# Defending Critical Infrastructure : SCADA Attacks

Sqn Ldr Shouqi (Retd)
Chief Defence Architect , APAC

© 2011 Cisco and/or its affiliates. All rights reserved.

# Agenda

Define the threat

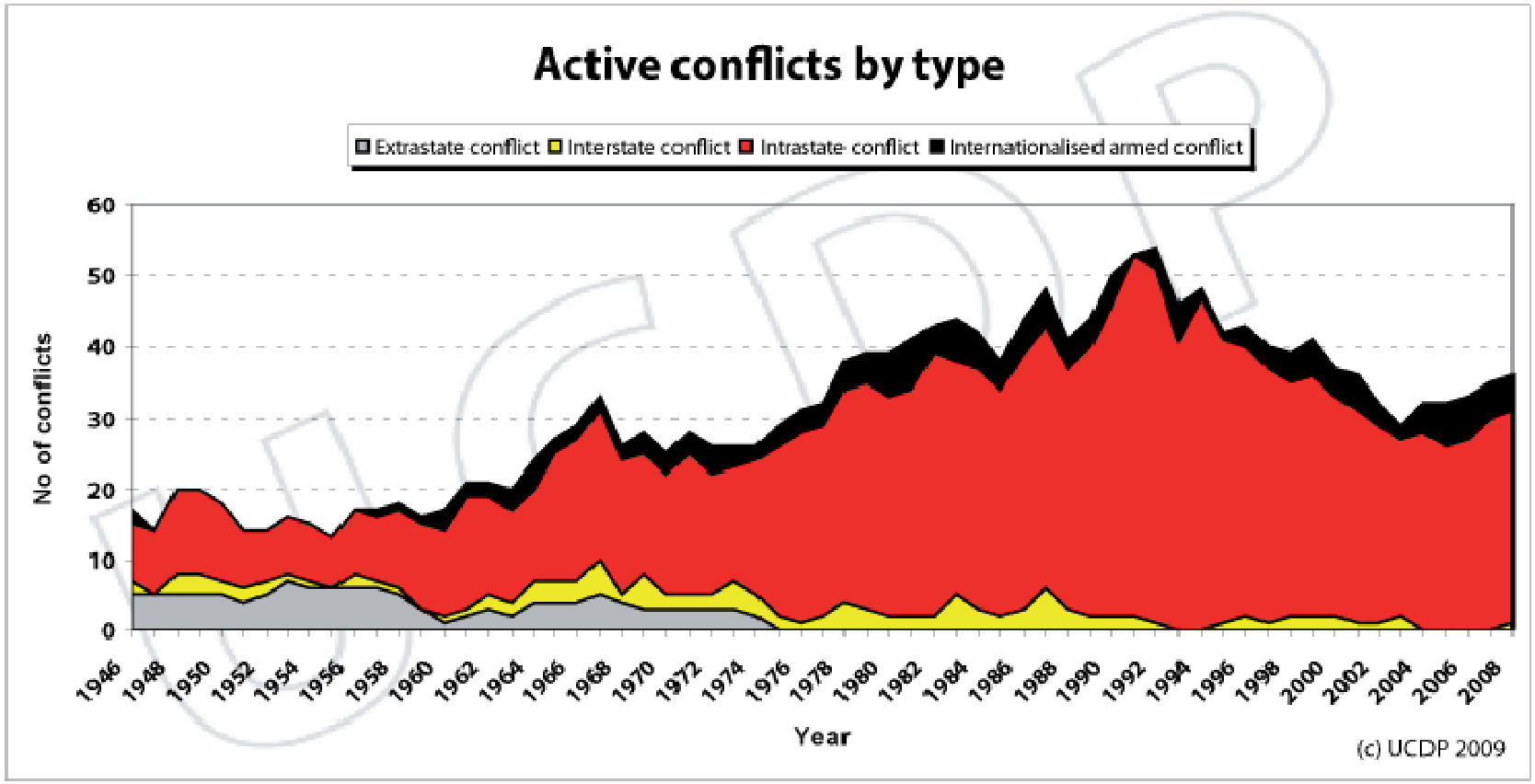
Define the Actors

The Supply Chain problem

SCADA attacks

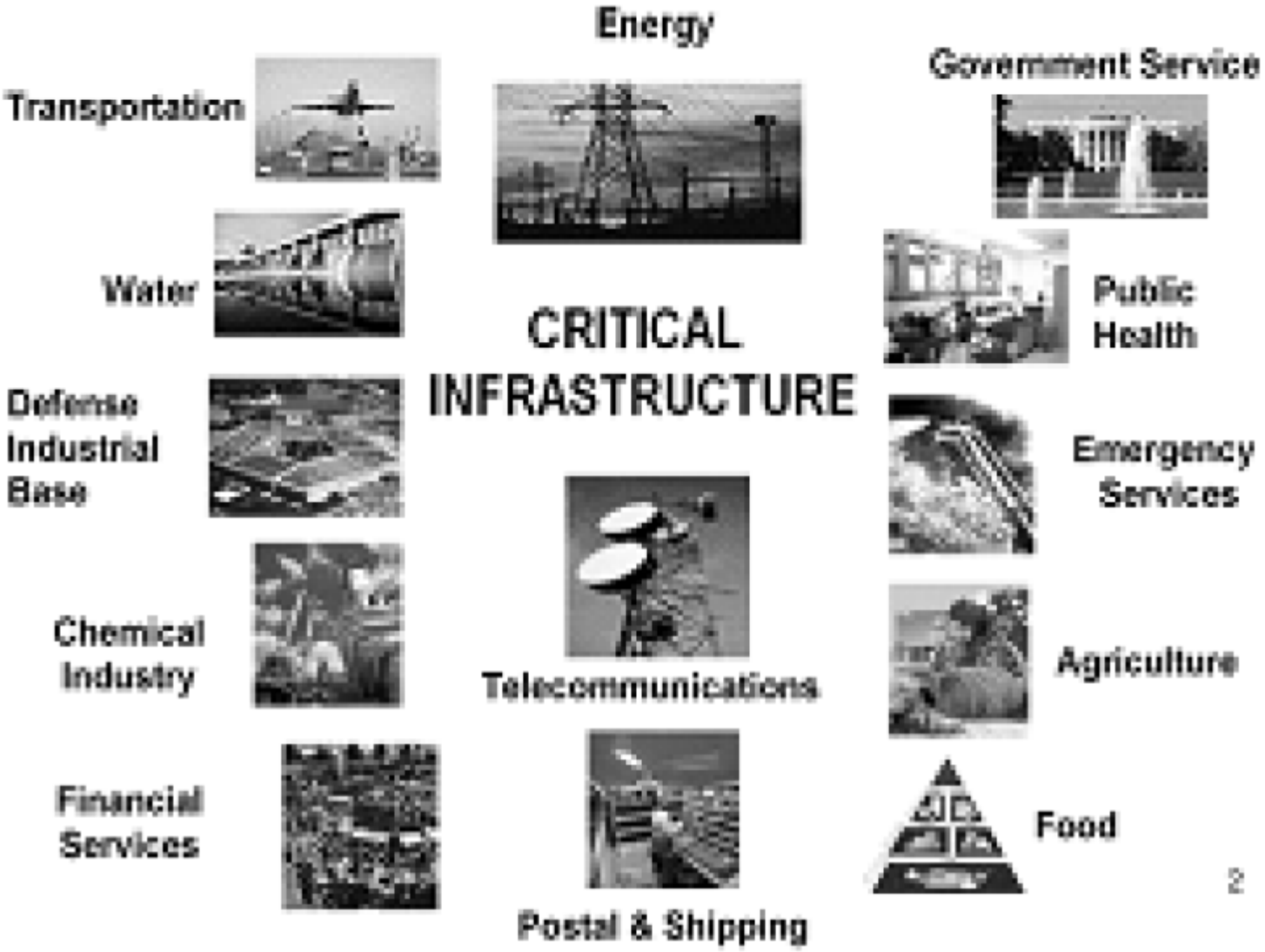
© 2011 Cisco and/or its affiliates. All rights reserved.

# A less violent world?




*Source: Uppsala Conflict Data Programme / International Peace Research Institute, Oslo*

© 2011 Cisco and/or its affiliates. All rights reserved.




© 2011 Cisco and/or its affiliates. All rights reserved.

- UK online economy was worth 100 Billion Pounds in 2010
  - That is larger than the construction, transport and the Gas+Electricity+Water industry
  - 99% of all transactions were on plastic or online.

