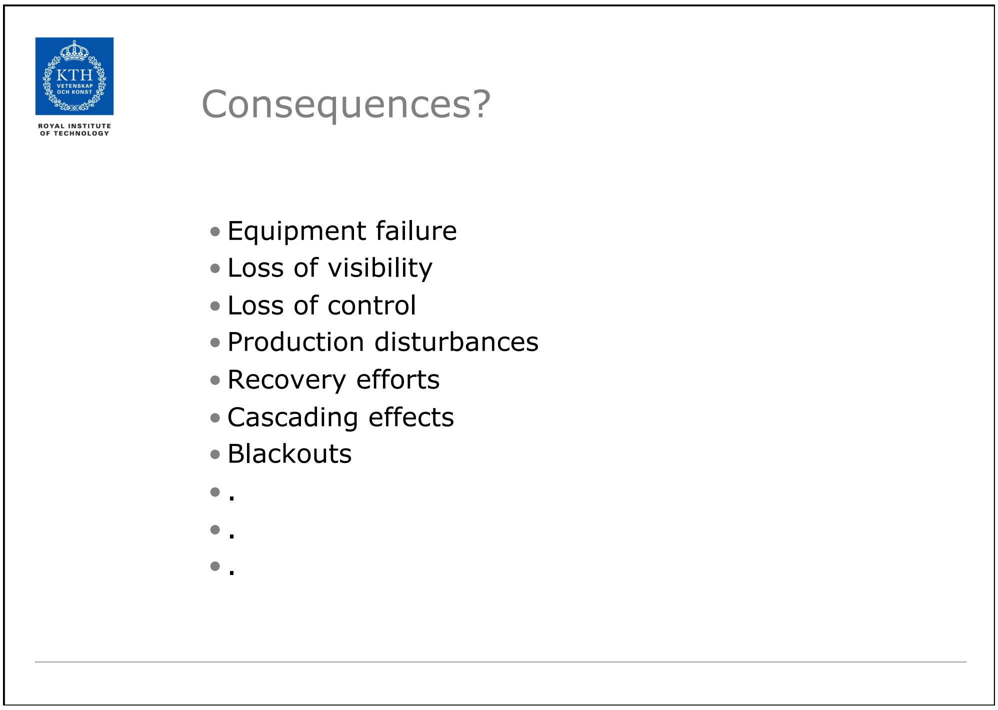


Owners
value
wish to minimise
impose
countermeasures
to reduce
that may possess
that may be reduced by
vulnerabilities
may be aware of
leading to
risk
Threat agents
that exploit
give rise to
threats
that increase
to
to
assets
wish to abuse and/or may damage



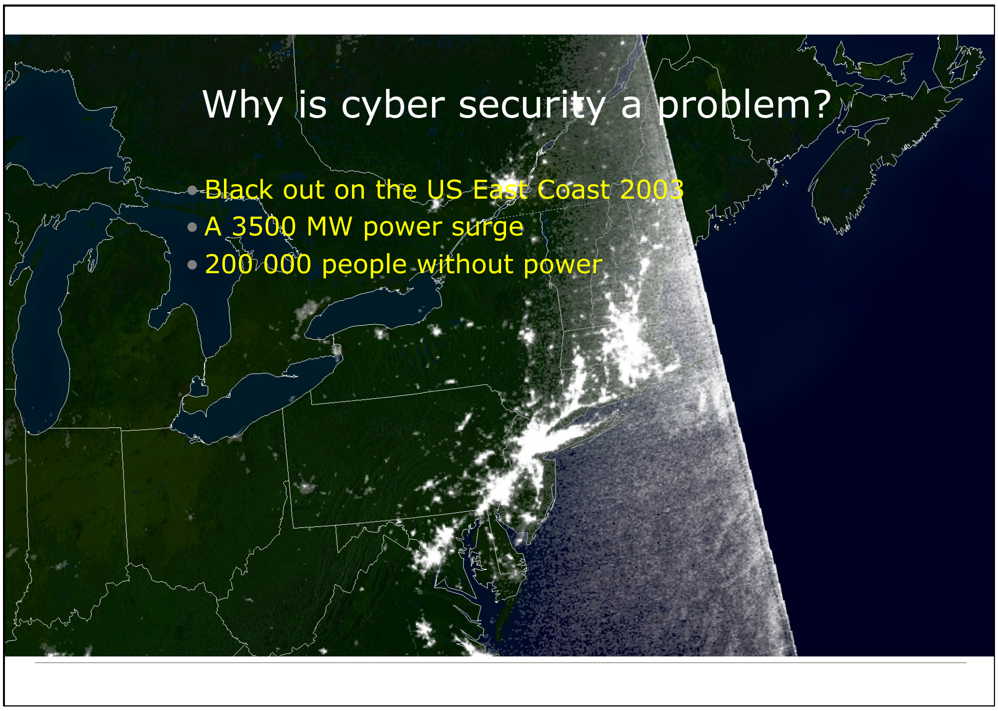
Consequences?

