Industrial Communications & Controls

ANIXTER®

IC²

ANIXTER

Anixter

Industrial Communications & Control

Industrial Cyber Security

Anixter with Belden Industrial Networking

HIRSCHMANN
A BELDEN BRAND

TOFINO SECURITY
A BELDEN BRAND

GarrettCom™
Industrial Networking at Its Best™

- ✓Hardened Ethernet Switches
- ✓Media converters
- ✓Routers
- ✓Firewalls
- ✓Terminal Servers
- ✓Wireless 802.11

Agenda

- What is Cyber Security? Why is it Important?
- We Have a Firewall – Aren't We Secure?
- Introduction to Belden's Eagle and Eagle Tofino
- The Security Lifecycle: Managing Risk

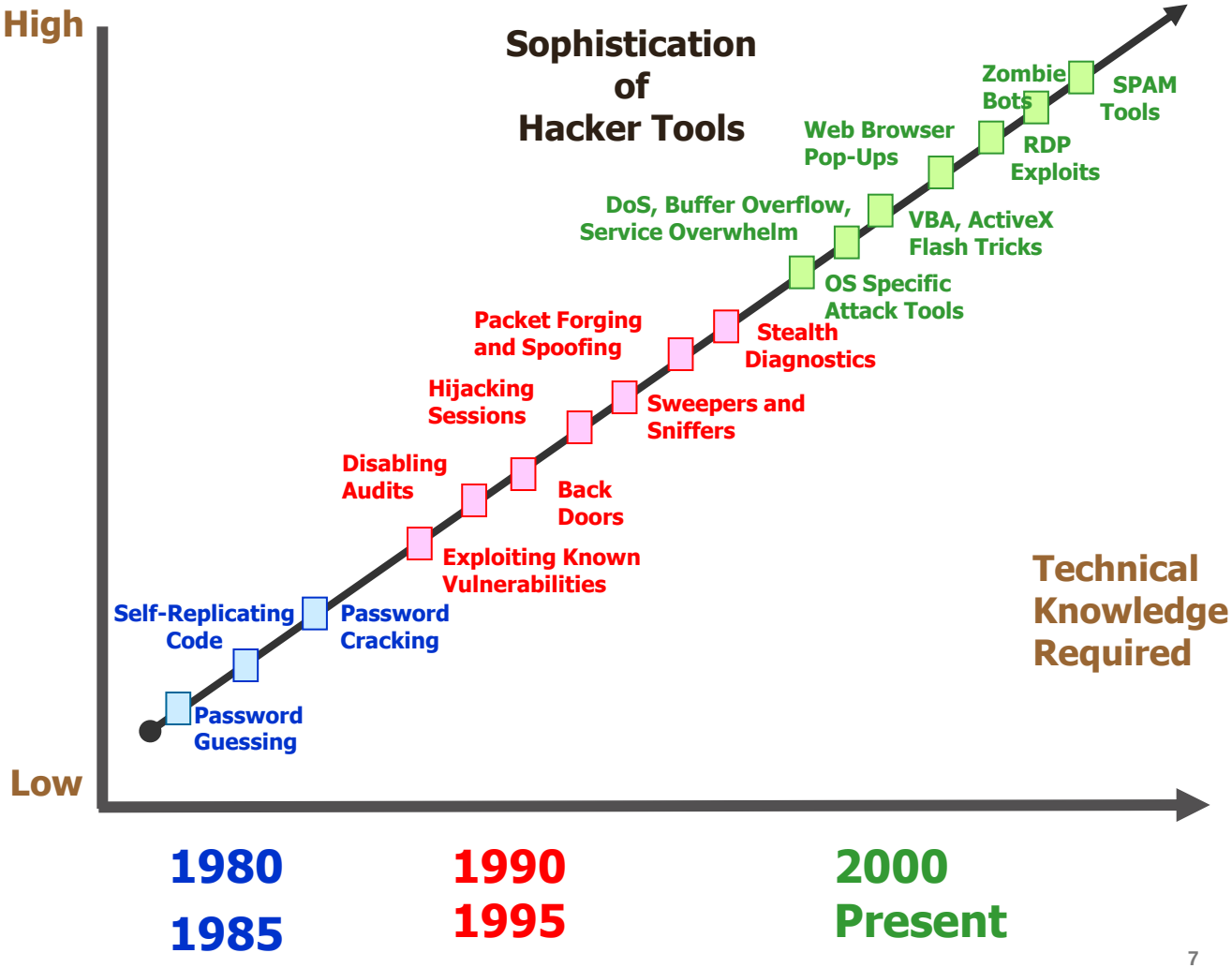
Cyber Security

What Is It? Why Is It Important?

Securing SCADA Networks

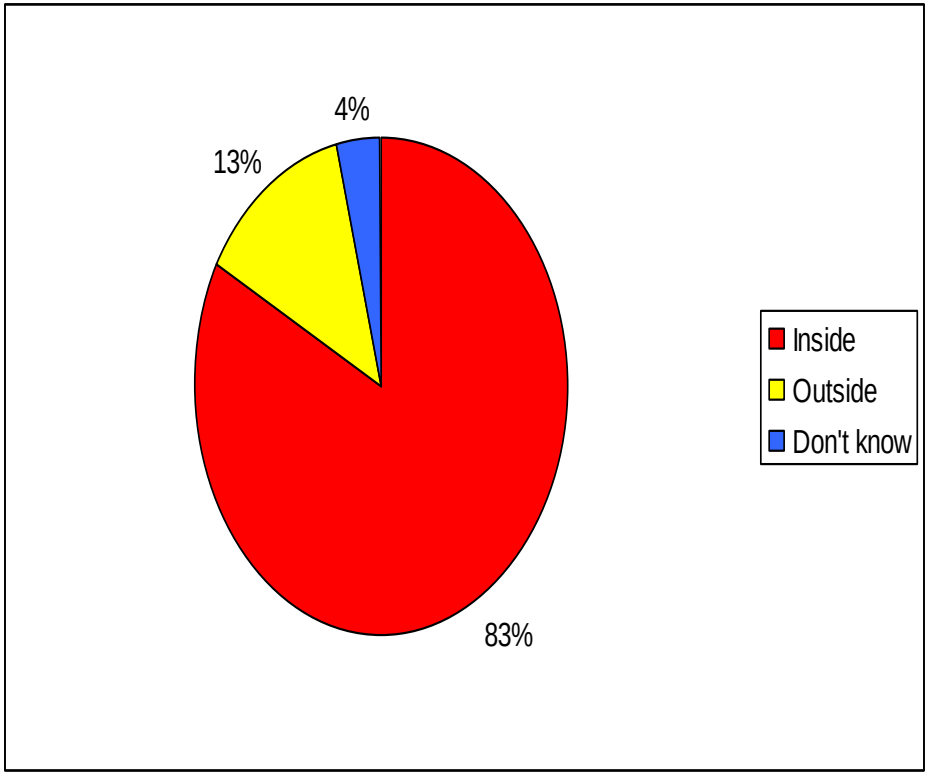
- Define a security policy
- Secure the SCADA network and operating environment
- Secure the SCADA application
- Detection of unauthorized intrusions
- Regulate and monitor physical access to the SCADA network

The trend of the hacker…



Did you know?

What percentage of network security attacks do you believe originate from inside or outside of your company?



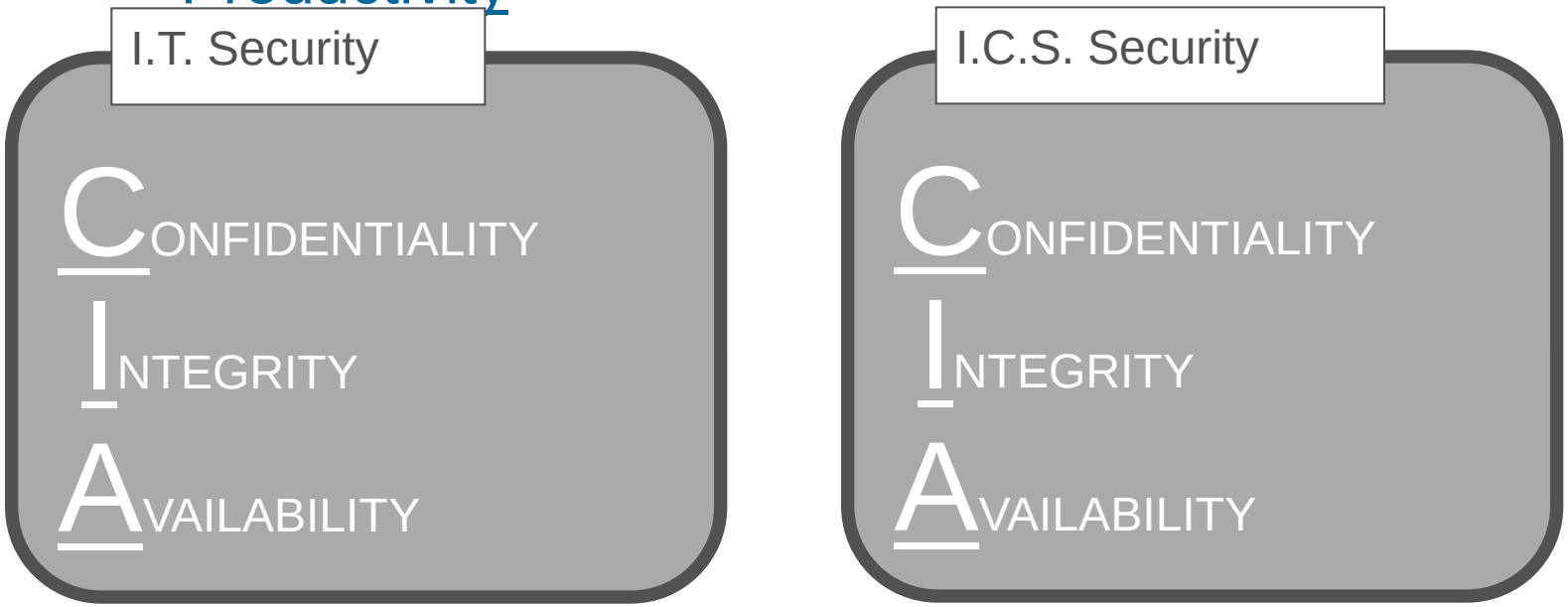
Source:AT&T/Economist Intelligence Unit Networking and Business Strategy Survey, March-April 2004

