Industrial Cyber Security Overview

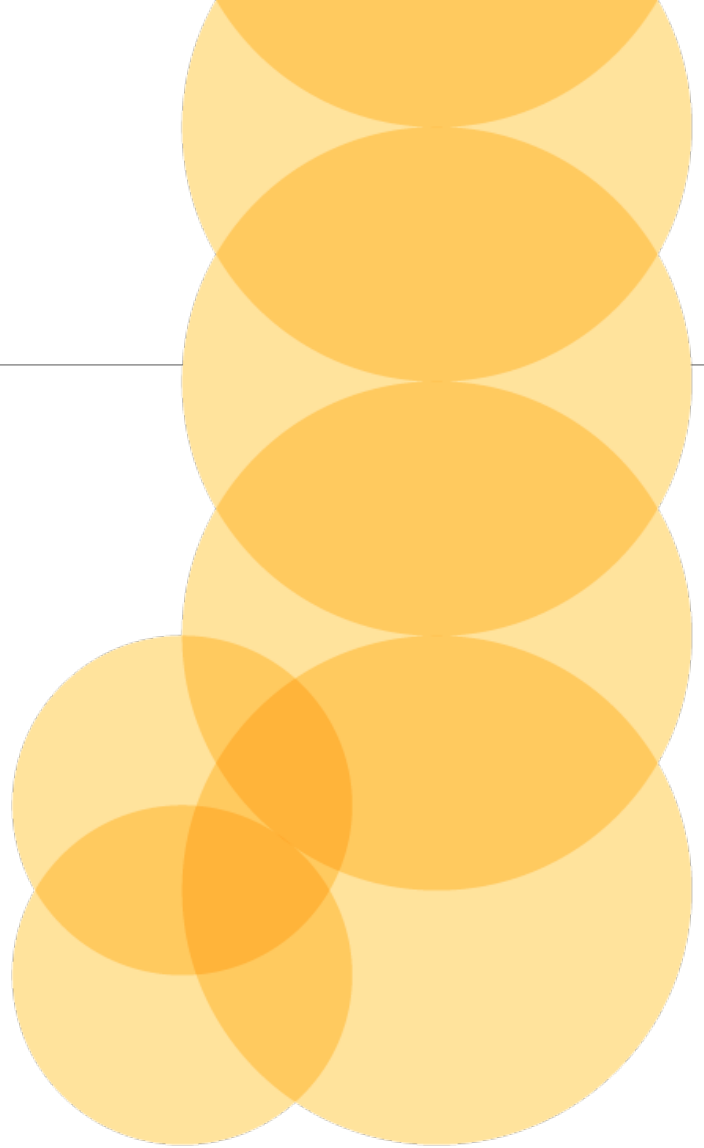
RON CLEMENT, GICSP, CISSP

CYBER SECURITY INSTRUCTOR

Industrial Cyber Security Overview

Agenda

1. Industrial Cyber Security Landscape
2. Recent Incidents



Industrial Cyber Security Landscape

Industrial control systems are more interconnected

…and hack-able, as air gaps no longer exist.

Systems are easy to target

Find them with tools like Shodan, the Google of hackers

SHINE (SHodan INtelligence Extraction)


SECURITY WEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS
Subscribe (Free) | Security White F
Malware & Threats Cybercrime Mobile & Wireless Risk & Compliance Security Architecture Man
Risk Management Security Architecture Disaster Recovery Incident Management Training & Certi
Home › Risk Management
Project SHINE Reveals Magnitude of Internet-connected Critical Control Systems
By Fahmida Y. Rashid on October 06, 2014

- Researchers identified 182 manufacturers who were considered traditional SCADA and control system manufacturers, and built relevant search queries based on those names to find devices exposed directly to the Internet
- Roughly 2.2 MILLION devices were identified as being exposed either directly or indirectly related to SCADA or control systems

