‘Absence of the Normal, Presence of the Abnormal’

Presented by Tim Harwood
2nd December 2013
Agenda

• Context
• What to look for
  – Physical
  – Digital
• Summary
Sun Tzu says....

• Know your Enemy
• Well actually.....
• ‘It is said that if you know your enemy and know yourself, you will not be imperiled in a hundred battles; .......if you do not know your enemies nor yourself, you will imperiled in every single battle’
Traditional IT

It used to be about the

- C Confidentiality
- I Integrity
- A Availability

of data and has traditionally been the domain of the IT department.
ICS changes this

Cyber security in the ICS environment is about much more than just protecting data.

It is about:

• Ensuring the safe and reliable operation of plant
• Protection of people, the environment and production from cyber security threats.

It is much more about availability than confidentiality.
The Firewall Protects!!
Or is it really....
Human Vulnerabilities

Humans, just like other operating systems, have vulnerabilities, but they are psychological ones, not technical ones

– Humans overestimate risk for highly visual events
– Humans overestimate risk for events in which they are not in control
1 in 251,800,000

Source: http://www.bookofodds.com/content/view/full/252163
in 112,000,000

Source: http://www.bookofodds.com/content/view/full/252163
Imagine.....

- You are sat in the control room in front of your screen and this happens...
What do you do?......

- Most sites have a Loss of View procedure which gives guidance for operators to follow (don’t they?)
But Loss of View is Easy...

• It’s highly visual
• Happens quite regularly
• But what do you do if this happens....
This system is shutting down. Please save all work in progress and log off. Any unsaved changes will be lost. This shutdown was initiated by NT AUTHORITY\SYSTEM.

Time before shutdown: 00:00:56

Message
The system process 'C:\WINDOWS\system32\lsass.exe' terminated unexpectedly with status code 0. The system will now shut down and restart.
The Consequence is......

• Without fully understanding your system(s) and what they should look like under normal operating conditions you place your ICS (and wider networks) at risk
What to look for

- Physical
- Digital
Physical

• What peripherals are attached to your systems, including under the desk!!
• Who has access to which system?
Look for the ‘Out of Place’
Digital - New

• If you have a new (ish) system, what were the results from the FAT/UAT?
• This will give you with a baseline with which to work from.
Digital - Older

• If you have an older system, what processes are running on what you consider to be a ‘normal’ day.

• Take readings on several days – print them off!
Digital

• Everyone talks about Stuxnet but what did it look like? Or Shamoon?

• Shamoon used a 2 stage attack
  – Infected a computer and turns it into a proxy to communicate back to C&C server
  – Branches out to connected computers and steals information
  – Executes payload and wipes machines
  – Communicates this to the C&C server
Physical/Digital - Vendors

• What is your site process for vendors updating the system?
• What do they carry in terms of ID and do you know them personally?
• ‘Never smile at a crocodile who is smiling at you’
Strategy

• Your people are one of your most important assets – and also one of your biggest vulnerabilities

• Schedule regular (quarterly) awareness sessions – invite your vendors

• This should include situational awareness

• Any changes should also be reflected in your policies

• Be aware of the skills shortage that is coming
George Bernard Shaw

“The single biggest problem in communication is the illusion that it has taken place”
Summary

• You are one of the first lines of defence – become a Human Sensor
• Understand your system, get to know it
• Get to know what is attached to it and what should not be there
• Understand what is happening out on the Wild, Wild Web
• What do you do when the worst happens?
Back to Sun Tzu

• If you don’t learn all about your systems (*know thyself*..)
  and the enemy do .....