It is indeed, real……

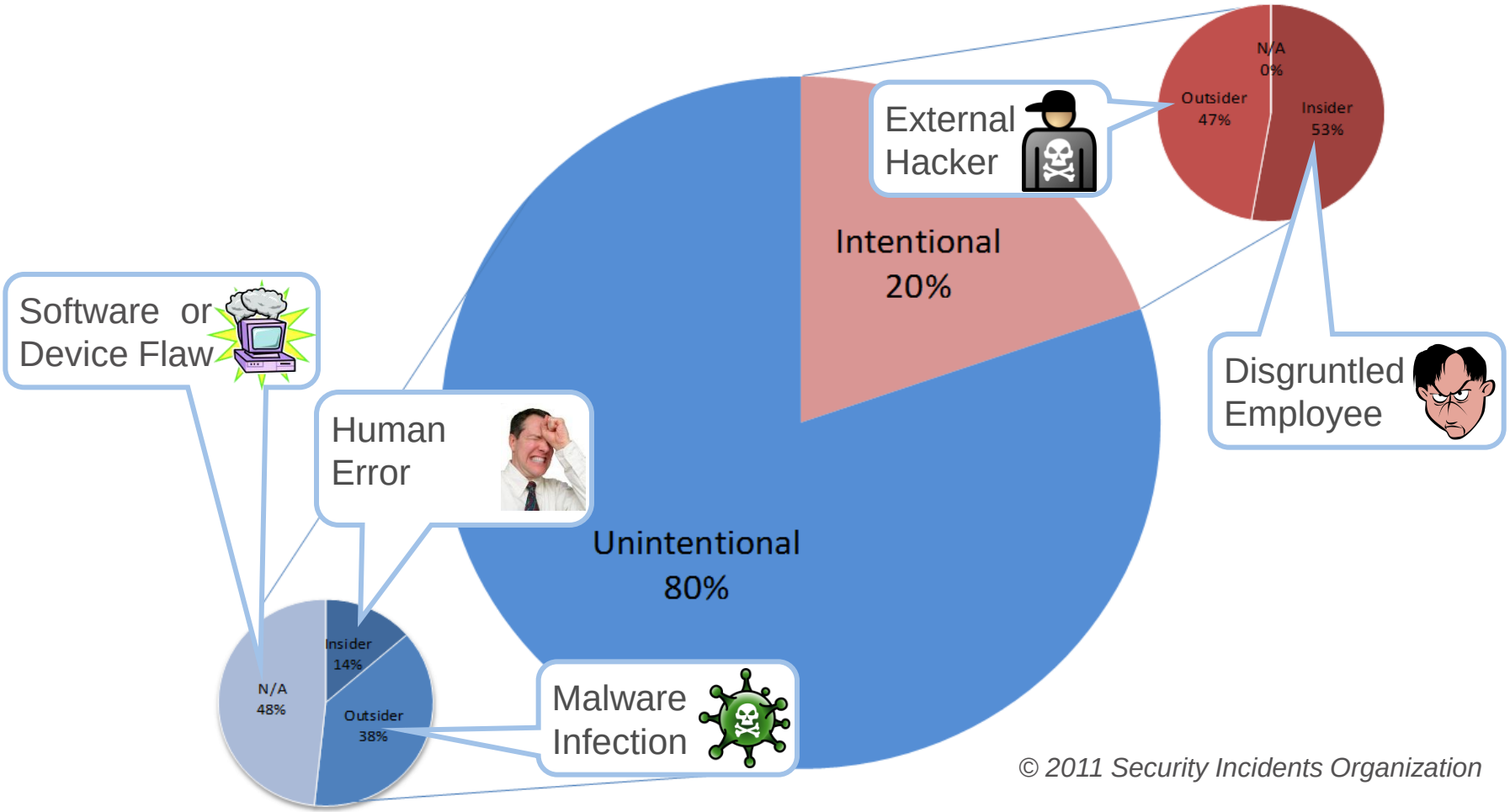
Industrial monitoring and control systems are directly connected to station equipment. A cyber terrorist attacking the control system layer can cause complete service interruptions, loss of generating capacity, environmental damage and unsafe working conditions.

What Is Cyber Security?

- I.T.: Protect Critical Business Information
- SCADA/ICS: Protect Critical Plant Safety and Productivity



Cyber Security Incident Types



It's Not About Hackers & Terrorists

- Oil pipeline shut down for 6 hours after software is accidently uploaded to a PLC on the plant network instead of test network

NET IMPACT: $250K

- 13 auto assembly plants are shut down by a simple Internet worm; 50,000 workers stop work for 1 hour while malware removed

NET IMPACT: $14M

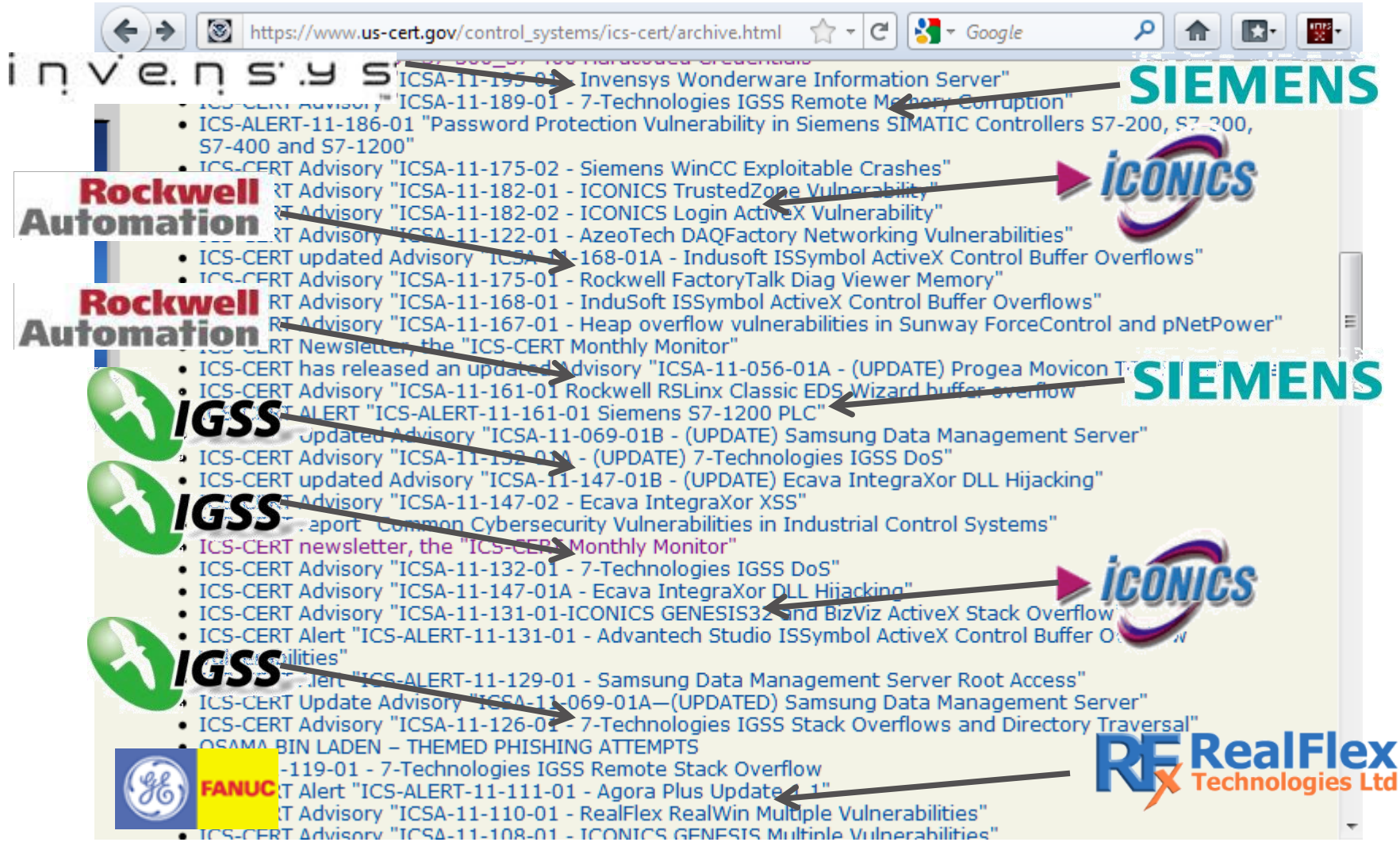
- Operators at a major US nuclear power plant forced to "scram" the reactor after cooling drive controllers crashed due to "excessive network traffic"

NET IMPACT: $2M

The Stuxnet Worm

- **July, 2010:** Stuxnet worm was discovered attacking Siemens PCS7, S7 PLC and WIN-CC systems around the world
- Infected 100,000 computers and at least 22 industrial sites
- Created to destroy uranium enrichment centrifuges in Iran
- Stuxnet software can be reused, enabling less sophisticated organizations to deliver new attacks to new targets
- Brought unwanted attention to the weaknesses of ICS/SCADA security
  - Public, Government and Senior Management in customer organizations
  - Security Researchers now targeting ICS and SCADA components