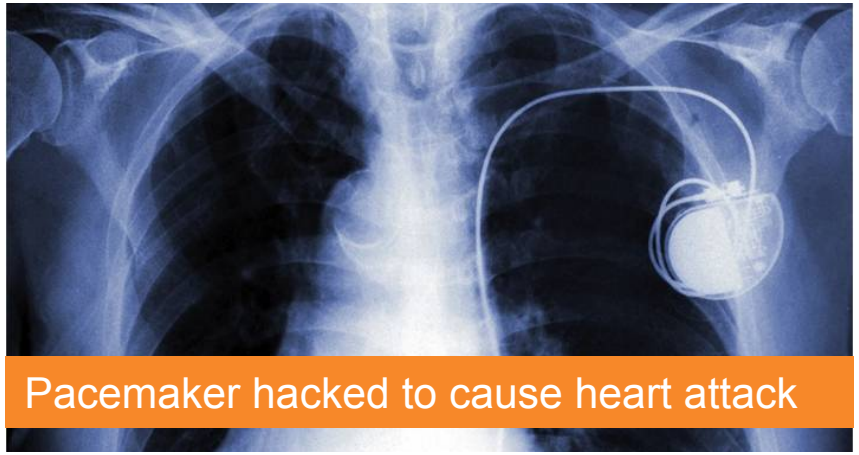
Why Cyber Security Matters…

…Because Successful Attacks Can Be Catastrophic

Pipeline explosion caused by remote attack

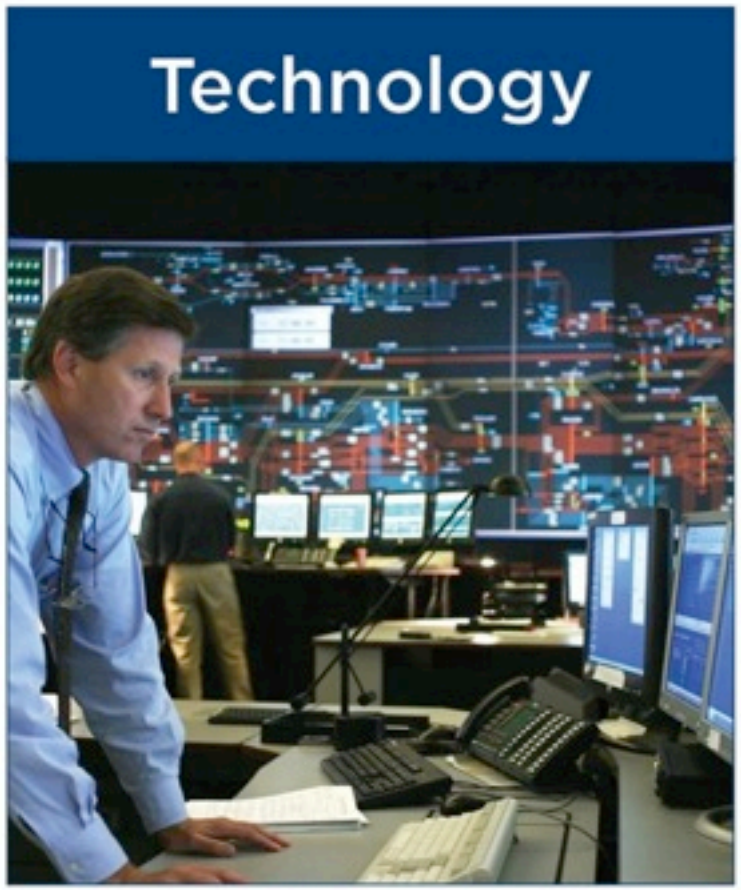
Wastewater plant spilled sewage into rivers

Prius crash triggered via mobile phone



Pacemaker hacked to cause heart attack

Weaknesses Prevalent Everywhere



79,790 security incidents across 61 countries in 2014 (Verizon DBIR 2015)

67% of critical infrastructure companies suffered an attack in the last year (Ponemon 2014)

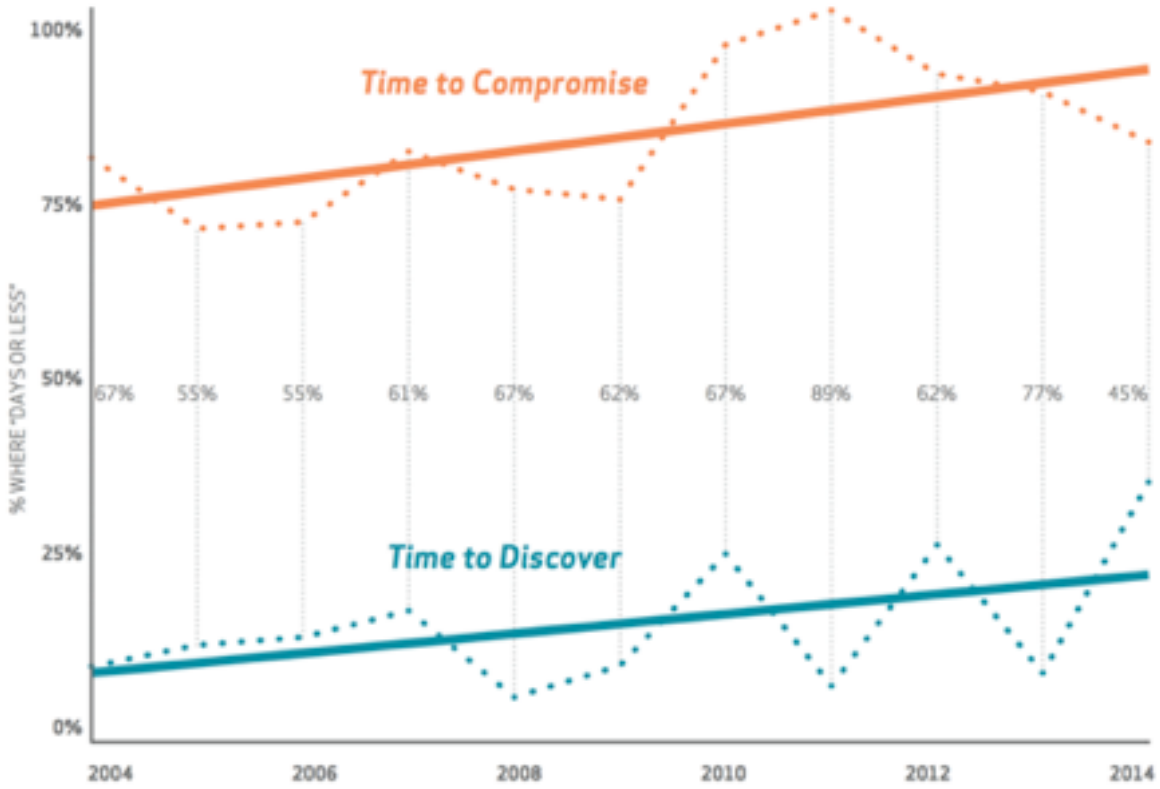
78% of senior security officials expect a successful attack on their ICS/SCADA systems within 24 months (Ponemon 2014)