- If someone gets control?
  - e.g. can send messages to breakers etc
- If someone fool operators?
  - e.g. sends false messages on load currents etc
- If operators loose visibility?
  - e.g. flood the network with rubbish or disables RTUs
- If the system goes down?
  - e.g. the control server is infected by malicious software
- If someone reads measurements?
  - e.g. communication in the SCADA WAN is eavesdropped



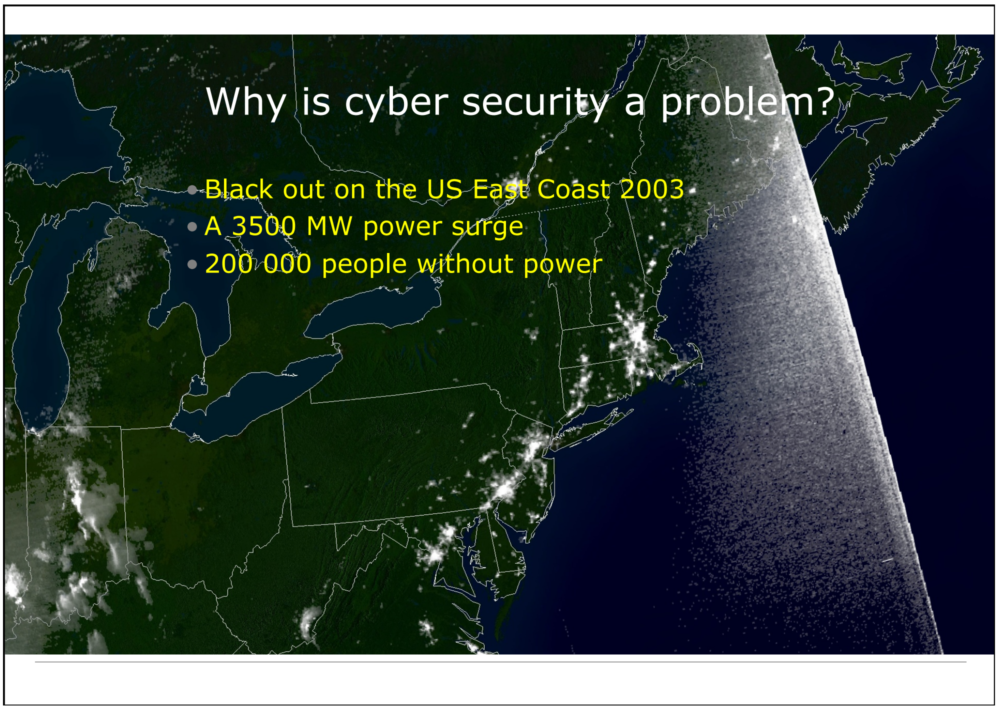
Consequences?

- Equipment failure
- Loss of visibility
- Loss of control
- Production disturbances
- Recovery efforts
- Cascading effects
- Blackouts
- .
- .
- .



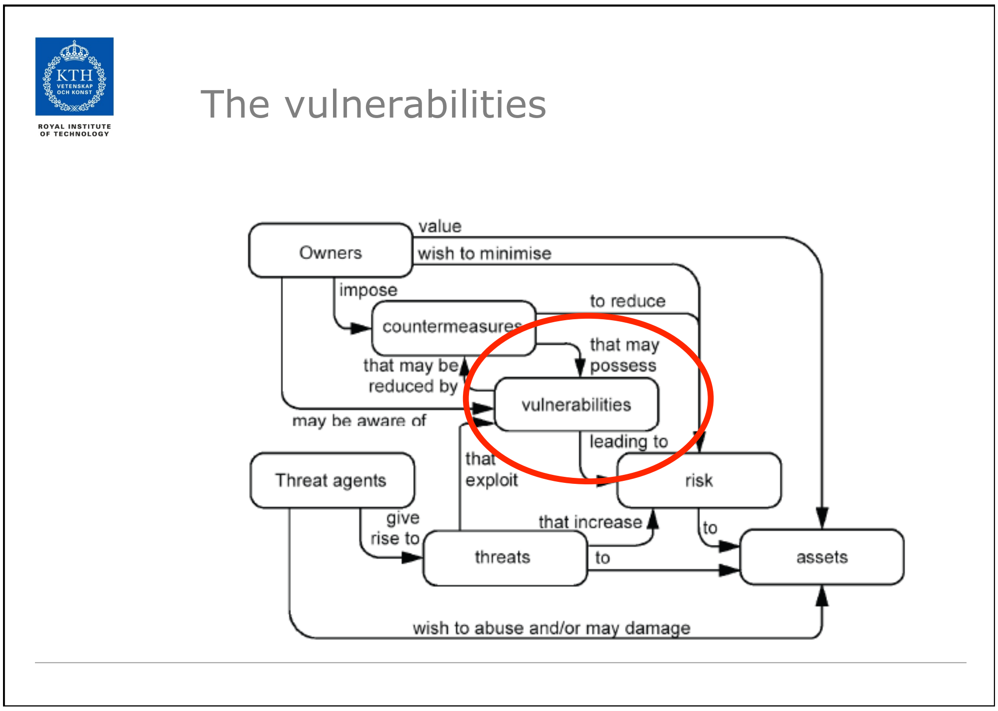
Why is cyber security a problem?