Many of our friends affected/infected…

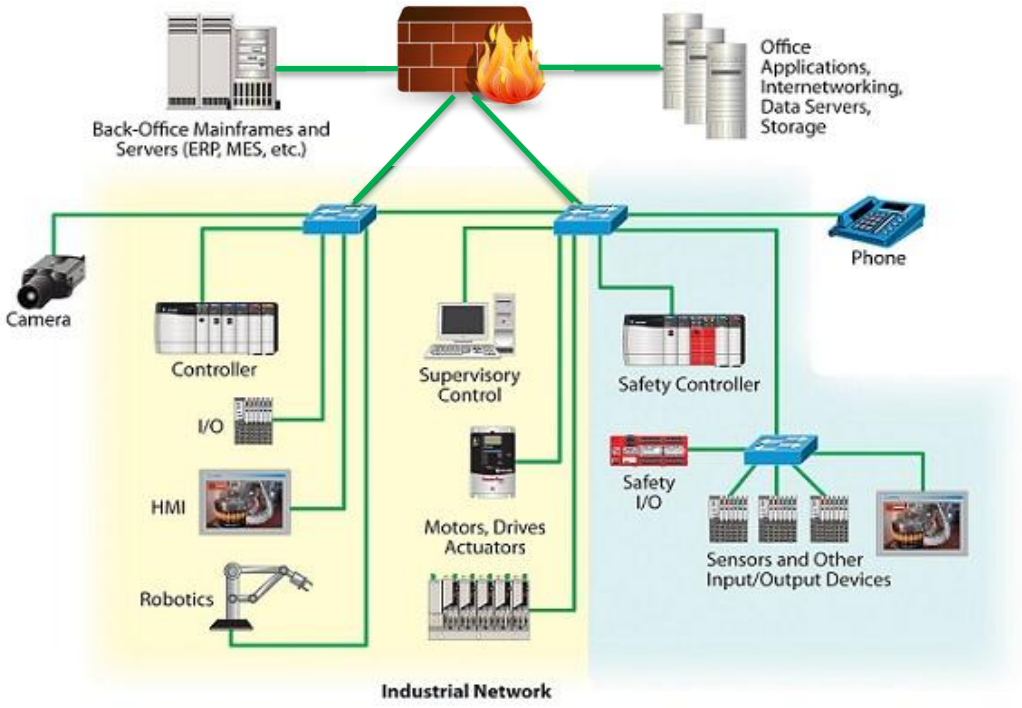


Cyber Security Take-Aways/Trends

- The importance of cyber security continues to increase regarding more reliable infrastructure design and best practice decisions
- ***Equipment vendors*** must include security requirements in the design of new products, and retrofit security on existing products
- ***Plant operators*** must act now to secure facilities against accidental and malicious cyber security incidents

We Have a Firewall – Aren't We Secure?

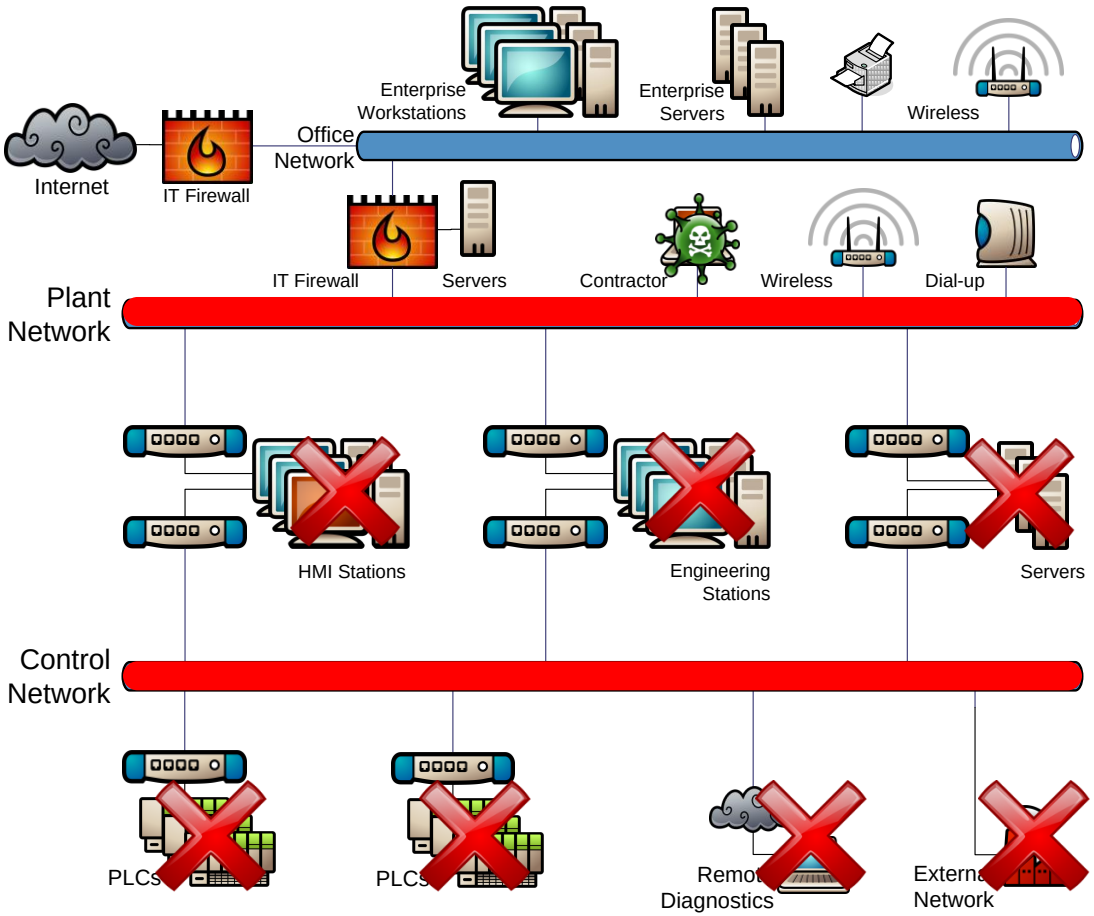
- Why Control and SCADA Networks are so Vulnerable
- Security Strategies that Work on the Plant Floor



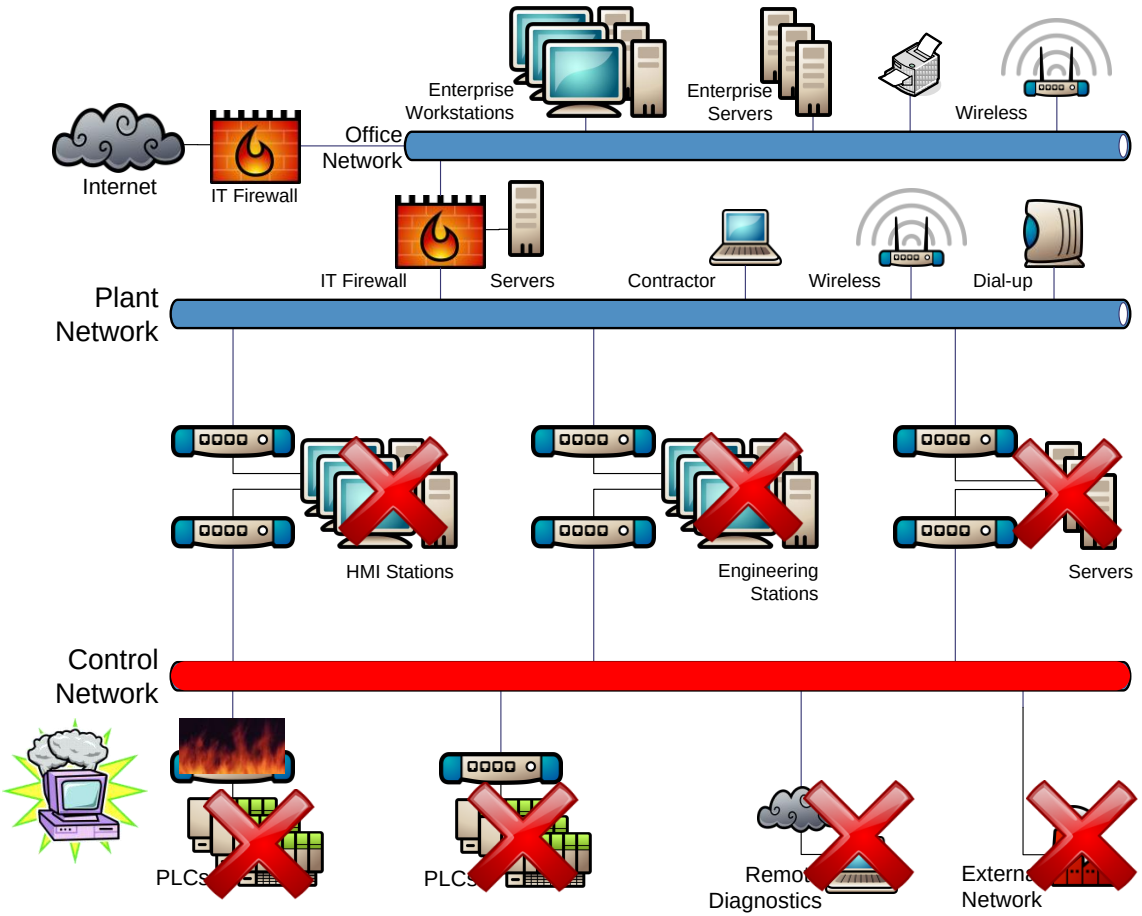
Security Issues in Control Networks

- "Soft" Targets
  - PCs run 24x7 without security updates or even antivirus
  - Controllers are optimized for real-time I/O, not for robust networking connections
- Multiple Network Entry Points
  - The majority of cyber security incidents originate from secondary points of entry to the network
  - USB keys, maintenance connections, laptops, etc.
- Poor Network Segmentation
  - Many control networks are "wide-open" with no isolation between different sub-systems
  - As a result problems spread rapidly through the network

We Have a Firewall… Aren't We Secure?