$7.82 billion total market size for ICS cyber security solutions in 2014 (Markets and Markets 2015)

Incident – Time to Compromise / Time to Discovery

The Verizon DBIR illustrated that 97% of breaches analyzed could have been prevented by simple or intermediate controls.

Malware is undetected for months or years.

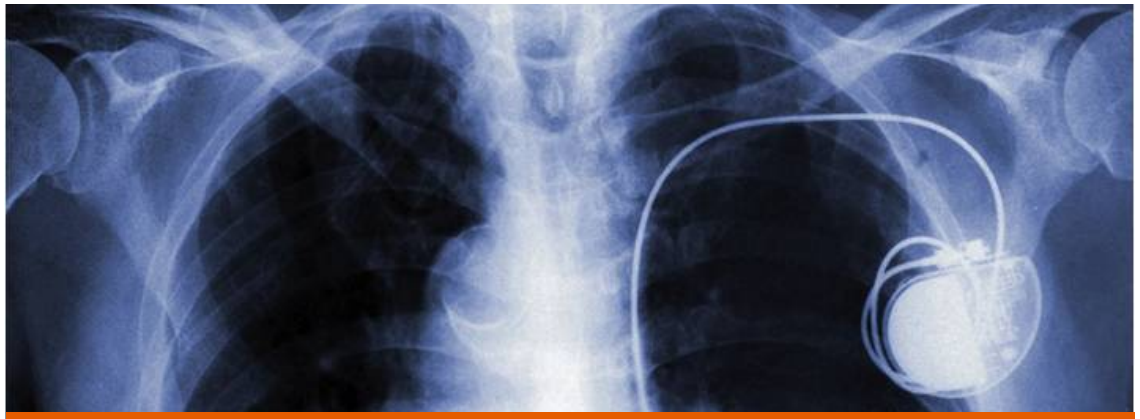


Why Security Matters

Pipeline explosion caused by remote attack

Wastewater plant spilled sewage into rivers

Prius crash triggered via mobile phone



Pacemaker hacked to cause heart attack

Industrial Threat Landscape

Targeted attacks are executed by professional, organized teams

- Sophisticated tools
- Well-funded, especially when sponsored by nation-states

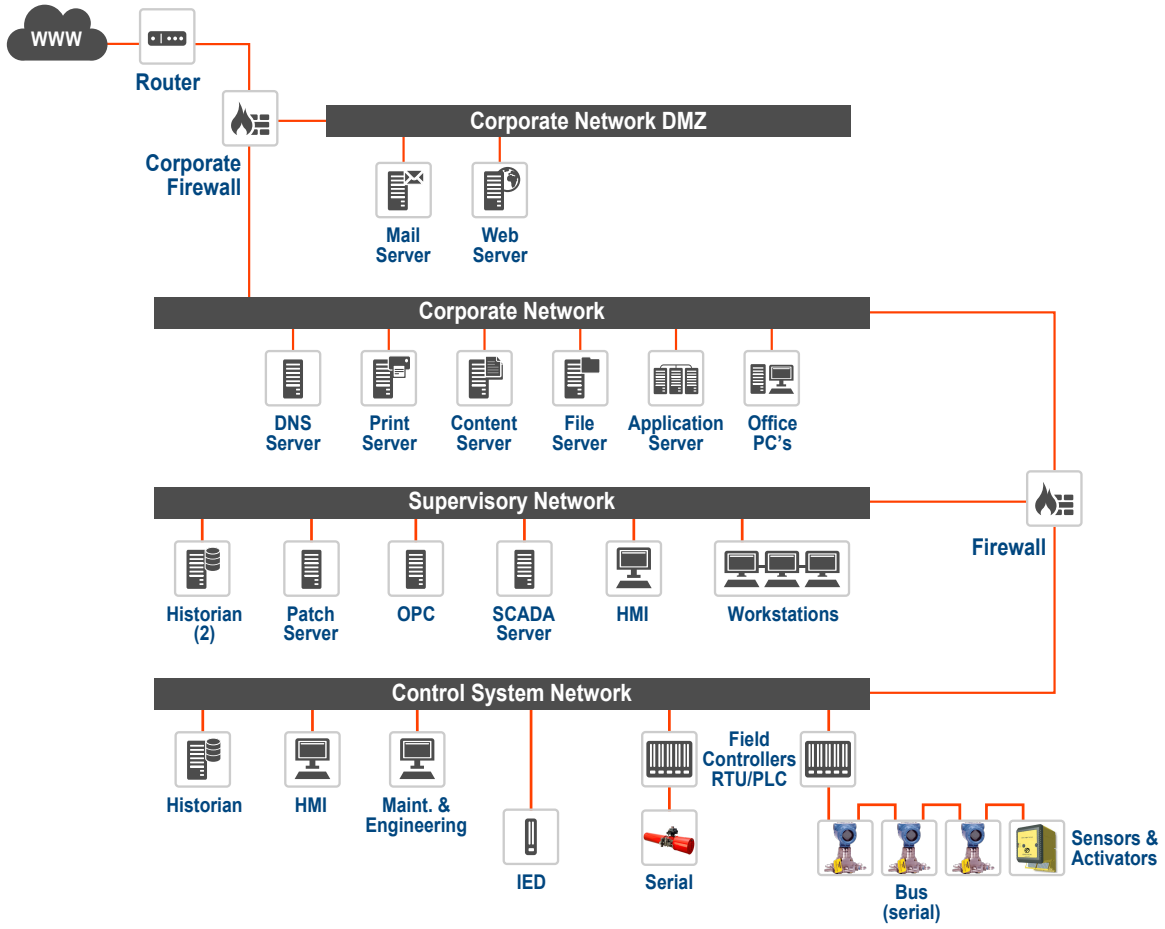
Threat actors evolve and use more advanced methods and tactics