- Black out on the US East Coast 2003
- A 3500 MW power surge
- 200 000 people without power

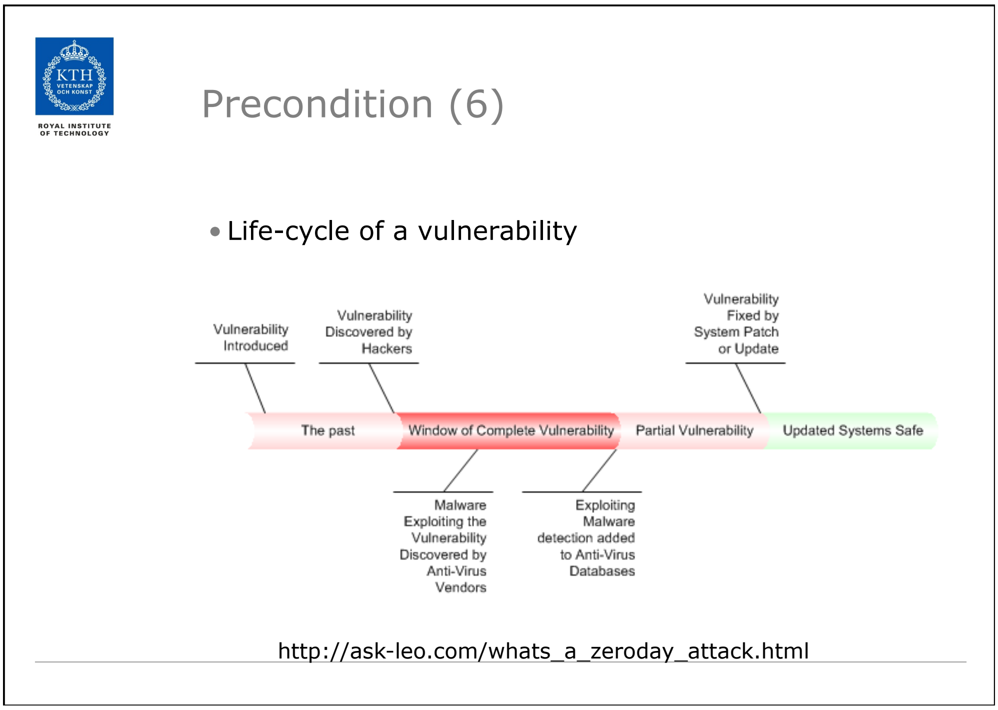


Why is cyber security a problem?

- Black out on the US East Coast 2003
- A 3500 MW power surge
- 200 000 people without power



The vulnerabilities



Precondition (6)

- Life-cycle of a vulnerability

Vulnerability Introduced
Vulnerability Discovered by Hackers
Vulnerability Fixed by System Patch or Update
The past
Window of Complete Vulnerability
Partial Vulnerability
Updated Systems Safe
Malware Exploiting the Vulnerability Discovered by Anti-Virus Vendors
Exploiting Malware detection added to Anti-Virus Databases

http://ask-leo.com/whats_a_zeroday_attack.html

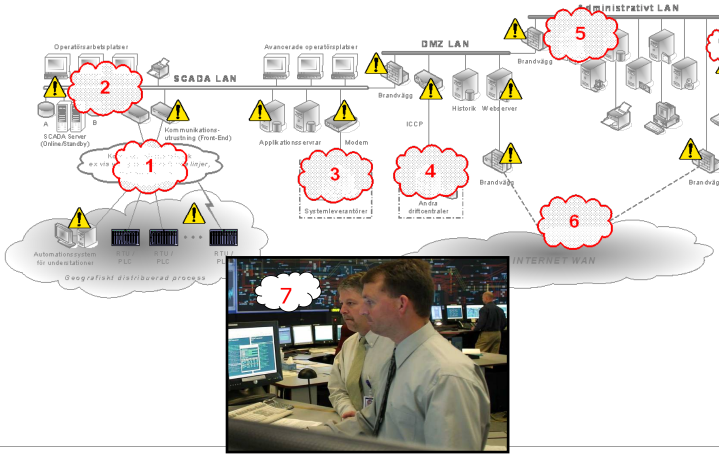
ROYAL INSTITUTE OF TECHNOLOGY

Bzzz…

- What vulnerabilities do you think exist?