- For every 1 Pounds' worth imported online, the UK exports 2.80 Pounds worth online
  - offline economy exports 90p for every £1 imported

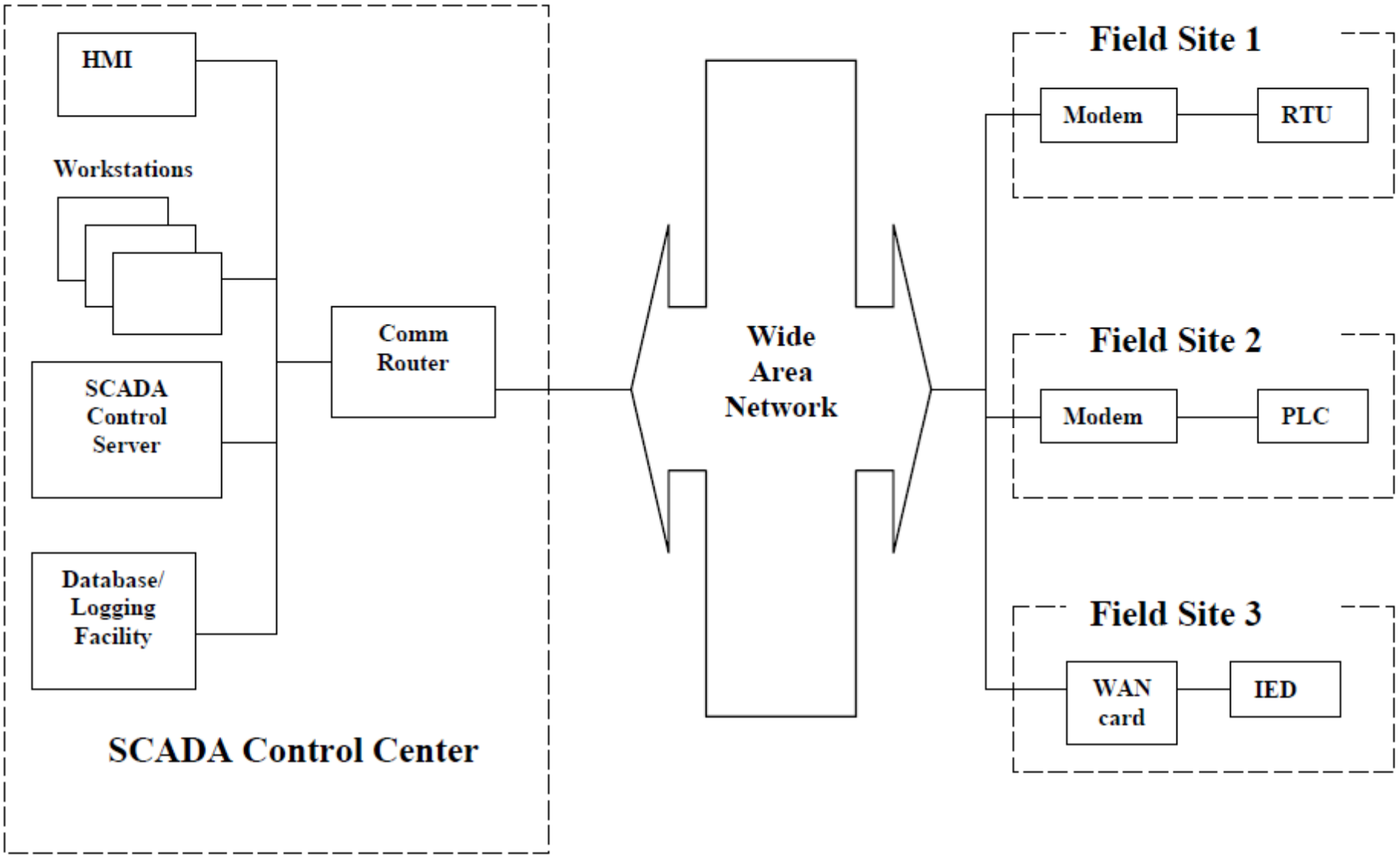
*"Just as in the 19th century we had to secure the seas for our national safety and prosperity, and in the 20th century we had to secure the air, in the 21st century we also have to secure our advantage in cyber space"*

© 2011 Cisco and/or its affiliates. All rights reserved.