- Cyber crime
- Hacktivism
- Insider attack
- Distributed attack
- Network Attack
- Physical damage

Attacker Goal Against Industrial Control Systems

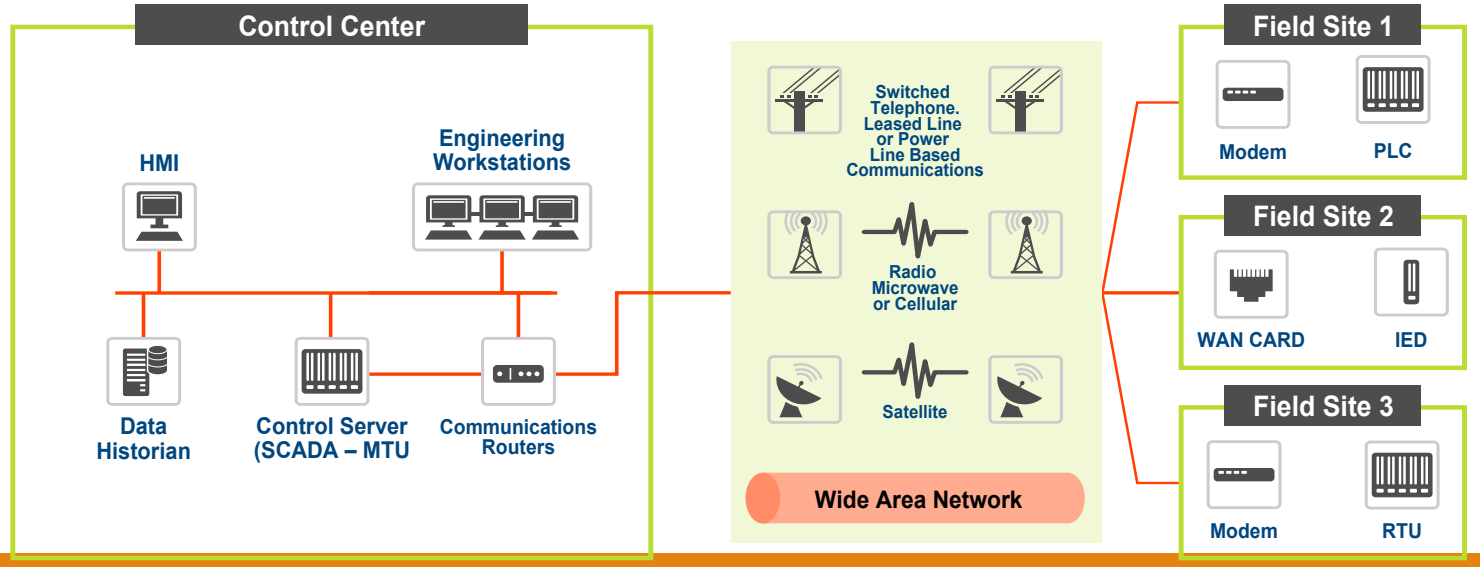
Gain access to the control system:

- Gain physical or remote access to an ICS host
- Compromise a machine with access to the ICS network
- Leverage a corporate system to attack the control system network
- Damage Physical assets remotely



Gaining Physical Access Examples

- Attackers with physical access can wreak significant damage
- Attackers use pre-existing malware and adapt
  - Metasploit
  - Tools from underground forums
- Attackers focus on areas of weaker physical security
  - Radio links by Software Defined Radio hacks
  - Fiber connections via fiber tapping
  - Systems with weak or no passwords



IT vs. OT Security Priorities

IT

- **Confidentiality** – data and assets can only be read by authorized users
- **Integrity** – data and assets can only be modified or deleted by authorized users in authorized ways
- **Availability** – data and assets are accessible to authorized users in a timely manner

OT

- **Availability** – automation and production systems must maximize uptime
- **Integrity** – controller commands must be issued only by authorized users in authorized ways
- **Confidentiality** – assets and data can only be read by authorized users

IT emphasizes data.