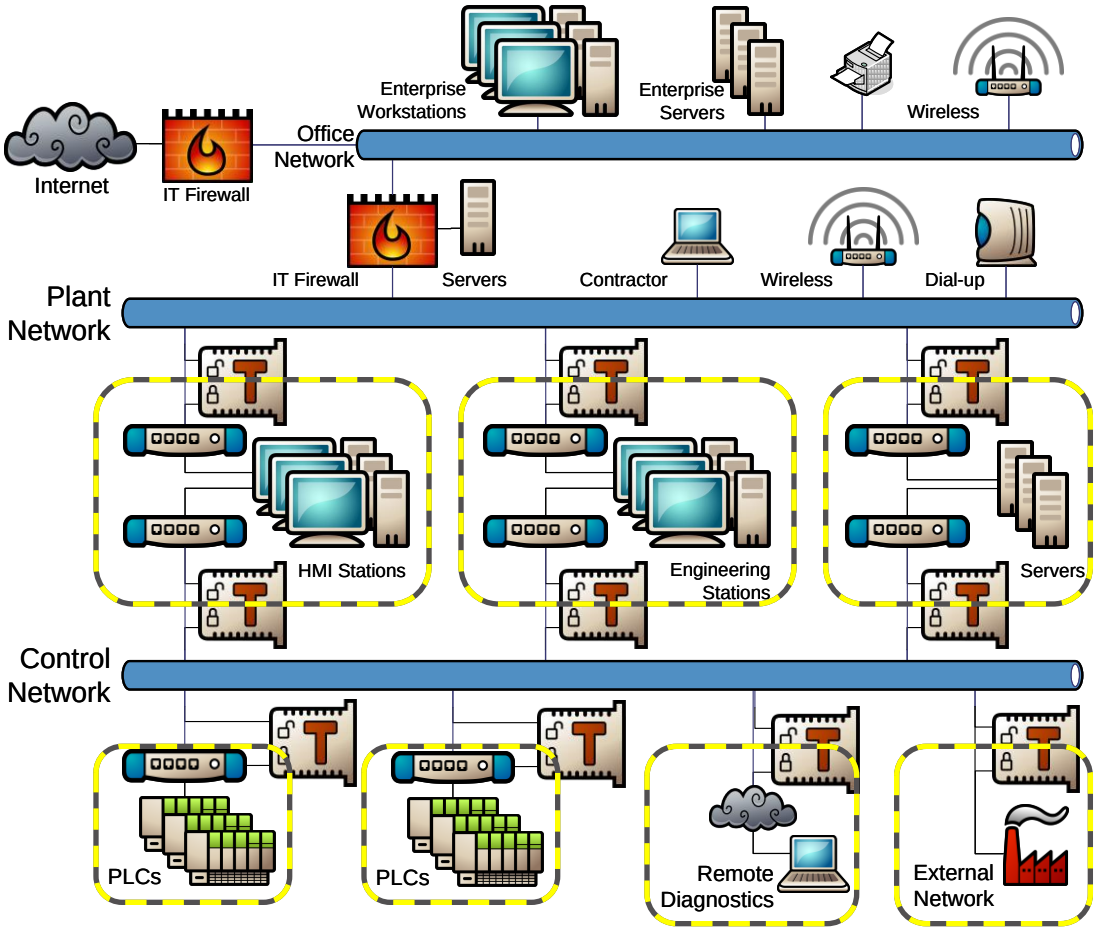
We Have a Firewall… Aren't We Secure?



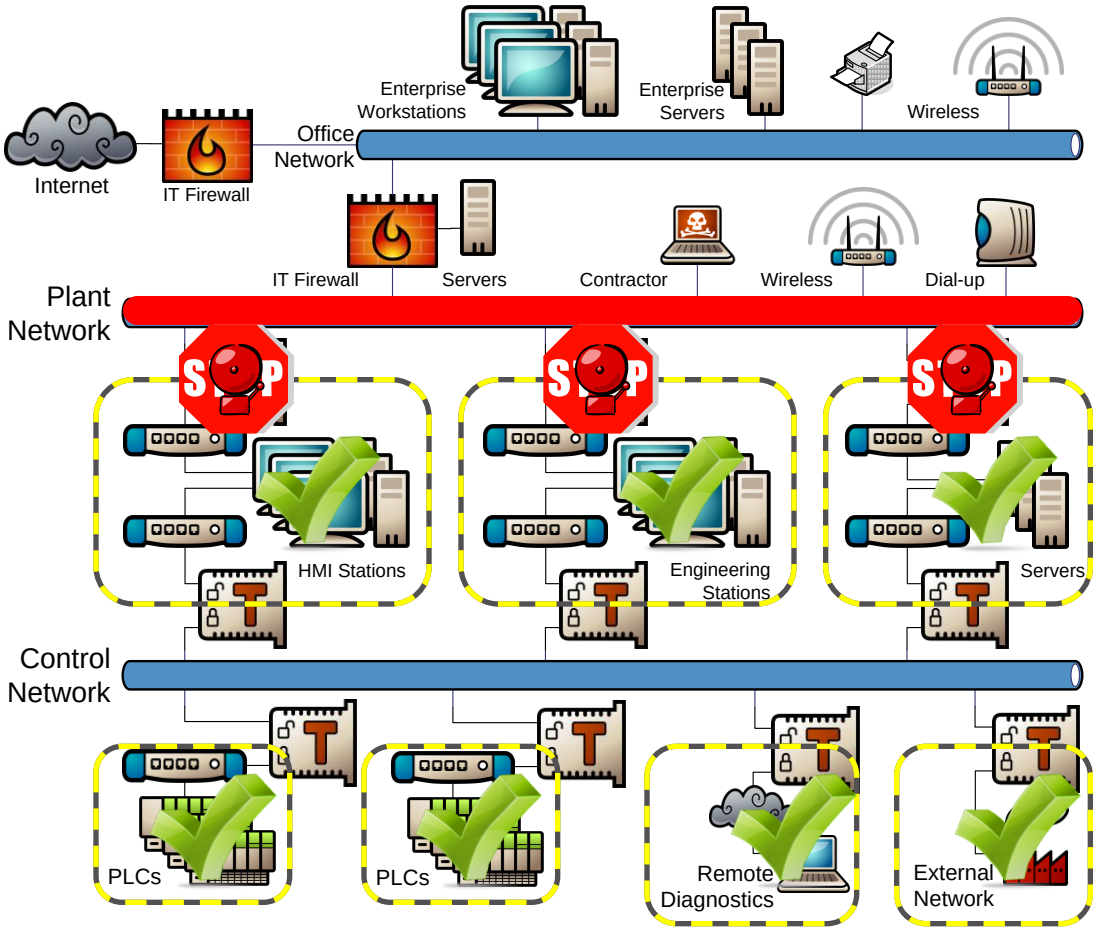
A Perimeter Defense is Not Enough

- We can't just install a firewall at the edge of the network and forget about security.
  - The bad guys will eventually get in
  - Many problems originate inside the plant network
- We must harden the plant floor.
- We need Defense in Depth.
  - Identify the ISA99 'Zones' and 'Conduits' in the network
  - Allow only minimum required network traffic to pass between zones
  - Generate alarms when traffic blocked

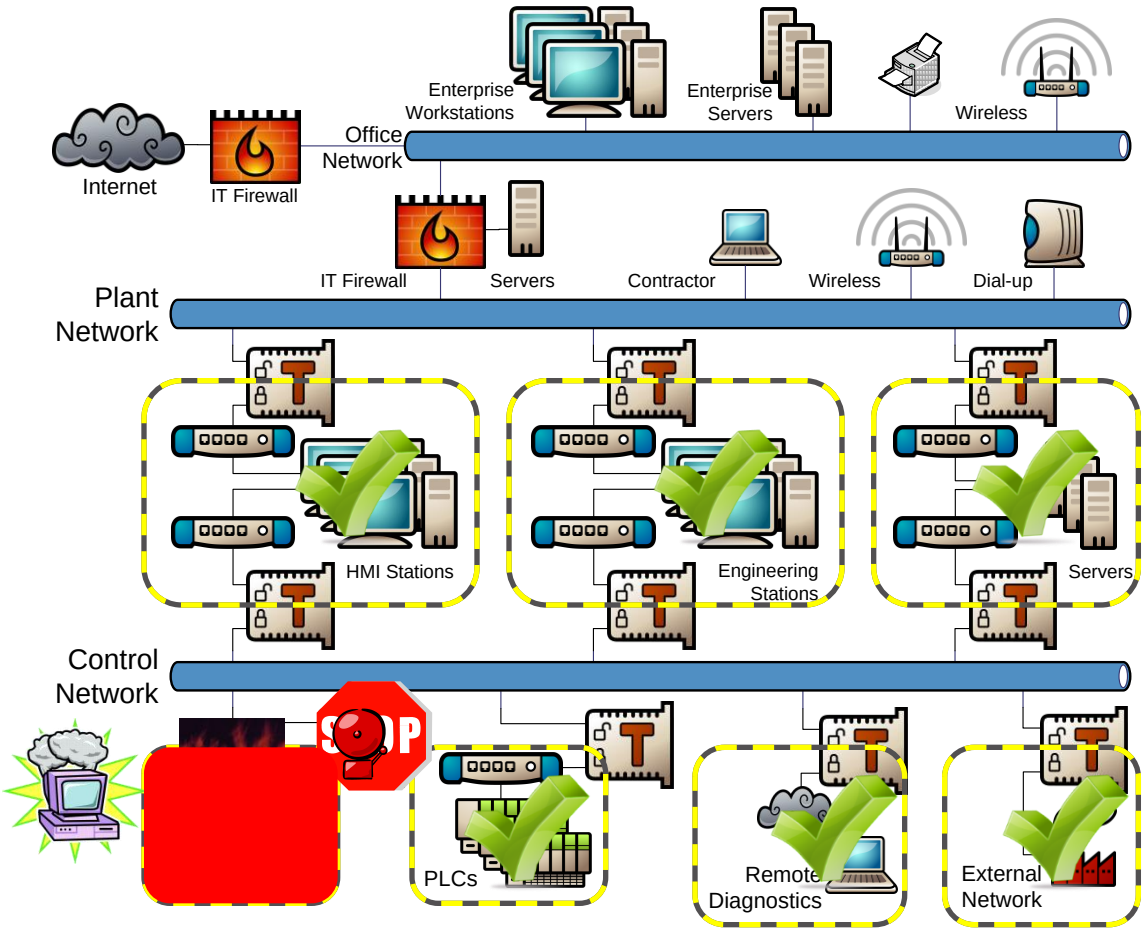
Zones and Conduits Provide Defense in Depth



Zones and Conduits Provide Defense in Depth



Zones and Conduits Provide Defense In Depth



Why is This Still a Problem?