Number of hostile players increasing

- Cyber Criminals
- Corporate conflict/rivalry
- Nation states
- Terrorists

© 2011 Cisco and/or its affiliates. All rights reserved.




© 2011 Cisco and/or its affiliates. All rights reserved.

# SCADA attacks : Much Neglected

- In January 2000, a contractor company installs a sewage control system
- A few days later, system misbehaves mysteriously
- A  total 240 tons of raw sewage was spilt  onto a hotel, as school, and a park
- Investigation revealed an ex-employee had sabotaged the control system
- He mounted a total of 46 attacks before being caught

*This is a classic case of an insider SCADA attack.  In the most famous SCADA attack, Iran's nuclear programme was set back by 2 to 5 years by  the Stuxnet virus*

© 2011 Cisco and/or its affiliates. All rights reserved.

# **Advanced Malware:** Stuxnet

**Target:** Iranian Nuclear Reactors

**Impact:** 2-5 Year Delay

**Exploit:** Siemens PLC Software

**Origin:** Unknown

© 2011 Cisco and/or its affiliates. All rights reserved.

# Jun 2010, and the game changed…

- A small company in Belarus discovered a new virus that had infected his client.
- Symantec engineers studied it, and discovered something very strange
  - It was designed to spread not over the internet, but over LANs that were not connected to the internet
  - If would check if the infected machine had a Siemens controller attached to it, if not, it would just ignore the machine

*The Virus would check for a particular number in the windows registry – if the registry number existed it would not harm that machine…..*

© 2011 Cisco and/or its affiliates. All rights reserved.

# Jun 2010, and the game changed…

- If there was Siemens machine, it would check if the controller was programmed to run at 1064 RPM, if not, it would ignore the machine
- If there were less than 164 machines on the LAN, it would ignore all the machines
- If a particular make of frequency converter was not on network, would ignore the machines

*The Virus had an expiry date of 24 Jun 2012 : clearly the designers did not want it lingering forever and damaging machines forever*

© 2011 Cisco and/or its affiliates. All rights reserved.

# Jun 2010, and the game changed…

- If all of the above matched, then the virus would kick into action….
- It would increase the frequency from 1064 to 1410 Hz for 15 minutes, bring it back to normal,
- keep quiet for 27 days,
- Reduce it to 2Hz for 50 minutes, bring to normal.
- Then keep quiet for another 27 days

*It was clearly trying to destroy whatever it was infecting, and it was infecting a very specific target*

© 2011 Cisco and/or its affiliates. All rights reserved.

# Cyber Weapon

- In Jan 2010, Natanz had 8700 Centrifuges
- Annual wastage was 10 percent, around 800 needed replacement per year
- IAEA inspectors noticed that in just last three months, over 2000 centrifuges had been replaced
- Natanz operated centrifuges in groups of 164, frequency of 1064 Hz
- Symantec found 22000 infections in Iran, and only 400 in the US

*A few months later the head of Natanz unexpectedly resigned*

© 2011 Cisco and/or its affiliates. All rights reserved.

# Cyber Weapon

- Stuxnet  is not a virus, it is a cyber weapon
- It is the most sophisticated  malware ever found, and there are parts of it we do not yet understand
- It used up 4 day-zero vulnerabilities (each sell for 500000 USD in the market), two stolen certificates and one hard coded password
- I was clearly not for profit, and created by an agency with vast resources

*This class of threats, called APT, are the ones SCADA networks should worry about the most…..*

© 2011 Cisco and/or its affiliates. All rights reserved.

# SCADA attacks : Much Neglected

- June 1999 : 237,000 gallons of gasoline leaked from pipeline in Bellingham, Washington.
- Gas caught fire, killing 3 and injuring 8, and causing $45 M of damage.
- The SCADA server also had a database application running on it
- The database hogged so much resources that SCADA did not react in time to the leak, causing the tragedy

*This is not an attack, but an illustration that SCADA malfunctions can kill*

© 2011 Cisco and/or its affiliates. All rights reserved.