For OT, safety of people and industrial controls are most important

OT & IT Security Differences

Security Priorities – AIC (IAC) vs. CIA

Threat Types – Physical vs. data

Staffing – Differing expertise needed

Vulnerability Lifecycle – Longer for OT

Protocols – Need OT visibility

Segmentation – No more “air gap”

Solution Availability – Need ease of use

Recent Incidents

Stuxnet 2010

Discovered in July 2010

Targeted Iran's nuclear enrichment program

Attacked Siemens PCS7, S7 PLC and WIN-CC systems

Infected 100,000 computers and at least 22 manufacturing sites

Destroyed up to 1000 centrifuges between November 2009 and January 2010

Stuxnet 2010 (cont'd)

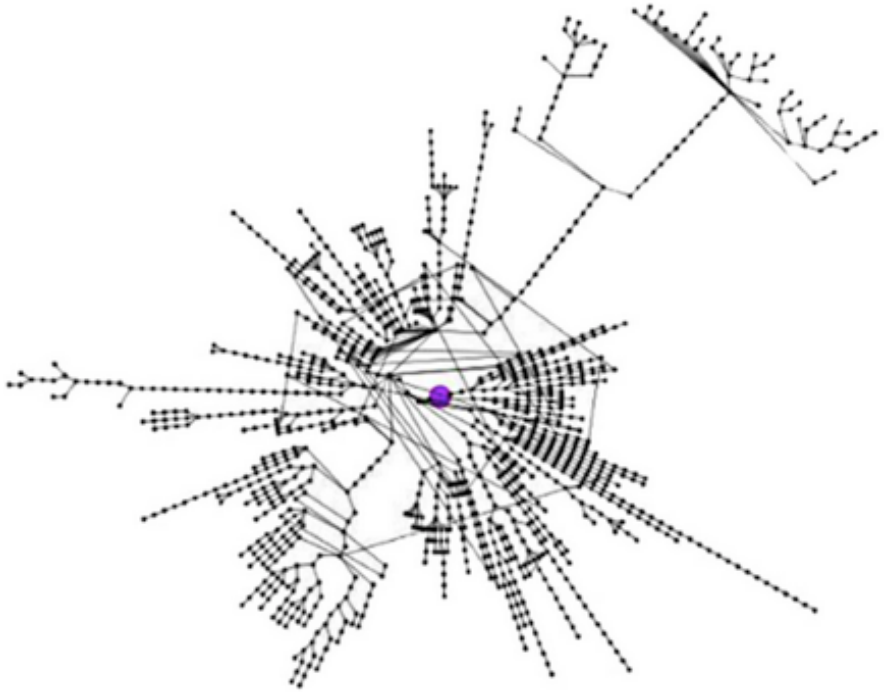
Initially spread using infected removable drives

Exploited the architecture of the controller by hijacking the vendor's DLL driver

Modified ladder logic sent to/received from the controller without the notice of the development application or the controller

No signed code was in use

No code execution or configuration tamper control was developed



Source: Symantec

DUQU and FLAME (2011 and 2012)

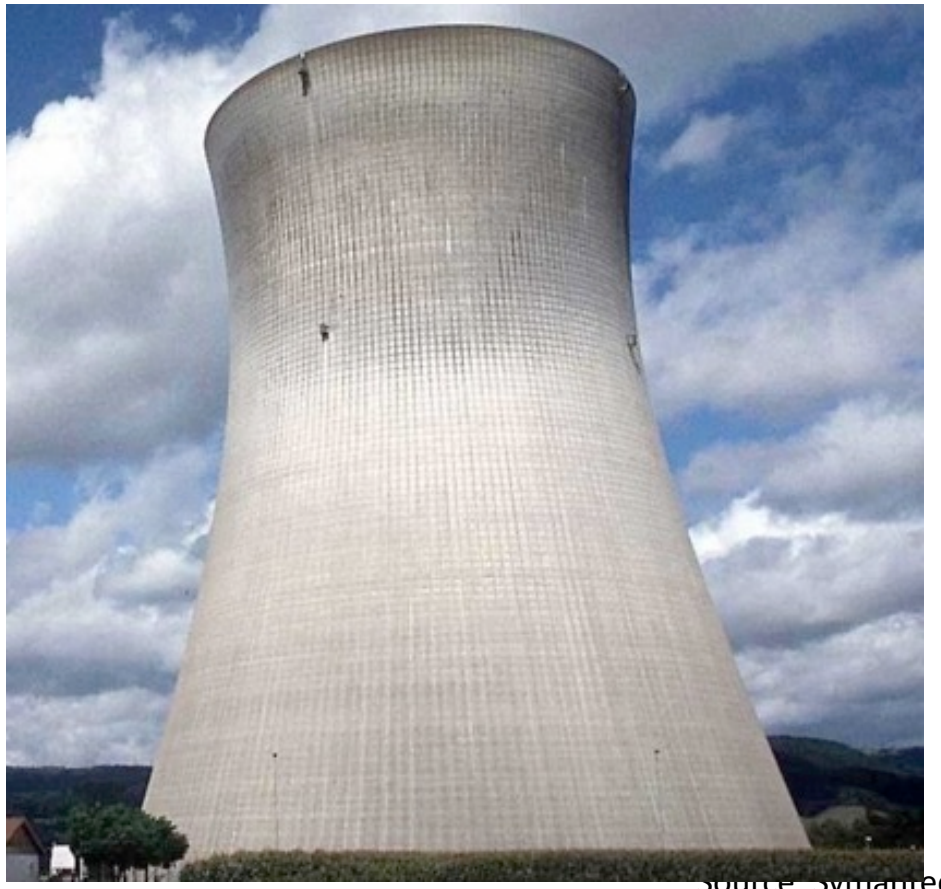
The Sons of Stuxnet

Duqu

- Malware had large similarities with Stuxnet
- Trojan horse aimed to capture and **exfiltrate** information via a jpeg file