ROYAL INSTITUTE OF TECHNOLOGY

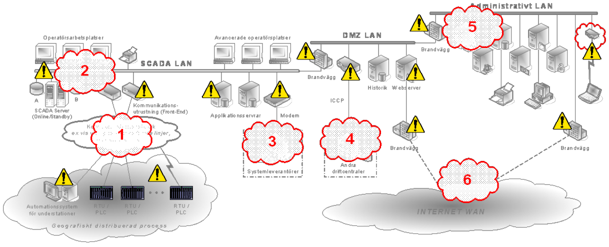
Vulnerabilities



ROYAL INSTITUTE OF TECHNOLOGY

Bzzz…

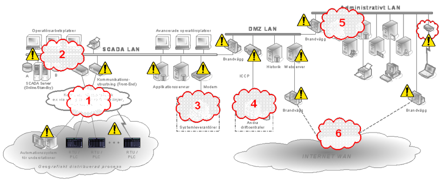
- What vulnerabilities do you think people should ***be most concerned about***?



ROYAL INSTITUTE OF TECHNOLOGY

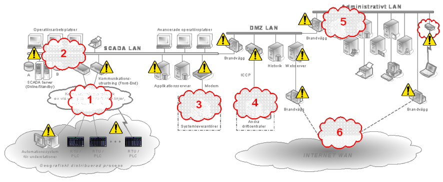
1 – The SCADA Network

- Geographically dispersed – physcial access
- Unauthicated communciation
- Rogue connections
- Over different mediums



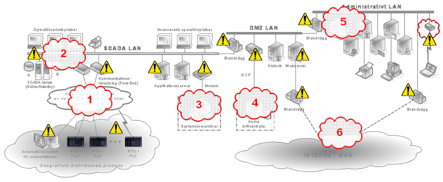
2 – The control center

- Physical access
- Unnecessary services activated
- Unpatched OS and software
- Antivirus software, security functionality inactivated
- Passwords and access control
- Authorization
- Rogue connections



3,4, 6 – External connections

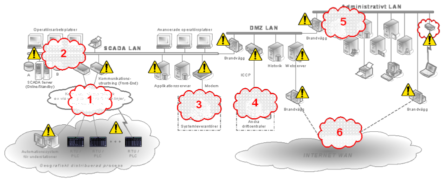
- Access (over there)
- Network segmentation
- Firewall configurations
- Access control (passwords/keys)



ROYAL INSTITUTE OF TECHNOLOGY

5 – The Office LAN

- Access control
- Network segmentation
- Firewall configurations
- Access control (passwords/keys)
- Rogue connections
- And everything else

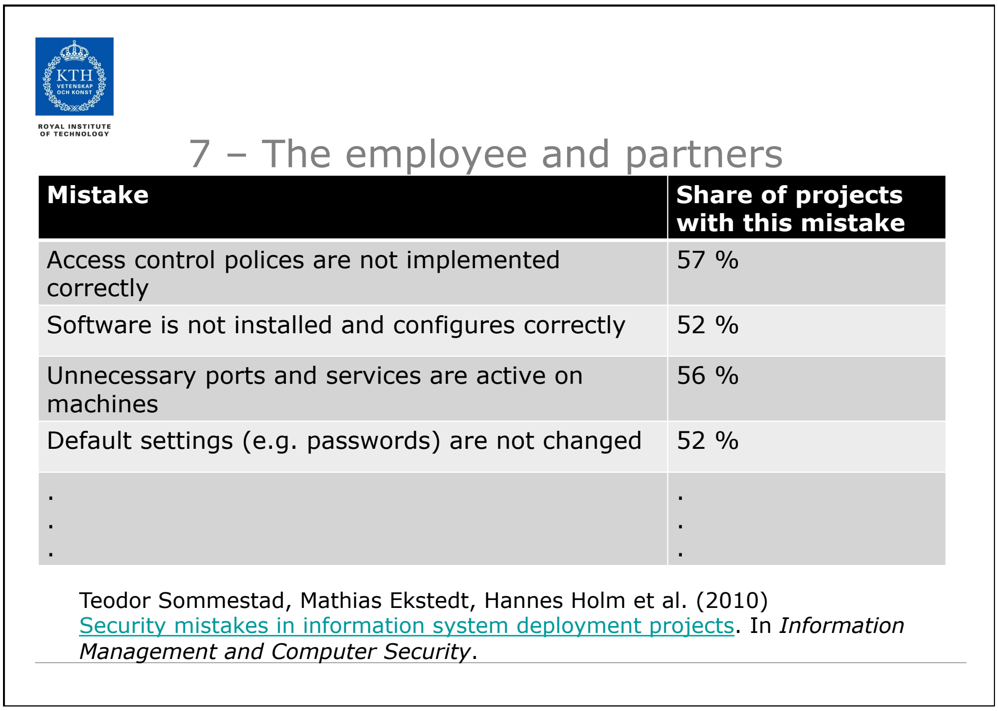


ROYAL INSTITUTE OF TECHNOLOGY

7 – The employee and partners

- Lack of policies
- Lack of access management
- Lack of logging
- Lack of training