- IT engineers have been successfully dealing with cyber security threats for years.
- Why not apply the same solutions to Control and SCADA networks?
- Control devices impose severe limitations
  - Cannot be secured with automated/third party tools
  - Patching or updating PLCs is usually not practical
- Security solutions must be specially adapted to the plant environment
  - Support for SCADA and industrial protocols
  - Configure, test and maintain without shutting down the network
  - Built to survive the harsh electrical & environmental conditions
  - Long life cycle (decades for control systems, vs years for IT)
  - Reduce complexity to reduce the risk of human error

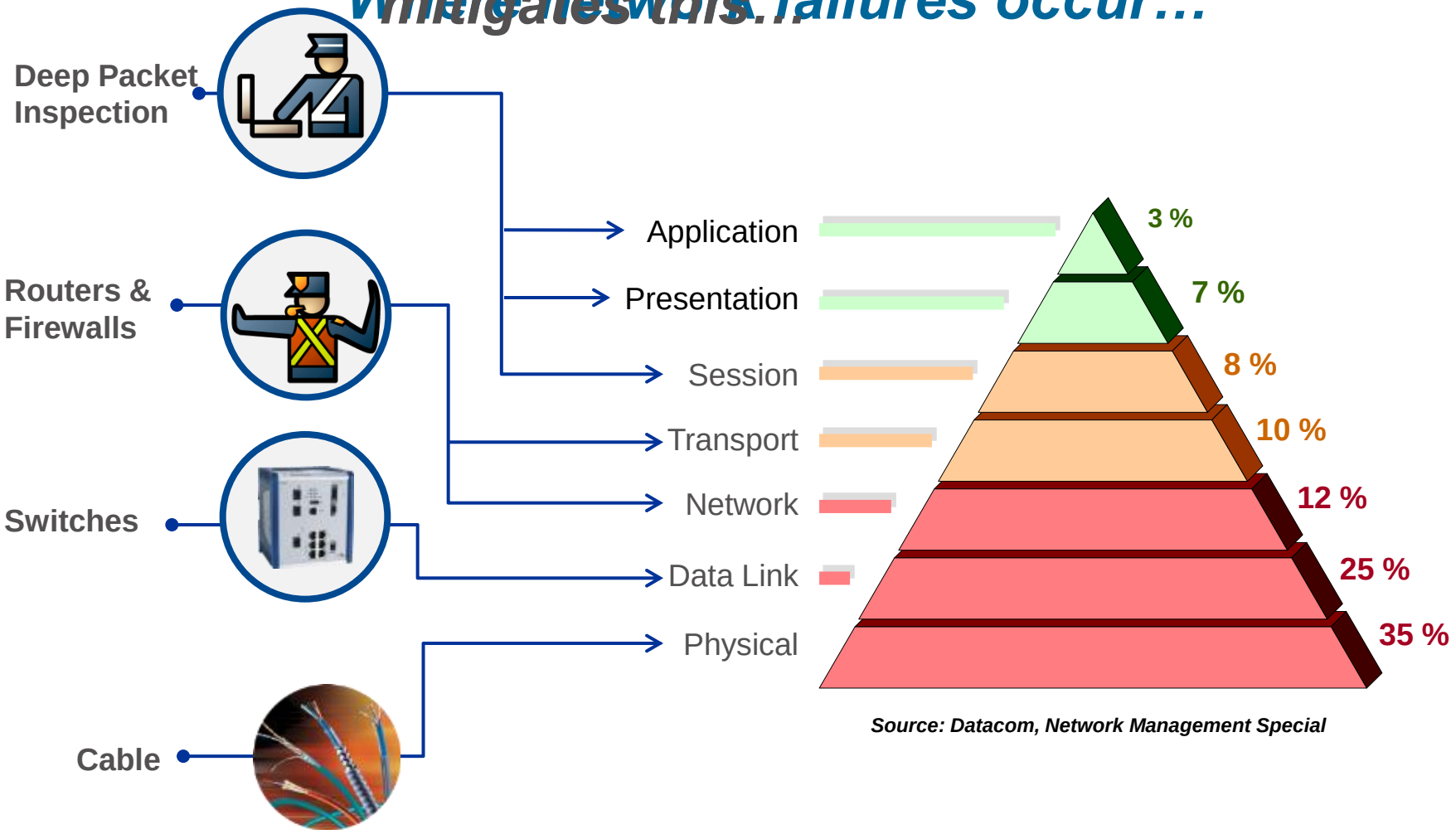
Defense in Depth via Distributed Security Appliances

- Add the missing layers of defense using security appliances that are specifically designed for the task
- Make sure the product is easy to install, configure, and manage *in the plant environment*
  - Ultra-reliable hardware
  - Install, configure, and manage with no plant down time
  - Support the equipment and protocols commonly used on the plant floor
  - Tools that are focused on the needs and capabilities of plant personnel

Network Reliability in the OSI Model

How Industrial Security Mitigates this…

Where network failures occur…



Source: Datacom, Network Management Special

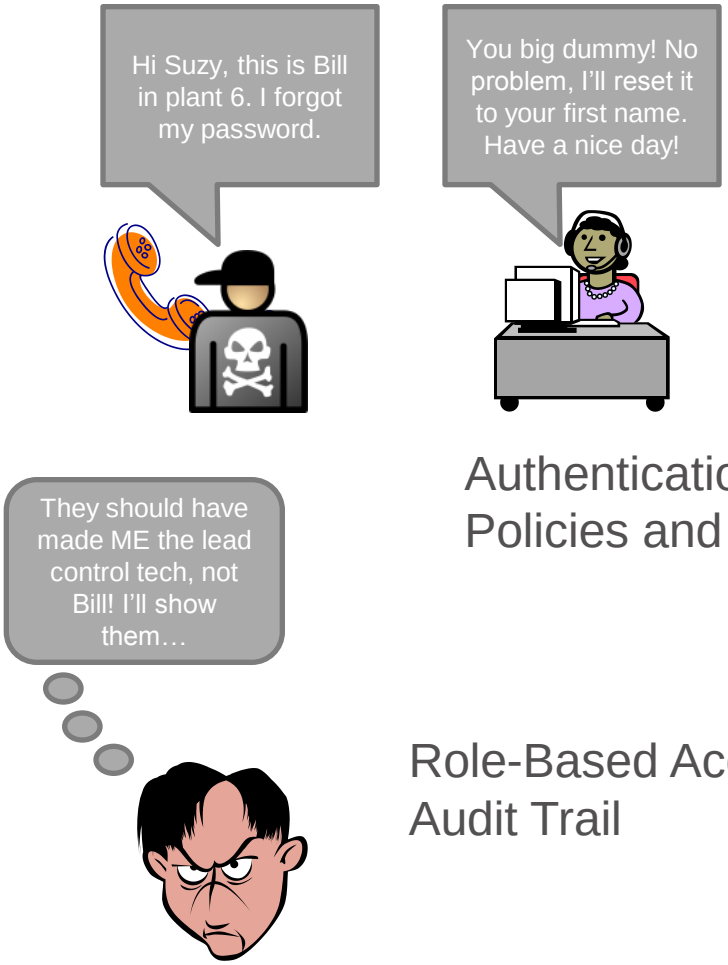
The Security Lifecycle

Managing Risk

Now my Network is Secure. I'm Done, Right?

Not So Fast…

Physical Security



Authentication,
Policies and Procedures

Role-Based Access Control,
Audit Trail

Security Policy

A security policy should cover the following key components:

- Roles and responsibility of those affected by the policy
- What actions, activities and processes are allowed and which are not?
- What are the consequences of non-compliance?

Key personnel who need to be included in the development of the policy include:

- Senior management
- Process Control and Plant Management
- Information Technology
- Human Resources
- Legal

The following areas of vulnerability should be considered:

- Network and operating environment security
- Application security
- Intrusion detection
- Regulating physical access to the SCADA network

Secure the SCADA Network

Corporate networks linked to the Internet or that use wireless technology may be more easily accessible to cyber terrorists and hackers. An organization can heighten its level of network security by isolating its SCADA network thereby restricting channels of external access.

Counter measures:

- Firewalls – appliance or software
- Virtual Private Networks – remote access
- De-militarized Zones – buffer zone
- Authentication – encryption techniques and software

Tips for Cyber Terrorism Defense:

1. Focus on the fact that you are a target. This is especially true for part of the Government and the 5 sectors of critical infrastructure: finance, health and safety, communications, transportation or public utilities.
2. Implement a full-scope Intrusion Management Strategy, not just Intrusion Detection. Understanding, planning, managing, detecting, responding, recovering and replanning, not just detecting, is critical to survival.
3. Understand that patterns evolve. Before a system can be compromised, an attacker needs to identify the perimeter defense and needs to find a weakness in that defense that allows them to gain access to a meaningful application. There are several signs that occur as a prelude to an attack. The earlier that those signs are recognized and corrective actions taken, the better the likelihood of successfully removing vulnerabilities, changing security weaknesses and ultimately resisting the security attack.

Tips for Cyber Terrorism Defense:

4. Humans can recognize patterns faster than they can analyze data. Let the computer store and organize data, which it can do best, but let the human brain spot the offending pattern, its key strength. Successful Event Recognition systems don't rely solely on hardware and software. They use that hardware and software to aid and assist a trained, experienced human expert.
5. An architecture must be resilient and easy to update. Cyber terrorists and attackers intelligently mutate their attack signatures; utilizing alternate channels. It is important to be able to change recognition methods and procedures for repelling such attacks quickly and effectively. There is not enough time to buy new equipment or change a software platform. The solutions implemented must have the flexibility to morph itself to provide an ever stronger, and unpredictable defense.