Flame

- **Spyware** discovered in Iran oil and nuclear installations
- Was **more complex** than Stuxnet
- Could record audio, screenshots, keyboard activity and network traffic



Source: Symantec

Shamoon (2012)

Targeted Saudi Aramco (Oil and Gas Company)

Was the most destructive attack on the business sector seen to date

Infected more than 75% of the company's workstations (30,000 to 55,000 workstations)

Replaced crucial system files with an image of a burning U.S. flag

Impacted messaging services severely for several weeks

US Power Plant Hit by USB-based Malware (2013)

An infected USB stick used for software updates and to back up control system configurations

A virus in a turbine control system that impacted about 10 computers on its control system network, and affected operations for about three weeks

Dragonfly (2013, 2014)

- AKA Energetic Bear in operation since 2011
- Initially targeted defense and aviation companies in the US and Canada followed by European energy firms
- Targeted companies related to industrial control systems
- Managed to compromise a number of strategically important organizations for spying purposes
- Damaged and disrupted target companies
- Used spam email campaigns and watering hole attacks to infect targeted organizations

Havex (2014)

Attackers add Trojan to ICS software on vendor's site

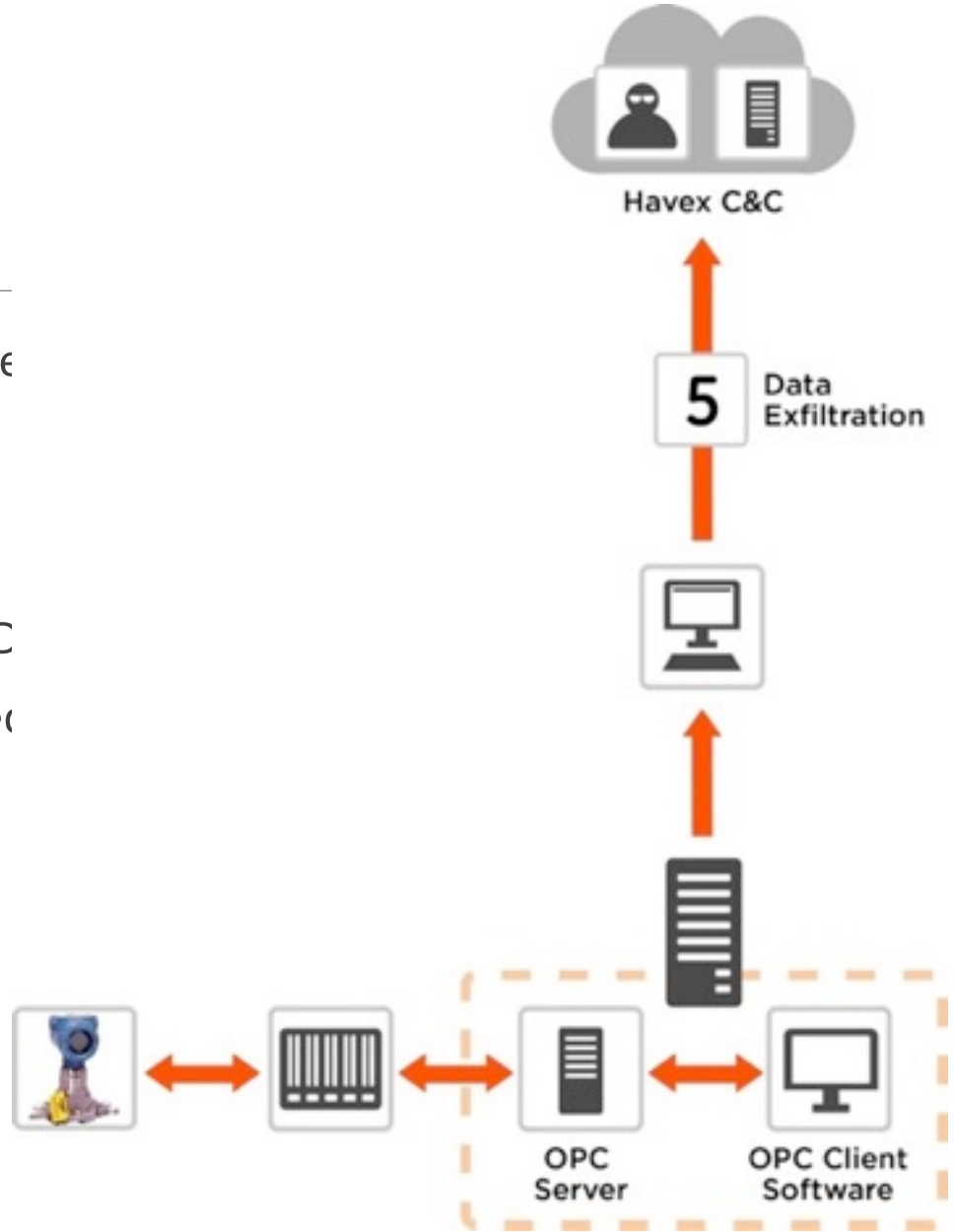
ICS customer downloads software to their PC