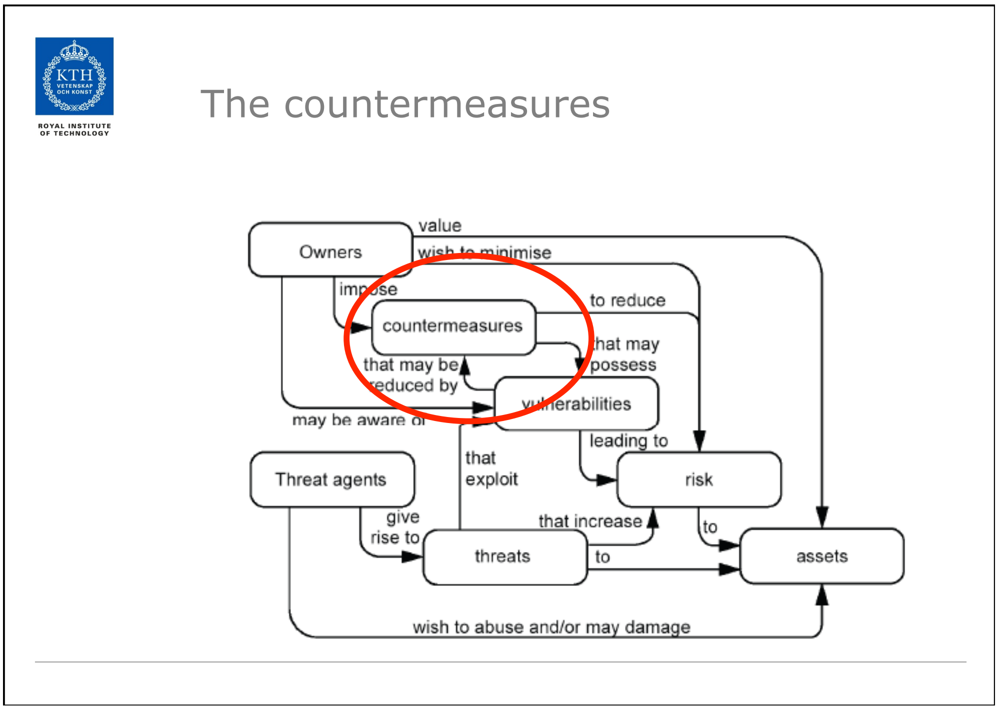
- **“The weakest link”**



7 – The employee and partners

Mistake	Share of projects with this mistake
Access control polices are not implemented correctly	57 %
Software is not installed and configures correctly	52 %
Unnecessary ports and services are active on machines	56 %
Default settings (e.g. passwords) are not changed	52 %
. . .	. . .

Teodor Sommestad, Mathias Ekstedt, Hannes Holm et al. (2010) Security mistakes in information system deployment projects. In *Information Management and Computer Security*.