Layers of Security in a Control Network

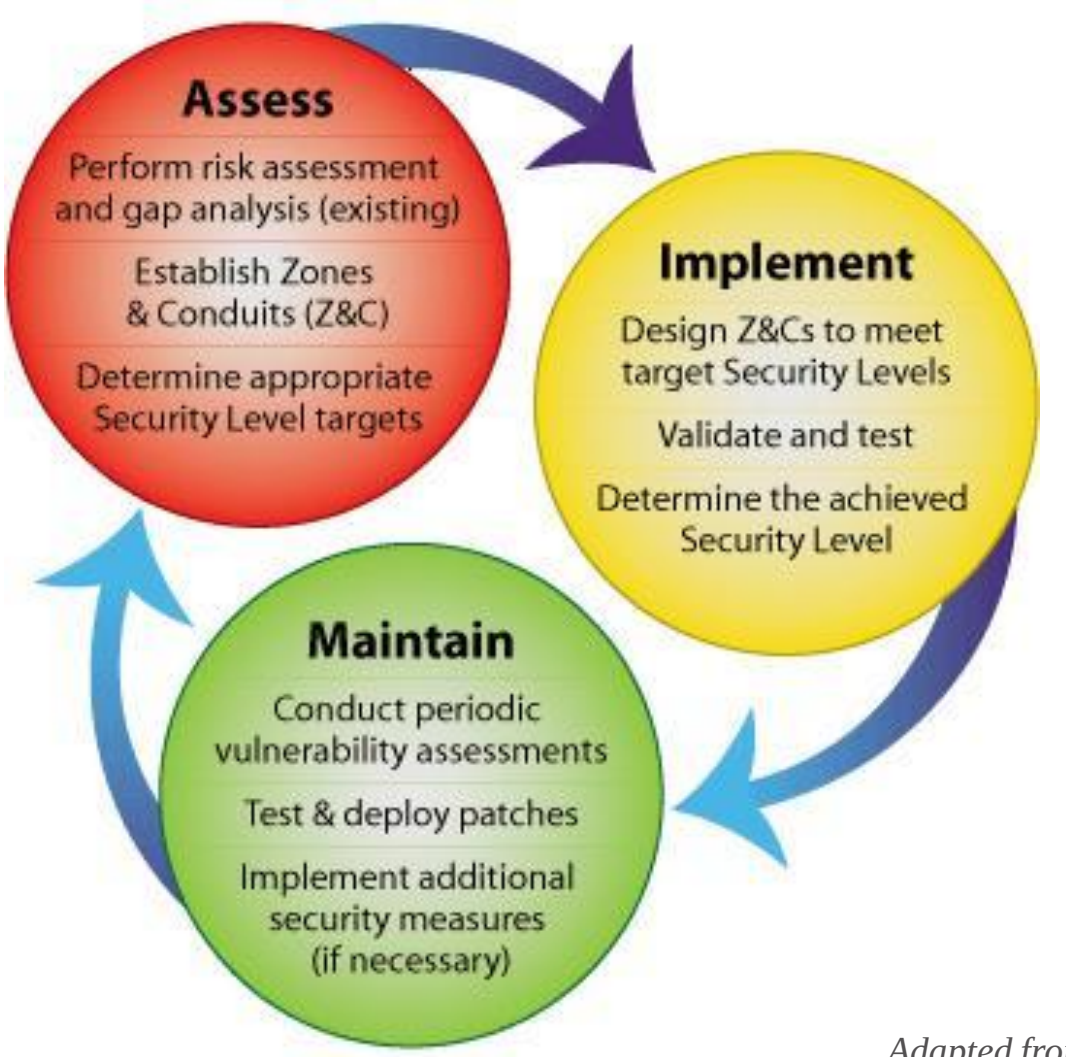
Layer	Solutions
1. Policy and Procedure	• DHS, ICS-CERT, ISA, IEC, NIST • Service providers
2. Physical	• Industrial security-specific wire, cable, cabinet, connectors • Industrial PoE switches & Industrial Ethernet cable • Cameras, keypads, alarmed doors, locks etc.
3. Computer	• Antivirus & whitelist products • Patch management policy & procedures • Role-based access control • Control other entry points (eg: USB, optical media)
4. Control Network	• Segmentation (Defense in Depth via Zones and Conduits) • Switch and Router security features • Intrusion Detection • Logging & Alarming
5. Automation Devices	• Configure & update wherever possible (turn off unused services; set up passwords; etc)

Layers of Security in a Control Network (Anixter Solutions in Red)

Layer	Solutions
1. Policy and Procedure	• DHS, ICS-CERT, ISA, IEC, NIST • Service providers
2. Physical	• Industrial security-specific wire, cable, cabinet, connectors • Industrial PoE switches & Industrial Ethernet cable • Cameras, keypads, alarmed doors, locks etc.
3. Computer	• Antivirus & whitelist products • Patch management policy & procedures • Role-based access control • Control other entry points (eg: USB, optical media)
4. Control Network	• Segmentation (Defense in Depth via Zones and Conduits) • Switch and Router security features • Intrusion Detection • Logging & Alarming
5. Automation Devices	• Configure & update wherever possible (turn off unused services; set up passwords; etc)

How Much Security Do I Need? Where Do I Put It?

The Security Lifecycle



Adapted from ISA S99.01.01

Risk Assessment with Mitigations

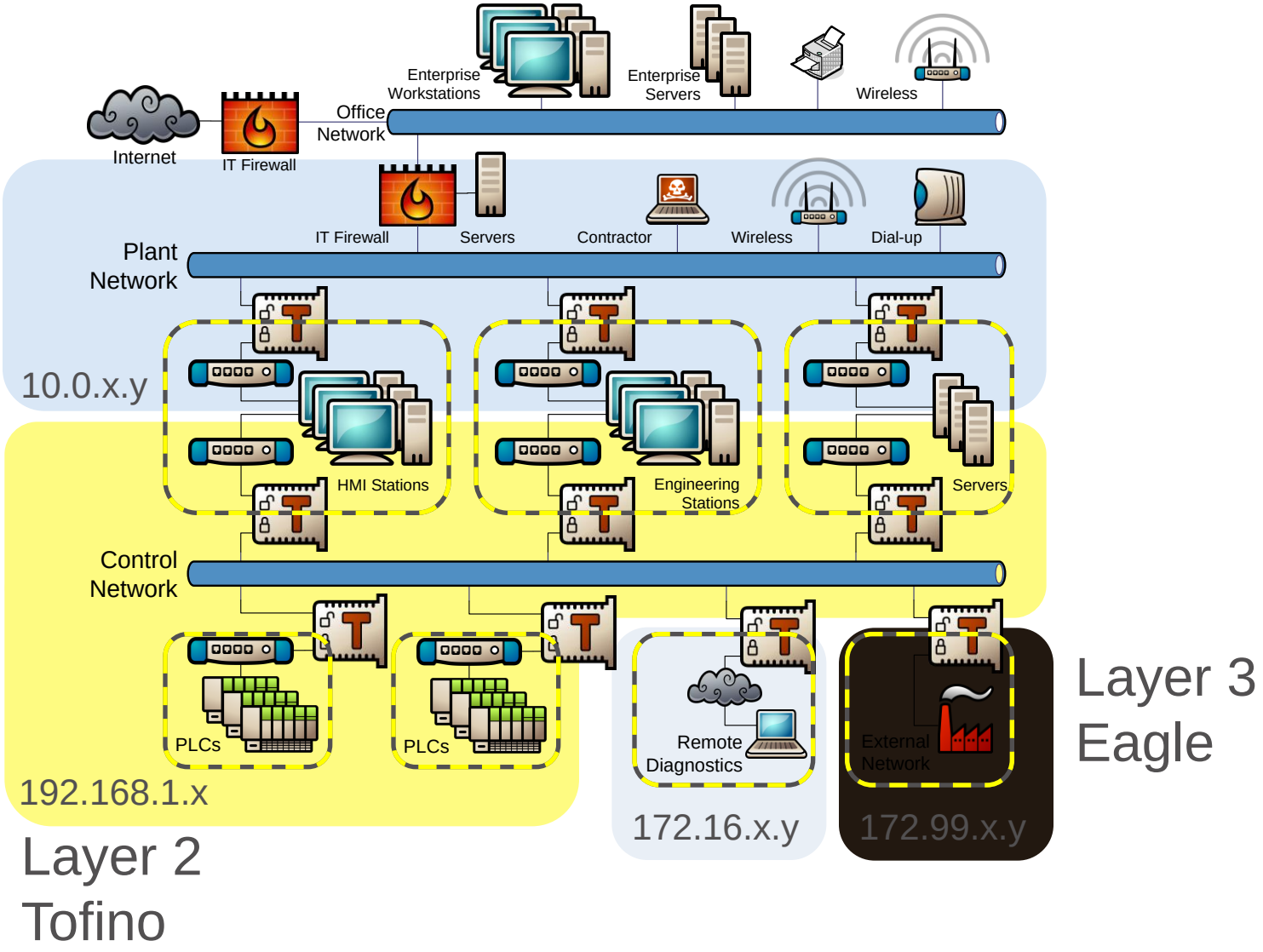
- A Security Risk Assessment answers some key questions:
  - What are my key risks and vulnerabilities?
  - Where do I install my security solutions, and what types do I need?