Customer connects PC to ICS

Active scan of OPC servers used for controlling SCAD

Also scan for other connected computers and shared

Data Exfiltration starts



US Utility’s Control System Hacked (2014)

A sophisticated hacking group attacked a U.S. public utility’s control system network

Hackers may have launched the latest attack through an Internet portal that enabled workers to access the utility's control systems.

Hackers used brute-forcing to break the simple password mechanism

BlackEnergy (2014)

'Trojan Horse' bug lurking in vital US computers since 2011

A coal-fired power plant in Wyoming is seen on March 14, 2014 and the Trans-Alaska oil pipeline, pictured on June 14, 2009.

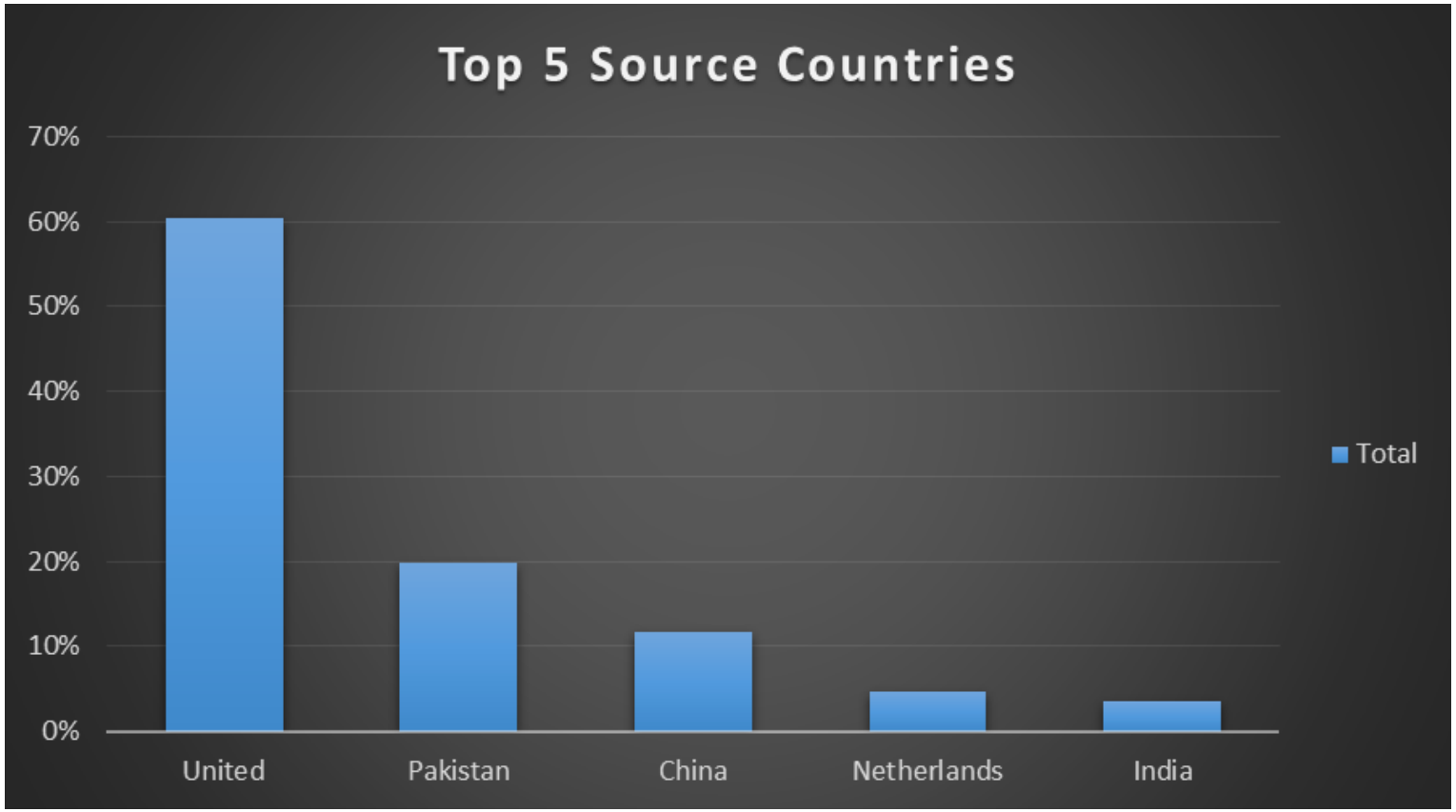
German Steel Mill Attack (2014)