# SCADA attacks : Much Neglected

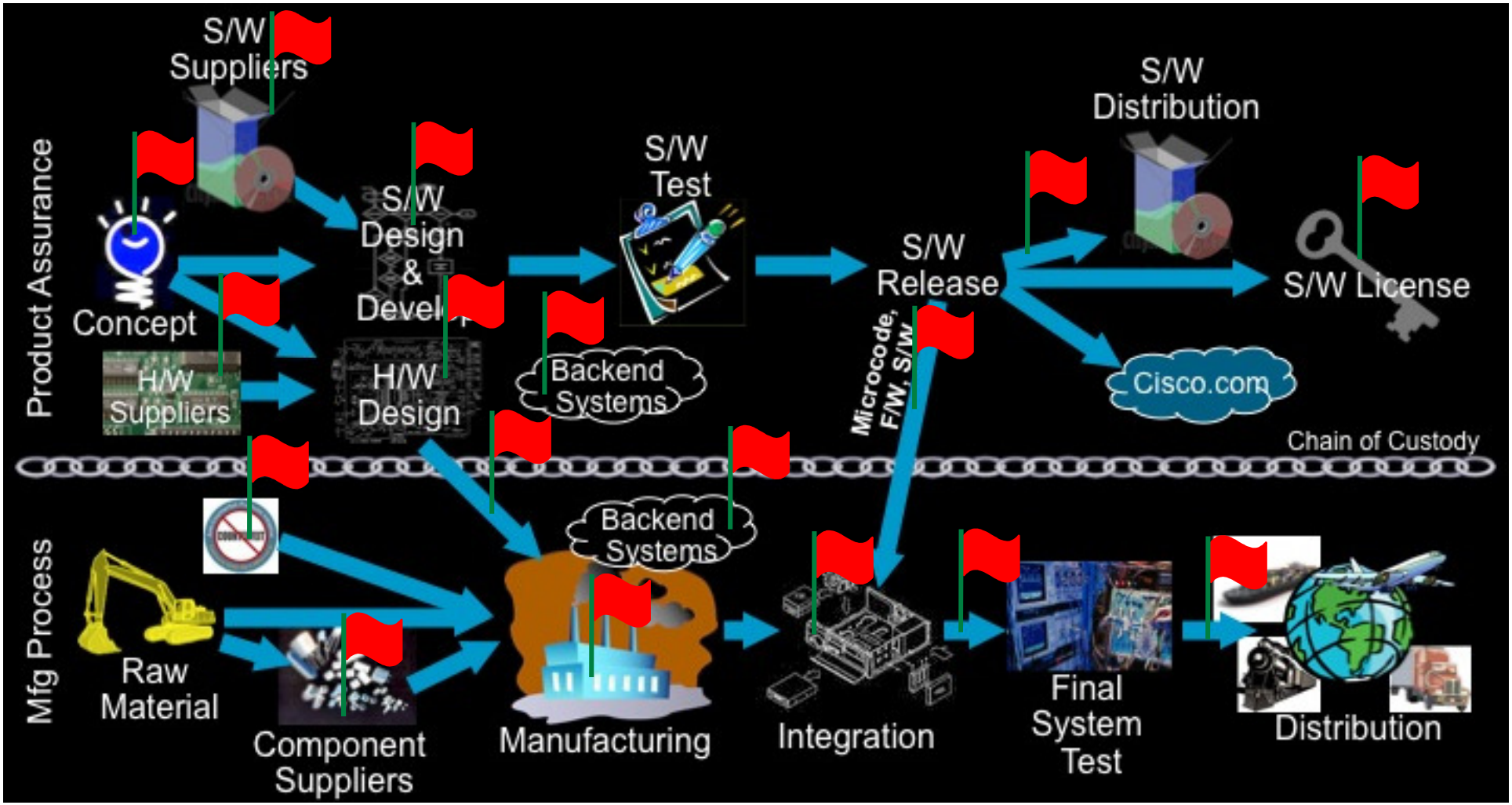
- According to a MacAfee survey, 80 percent of executives surveyed in Mexico reported Cyber extortion using SCADA attacks
- ***The same survey reported that 60 percent of Indian companies reported cyber extortion attempts***

*"Hundreds of millions of dollars have been extorted [from various companies], and maybe more […] This [cyber ] kind of extortion is the biggest untold story of the cybercrime industry."*

- Allan Paller, Director of the SANS Institute

© 2011 Cisco and/or its affiliates. All rights reserved.

# Securing the Supply Chain




© 2011 Cisco and/or its affiliates. All rights reserved.