The countermeasures

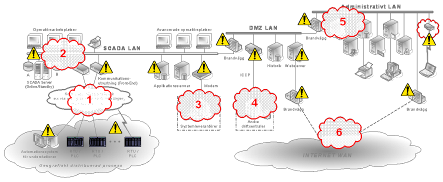
Countermeasures…

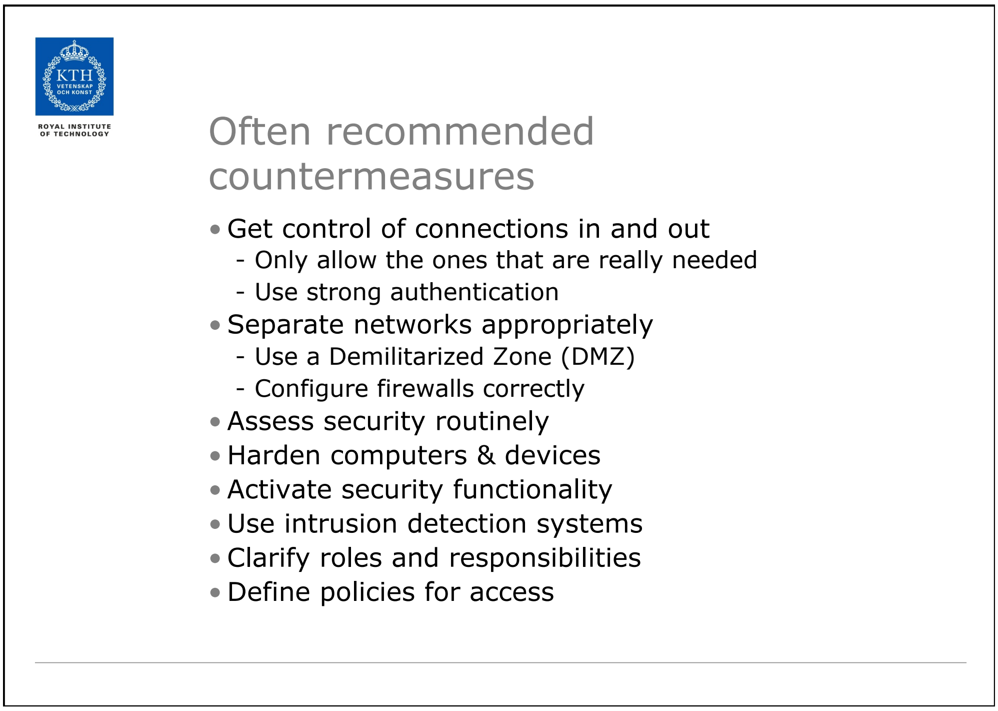
Digital signatures
Passwords policies
Biometrics
Response planning
DMZ
Information security policy
Defense-in-depth
Privacy
Authentication
Procedures
Anti-virus software
Identity management
Network segregation
Honeypots
Attack surface
Access control
Authorization
Continuity planning
Media access control
Access tokens
Access logs
Gateways
Smartcards
Physical protection
Certificates
Device authentication
Firewalls
Media redeployment
Security training
Communication protection
Packet filters
Perimeter protection
Security awareness
Separation of duties
Recovery planning
Cryptography
Mandatory access control
Intrusion detection
Personnel screening
Forensics
Alarm systems
Security Architecture
Monitoring and assessment
Discretional access control
Security domains
Log retention
Patch updating
System hardening
Password qualities
Information classification
Video recording
Media disposal

Bzzz…

- What countermeasures do you think utilities should focus on?

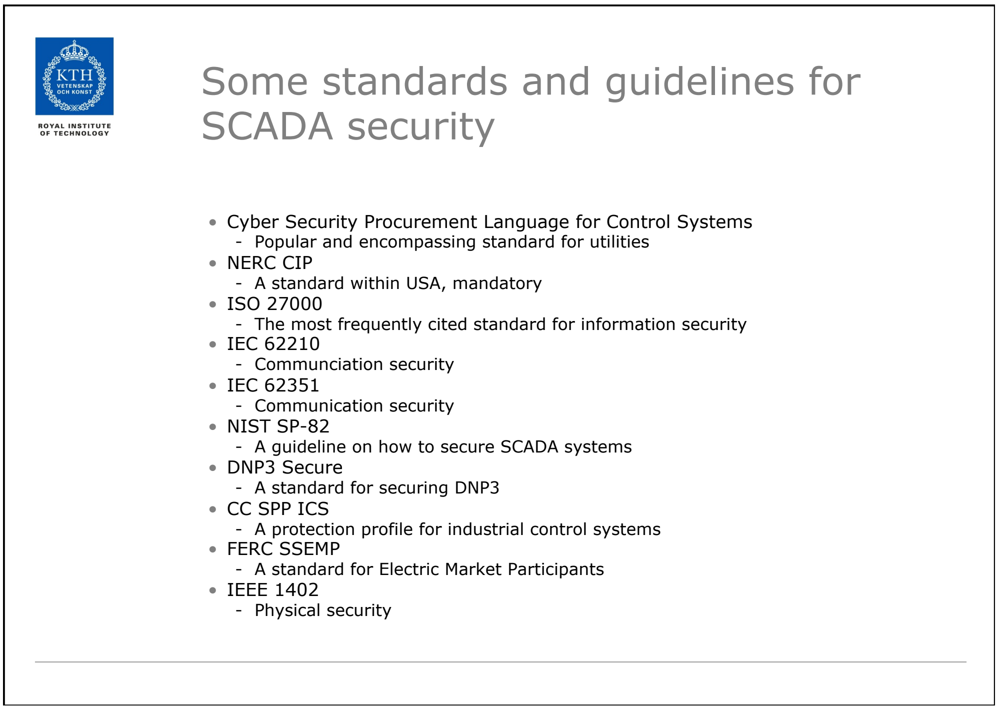
Communication protection
Packet filters
Security awareness
Perimeter protection
Anti-virus software
Separation of duties
Recovery planning
Cryptography
Mandatory access control
Intrusion detection
Access logs
Personnel screening
Information security policy
Forensics
Alarm systems
Media access control
Security Architecture
Defense-in-depth
Biometrics
Network segregation
Monitoring and assessment
Discretional access control
Security domains
DMZ
Identity management
IDS
Honeypots
Log retention
Access tokens
Authentication
Patch updating
System hardening
Access control
Password qualities
Gateways
Procedures
Information classification
Privacy
Digital signatures
Passwords policies
Video recording
Response planning
Media disposal
Attack surface
Continuity planning
Authorization
Device authentication
Security training
Smartcards
Physical protection
Firewalls
Certificates
Media redeployment