		Threat	Vulnerability		Consequence		DELIBERATE		ACCIDENTAL			DELIBERATE		ACCIDENTAL	
Ref	Entry Point	What Could Happen?	Is it possible?	How?	What is the worst thing that could happen?	Sev.	Likelihood	Risk	Likelihood	Risk	Mitigations	Likelihood	Risk	Likelihood	Risk
A	Business to PCN Firewall	Introduce malware	Yes	Virus on business network	Virus modifies or shutsdown the process	High	Med	Med	High	High	1.) Anti-virus on all Win SCADA boxes	Low	Med	Low	Med
		Introduce malware	Yes	Virus on business network	Virus modifies or shutsdown the process	High	Med	Med	High	High	1.) Anti-virus on all Win SCADA boxes 2.) Whitelisting on Win SCADA boxes	Neg.	Low	Neg.	Low
		Tamper (Modify/Delete data)	Yes	Gain access through firewall	Attacker modifies or shutsdown the process	High	Med	Med	Neg.	Low	1.) Strengthen firewall rules	Low	Med	Neg.	Low
		Tamper (Modify/Delete data)	Yes	Gain access through firewall	Attacker modifies or shutsdown the process	High	Med	Med	Neg.	Low	1.) Strengthen firewall rules 2.) Encrypt traffic	Neg.	Low	Neg.	Low
		Denial-of-service	Yes	Storm the firewall	No communications between Business and PCN	Med	Med	Med	Med	Med	1.) Intrusion detection 2.) Rate limiting	Low	Low	Low	Low

Belden's Security Solutions

Introducing the Eagle and Tofino

Minimizing Changes to Existing Equipment

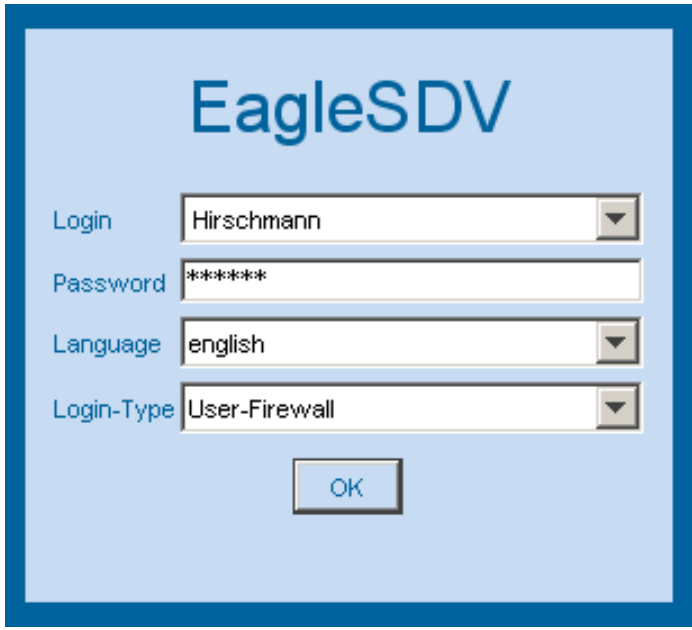


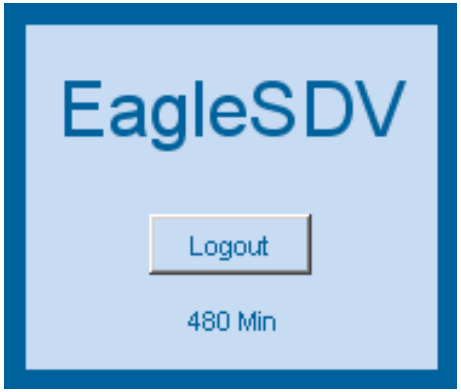
Eagle Secures the EDGE of the Network

- Firewall with Stateful Packet Inspection (SPI)
  - Both IP and non-IP (MAC address) filtering supported
  - Dynamic firewall rules based on user login credentials
- Layer 3 Router
  - 1:1 and 1:N Network Address Translation (NAT)
  - Dynamic DNS support for remote access
  - Layer 2 transparent mode option
- IPsec VPN
- Configuration and management via web browser, command line or HiVision

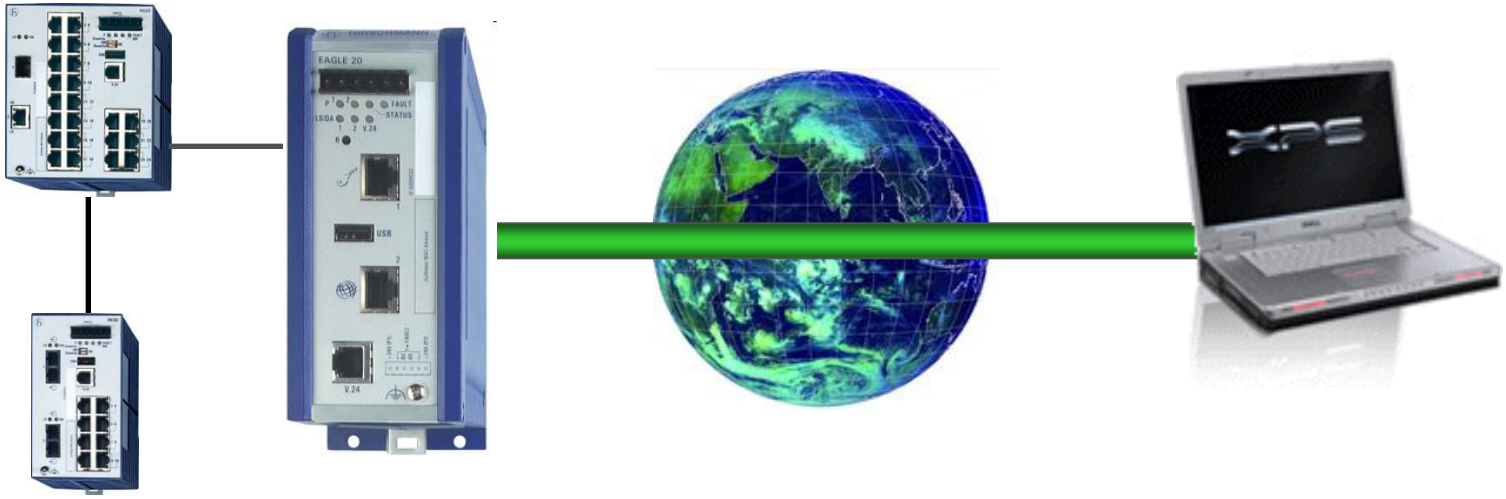
Dynamic Firewall Rules

- Additional firewall rules can be applied temporarily, based on a user logon
- Up to 32 different logons available
- Static or dynamic logout countdown
- Complete control of external service personnel
- For example, temporary firewall rules for access to:
  - Network components
  - PLCs
  - Robots
  - Drives
  - I/O