# Threats…..

- July 2009 13,073 fake Processors supplied to the US navy
- brand names of Intel, AMD, Fujistsu, Amtel, Altera and NCC, all reputed brands
- They were procured for unknown sources in China
- Some were ‘black topped’ and re-branded as Military Grade, sold for much higher sums

- FBI arrested three members of a family.

*Arab telecom provider Etisalat pushed to BlackBerry users what it said was a software update for improving performance. In fact, it was spyware capable of providing access to information on the devices.*

© 2011 Cisco and/or its affiliates. All rights reserved.

# Supply Chain Pitfalls

- BAE wanted some chips made by Philips Semiconductor for a modern weapon systems for the US military
- Port Electronic, supplied these chips, which were fakes.
- Philips had stopped manufacturing them in 1997.

*BAE wanted to use these old chips to avoid a redesign that would cost millions….*

© 2011 Cisco and/or its affiliates. All rights reserved.

# Threats…..

- Port Electronics had sourced them from Aapex International.
- Aapex international had purchased them from HKF International in Shenzhen, China
- The source remains unknown to this day.

*When asked if She knew they were fake, the GM of HK Fair International said "we are traders…we buy chips from one hand and sell them from the other"*

© 2011 Cisco and/or its affiliates. All rights reserved.

# The Supply Chain

*"If the supply chain can be conceived as an orchestra, then imagine 104 musicians; with no conductor; very little sheet music; and music not shared among musicians. Under such conditions, how can you play a symphony?"*

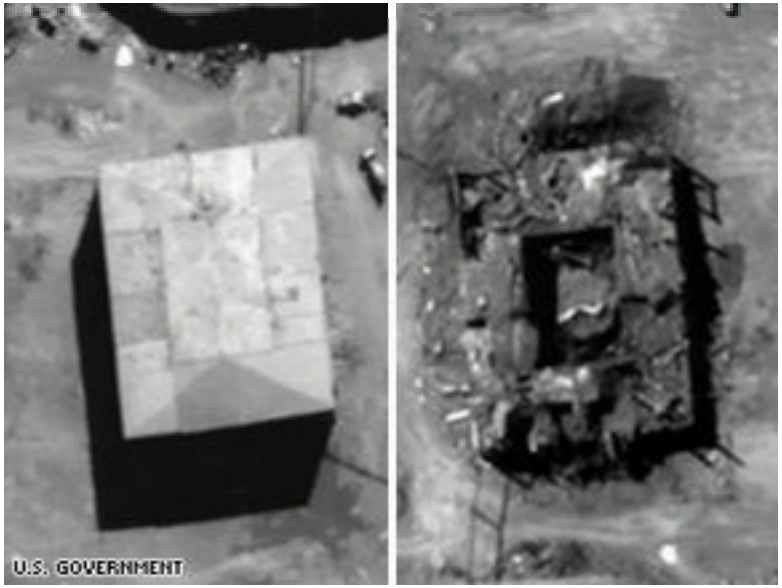
*Only 4 firms, Dell, Wal-Mart , Cisco and HP are approaching stage 4 supply chain maturity, but that is far below the critical mass needed for orchestrating and synchronizing  a global outsourced supply chain….*

http://www.saic.com/news/resources/Cyber_Supply_Chain.pdf

© 2011 Cisco and/or its affiliates. All rights reserved.

# Operation Orchard 2007

- Israeli air strike against Syrian nuclear reactor.
- Assisted by cyber attack on Syrian air defense.




© 2011 Cisco and/or its affiliates. All rights reserved.

# The Lloyd Omega Case

- Omega Corporation, leader is precision instrumentation and measurement devices
- Computerized their design and manufacture, sales took off and they beat competition hollow
- 25,000 different products, customizable to 500,000 distinct designs
- Software and databases controlled the entire process

© 2011 Cisco and/or its affiliates. All rights reserved.

# The Lloyd Omega Case

- Tim Lloyd was a star employee, who got sidetracked as the organization grew.
- At some point he was fired for misbehavior.
- Few days later a logic bomb destroyed every bit of the software used to run the company.
- Omega never recovered their prime position.

© 2011 Cisco and/or its affiliates. All rights reserved.