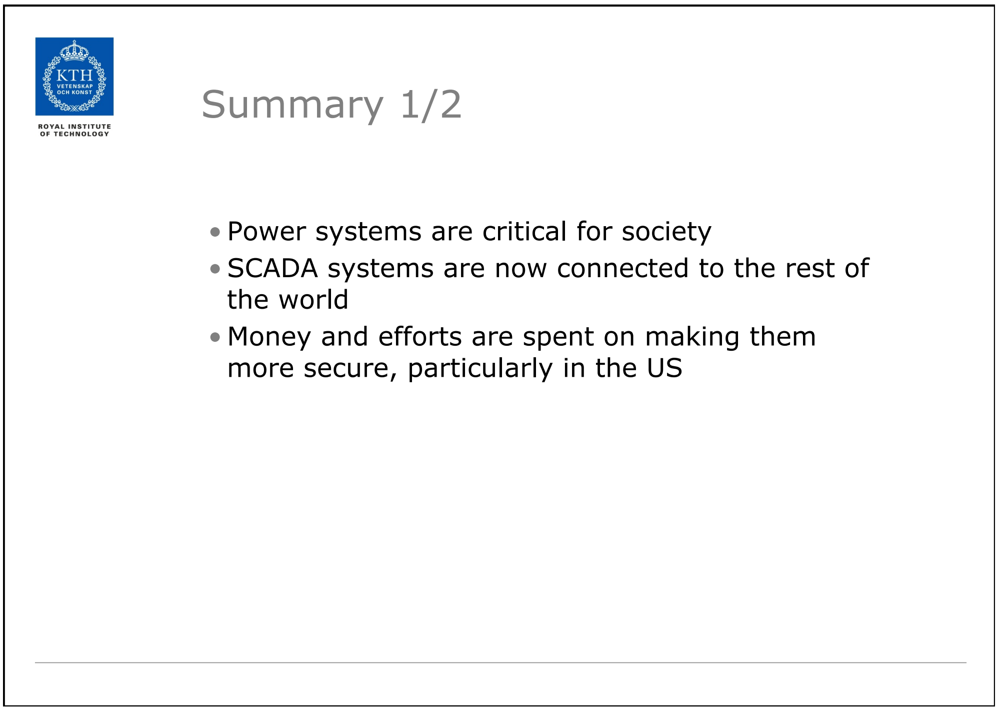
Often recommended countermeasures

- Get control of connections in and out
  - Only allow the ones that are really needed
  - Use strong authentication
- Separate networks appropriately
  - Use a Demilitarized Zone (DMZ)
  - Configure firewalls correctly
- Assess security routinely
- Harden computers & devices
- Activate security functionality
- Use intrusion detection systems
- Clarify roles and responsibilities
- Define policies for access



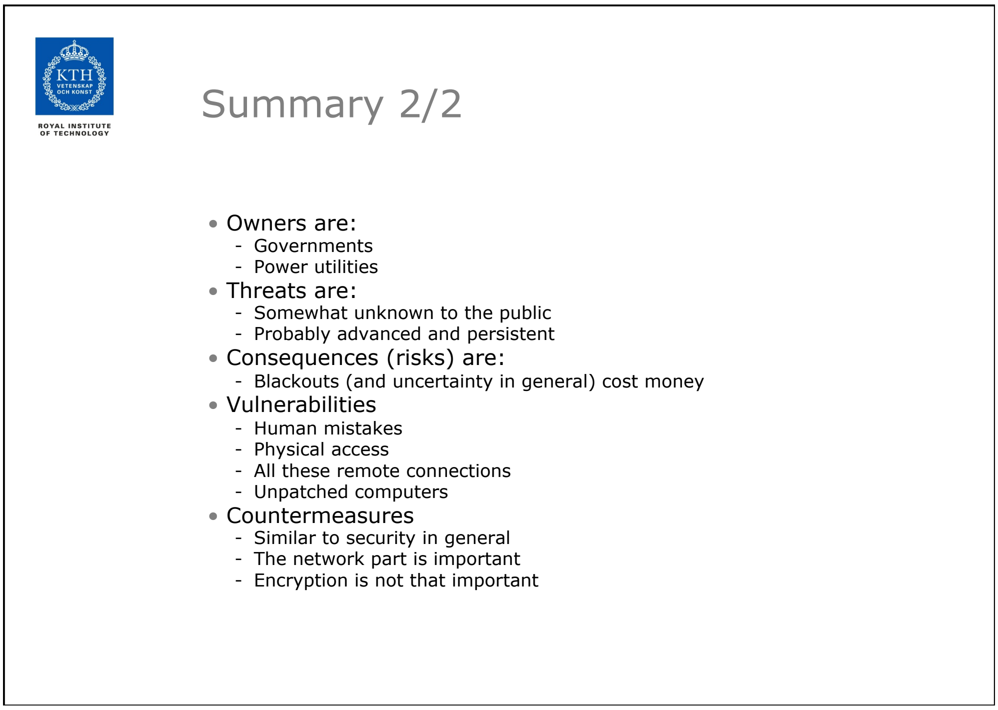
Some standards and guidelines for SCADA security