Attackers remotely manipulated the industrial control system

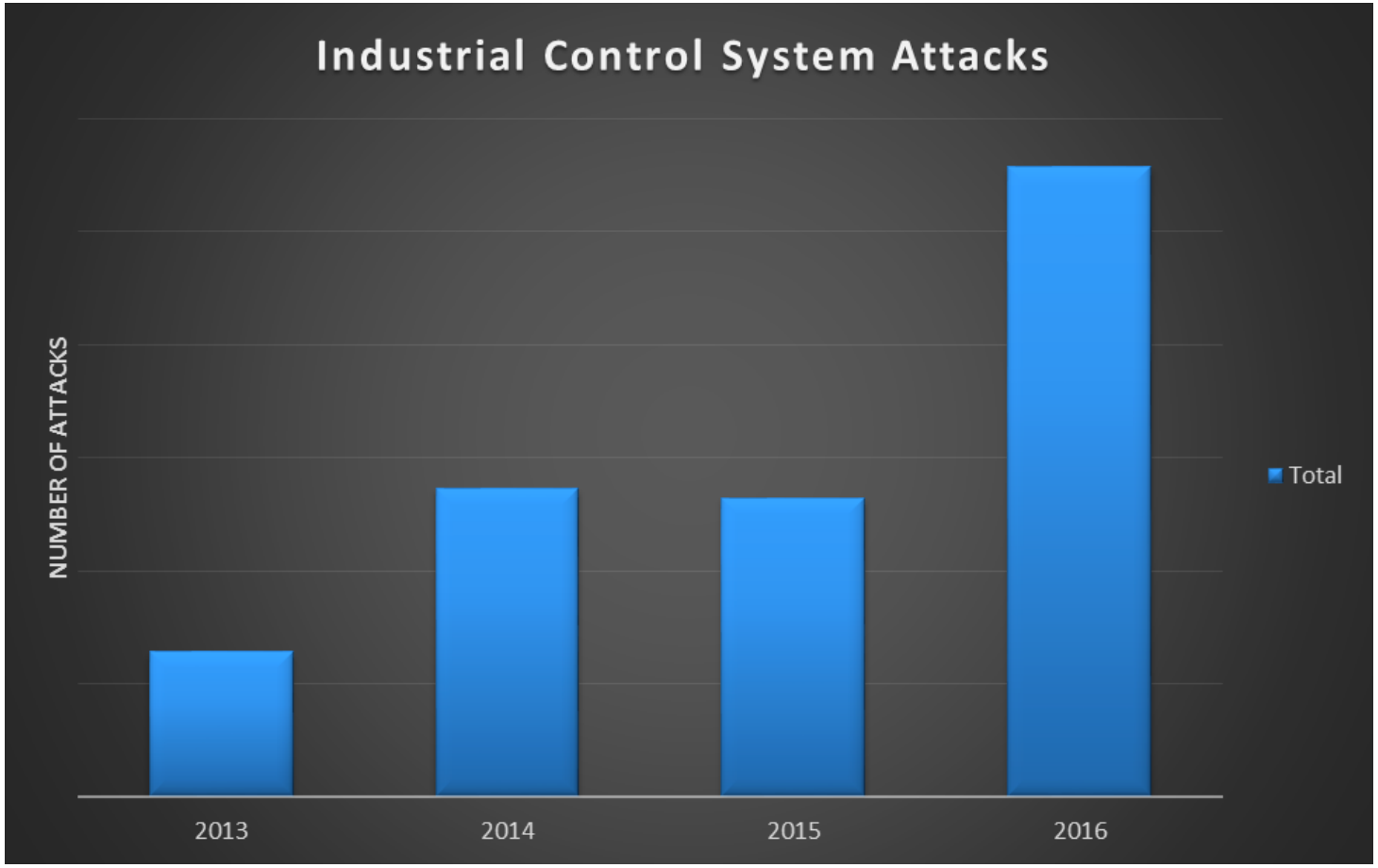
- Used spear-phishing to infiltrate the company network
- Successfully transitioned to industrial network and control systems
- Disrupted the blast furnace to not shut down properly
- Resulted in “massive” physical damage

Second occurrence of a fully digital attack leading to physical damage

U.S.-based actors accounted for the majority of ICS attacks in 2016. This was not surprising, since the U.S. has the largest presence of internet-connected ICS systems in the world



The spike in ICS traffic was related to SCADA brute-force attacks, which use automation to guess default or weak passwords. Once broken, attackers can remotely monitor or control connected SCADA devices



More Notable Recent ICS Attacks

- ***ICS Malware Targets European Energy Company***
  - The backdoor delivered a payload that was “used to extract data from or potentially shut down the energy grid”
- ***New York Dam Attack***
  - The attackers compromised the dam’s command-and-control (C&C) system in 2013 using a cellular modem
- ***Ukrainian Power Outage***
  - BlackEnergy malware to exploit the macros in Microsoft Excel documents. The bug was planted into the company’s network using spear phishing emails

The threat to ICS permeates across a nation’s entire economy and infrastructure

Summary

- The air gap no longer exists
- Industrial security is evolving as more devices and systems are interconnected
- Attacks are more frequent and sophisticated
- Attacks are increasing by skilled professionals, many times with assistance or by insiders
- Proprietary does not mean invincible or invisible
- The costs from a breach extend beyond direct financial losses
- Include security in your budget now: assessments, technology, training, and controls