# Lloyd Omega Modeling : Anomaly Detection

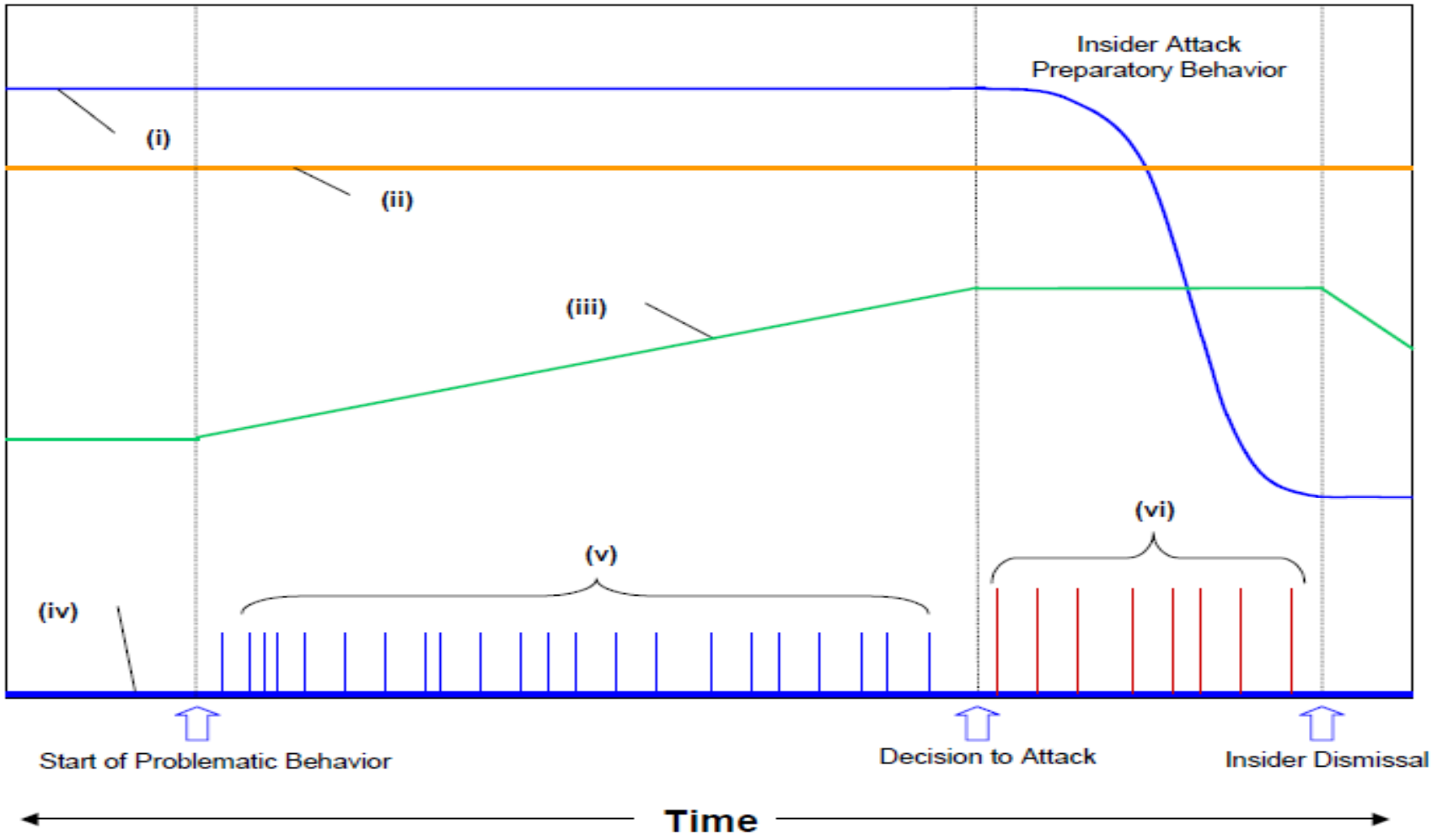



**Figure 3** (i) Security Level; (ii) Pressure to Grow; (iii) Workplace Discontent; (iv) Formal Controls; (v) Disruptions of Workplace Climate and Precursor Incidents; (vi) Actions to Reduce Security Level.

© 2011 Cisco and/or its affiliates. All rights reserved.

RISK = Likelihood x **Vulnerability** x Impact

Certain to be attacked

Catastrophic!!

© 2011 Cisco and/or its affiliates. All rights reserved.

Thank you.