- Cyber Security Procurement Language for Control Systems
  - Popular and encompassing standard for utilities
- NERC CIP
  - A standard within USA, mandatory
- ISO 27000
  - The most frequently cited standard for information security
- IEC 62210
  - Communciation security
- IEC 62351
  - Communication security
- NIST SP-82
  - A guideline on how to secure SCADA systems
- DNP3 Secure
  - A standard for securing DNP3
- CC SPP ICS
  - A protection profile for industrial control systems
- FERC SSEMP
  - A standard for Electric Market Participants
- IEEE 1402
  - Physical security



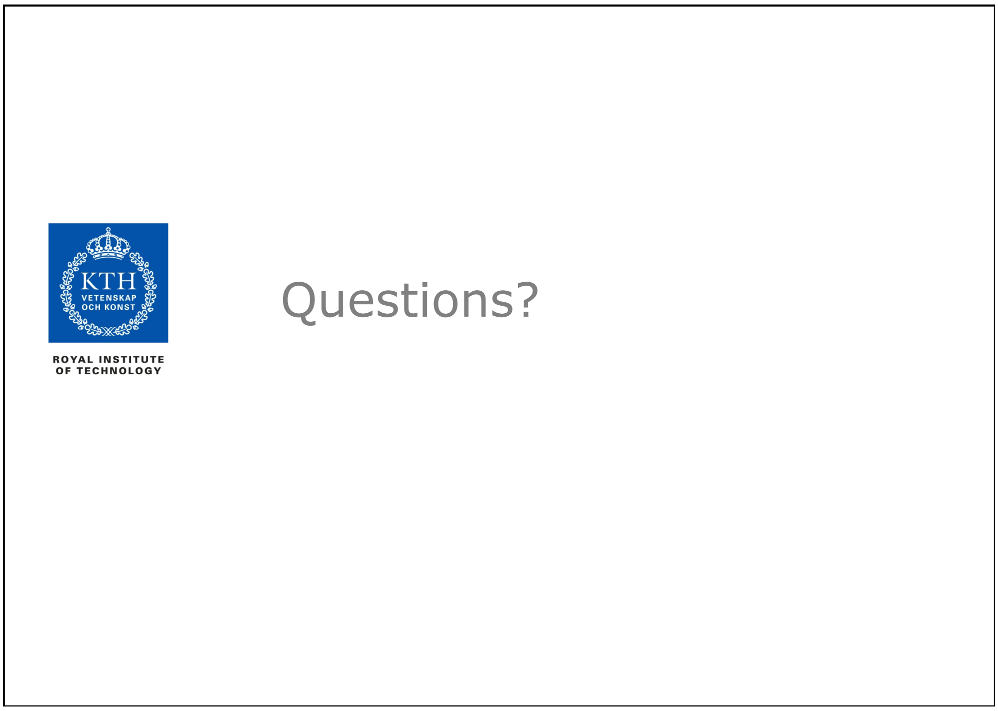
Summary 1/2

- Power systems are critical for society
- SCADA systems are now connected to the rest of the world
- Money and efforts are spent on making them more secure, particularly in the US



Summary 2/2

- Owners are:
  - Governments
  - Power utilities
- Threats are:
  - Somewhat unknown to the public
  - Probably advanced and persistent
- Consequences (risks) are:
  - Blackouts (and uncertainty in general) cost money
- Vulnerabilities
  - Human mistakes
  - Physical access
  - All these remote connections
  - Unpatched computers
- Countermeasures
  - Similar to security in general
  - The network part is important
  - Encryption is not that important



KTH VETENSKAP OCH KONST

ROYAL INSTITUTE OF TECHNOLOGY

Questions?