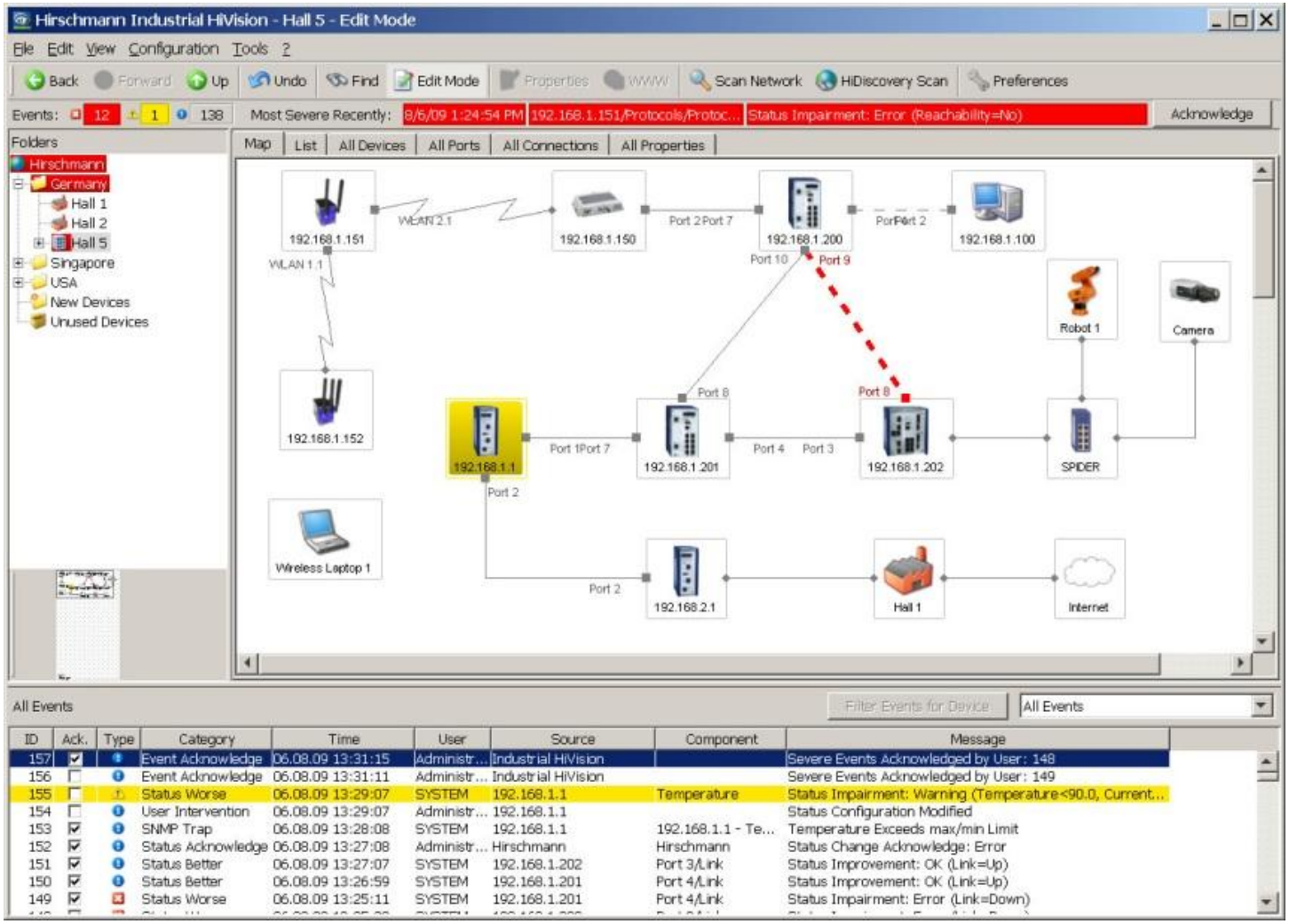




Client to Site VPN



Industrial HiVision

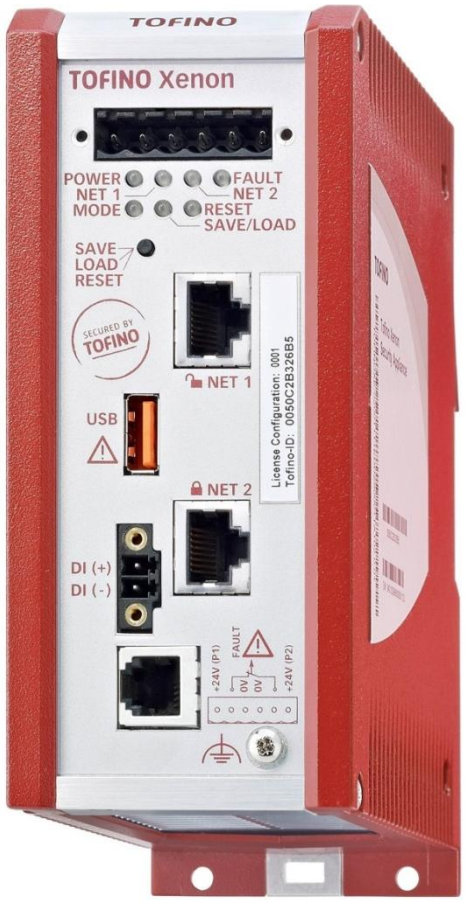


Belden Eagle Solutions

Feature	Eagle One	Eagle 20-0400	Eagle 30-0402
Application	Edge	Edge	Edge
LAN	2x 10/100	4x 10/100	4x 10/100
Uplink	-	-	2x SFP (GBE)
Redundancy	Ring Coupling	VRRP	VRRP
VLANs	1	Up to 64	Up to 64
Power Supply	9 - 60VDC / 24VAC	18 - 60VDC or 48 - 320VDC / 88 - 265VAC	18 - 60VDC or 48 - 320VDC / 88 - 265VAC
VPN	ipSEC	Q4 2014	Q4 2014
WAN	-	Q4 2014	Q4 2014
DI	1	1	1
Extended Temp, ATEX/C1D2	Yes	Yes	Yes

Tofino Secures the CORE of the Network

- Firewall with Stateful Packet Inspection (SPI)
  - Both IP and non-IP (MAC address) filtering supported
  - “Whitelist” approach provides high security with simple deployment
- Layer 2 Bridge with No IP Address
  - No disruption to existing network design
  - VERY secure
- Content Inspection filters traffic at the protocol level
  - Modbus/TCP, OPC, Ethernet/IP now; others to follow
- Simple deployment, configuration and management
- Test in the real network before deployment with no risk of plant disruption

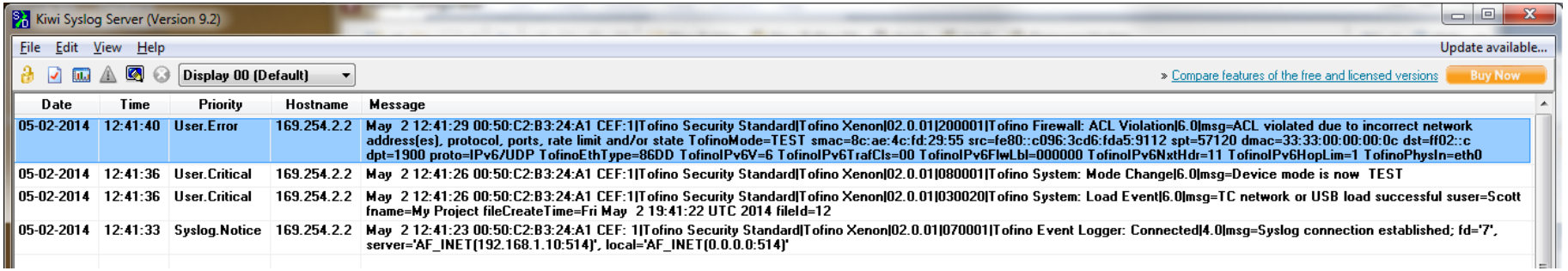


Tofino™ Enforcer Technology: Content Inspection for Industrial Protocols

- ‘Sanity Check’ blocks any traffic not conforming to the protocol standard
- Control engineer defines list of allowed commands and data points
- Blocks and reports any traffic that does not match your rules
- Modbus/TCP, OPC Classic, Ethernet/IP

Process-Friendly Test Mode

- Tofino™ operates in three modes:
  - PASSIVE - all traffic is bridged; logging off
  - OPERATIONAL – only permitted traffic is bridged; logging on
  - TEST – all traffic is bridged; logging on
- Test mode allows all traffic, but reports traffic that would have been dropped if in Operational



Only Belden Offers Plant-Wide Security Solutions

Application	Eagle EDGE Security	Tofino CORE Security
Primary mode of operation	Layer 3	Layer 2
Zones use different subnets	✓	
Zones within the same subnet		✓
Redundancy support	✓	✓
‘Retrofitting’ security into existing plant		✓
High-security applications		✓
‘step and repeat’ zones (NAT)	✓	
Securing critical Modbus controllers		✓
Securing OPC servers		✓
Remote access via VPN	✓	
Plant boundary security	✓	

Questions?

SCADA security – more holes than a leaky bucket?

March 2015, Software - SCADA/MES, This Week's Editor's Pick

By Andrew Ashton, contributing editor, SA Instrumentation and Control.

Is your ICS IT-security more effective than that of Nato or of nuclear energy plants? If not, best you read on.

In mid-2010 the Iranian nuclear industry suffered a major setback as a result of the Stuxnet computer malware – the first known malware targeted at Industrial Control Systems (ICS).

In mid-2014, Dragonfly, a second piece of malware targeted at ICS systems was discovered in the wild. Following hot on the heels of that discovery, in early October 2014, ICS-CERT alerted the ICS fraternity to the presence of the BlackEnergy2 virus1 and towards the end of 2014, the German Federal Office for Information Technology reported on physical damage at a blast furnace site after its ICS was compromised by a malware attack.2

Dragonfly

The name Dragonfly is used by Symantec to refer to the 'Dragonfly hacking group'. It has now become synonymous with a campaign, attributed to that group, aimed at stealing intellectual property from, inter alia, governments, utilities and the energy and manufacturing sectors. Dragonfly has been shown capable of discovering and listing OPC servers and OPC tags across ICS. That information could subsequently be used for industrial sabotage.

Aliases / associated with / in the same family as: Havex, Energetic Bear, Backdoor.Oldrea, Trojan.Karagany, Fertger, Peacepipe, Crouching Yeti.

Timeline

2014-05-12 The National Cyber Awareness System publishes confidential information3 on malware that it calls Dragonfly, which, ". . . allows remote attackers to execute arbitrary commands via unspecified vectors."

2014-06-23 Finnish security company, F-Secure, publishes a report titled "Havex Hunts for ICS/SCADA Systems".4 According to this report, F-Secure has been monitoring the Havex malware family and the group behind it for the prior year. In early 2014, the malware targeted industrial control systems through compromised downloads from multiple legitimate ICS suppliers. Of particular interest from this report:

• One of the components of the malware is able to harvest information from compromised systems.

• The malware leverages security flaws in OPC classic (previously OLE for Process Control) and the underlying Microsoft DCOM technology on which OPC classic was built, to gain information about connected devices, and to relay that information to Command and Control (C2) servers.
• F-Secure has recorded 88 variants of the malware.

2014-06-30 Symantec Security Response releases a whitepaper5 detailing a campaign that it refers to as, "[A]n ongoing cyber espionage campaign dubbed Dragonfly (aka Energetic Bear)". Symantec started monitoring the Dragonfly group in 2012. According to that whitepaper, initial targets were defence and aviation companies in the US and Canada, and then in spring 2013 the focus shifted to US and European energy firms. The Symantec white-paper notes:
• The Dragonfly operation shows signs of being state-sponsored.
• File dates and times seem to indicate regular daily working hours which tie in with the Eastern European time zone (UTC +2).
• Dragonfly utilises three methods to compromise systems – phishing emails, watering hole attacks and trojanised software upgrades.
• Oldrea gathers system information, file and program lists, Outlook address book data and VPN configuration files. This data is then written to a temporary file in an encrypted format before being sent to a remote C2 server controlled by the attackers.
• Karagany can upload stolen data, download new files, and run executable files on an infected computer. It is also capable of running additional plug-ins for password collection, screen capture and cataloguing documents.

2014-07-01 ICS-CERT issues Advisory ICSA-14-178-01 as a follow-up to updated alert CS-ALERT-14-176-02A. The follow-up provides additional details on Havex and ISC. Key aspects of this alert:
• The known components of the identified Havex payload do not appear to target devices using the OPC Unified Architecture (UA) standard.
• The Havex payload has the capability of enumerating OPC tags.
• ICS-CERT has not found any additional functionality to control or make changes to the connected hardware.
• The Havex payload has caused multiple common OPC platforms to intermittently crash. This could cause a denial of service effect on applications reliant on OPC communications.

2014-07-17 FireEye releases a detailed report6 after examining the OPC activity of one variant of Havex. According to the report:
• The malware scans for OPC servers on the infected machine and laterally across the network, building a list of all OPC servers that are globally accessible through Windows networking, along with the capabilities supported by each such server discovered.
• The details of discovered servers and of their capabilities are saved in two separate unencrypted .dat files, and once the recursive scanning task is completed, the unencrypted log is encrypted using a 168-bit 3DES key.
• The version of Havex used in this test also creates a file for each OPC server, with its state and with each OPC tag enumerated by tag name, tag type, access level and id.
• It is presumed that encrypted files are sent to one of the many C2 servers under the control of Dragonfly.

2014-07-31 A report7 by the Global Research and Analysis Team (GReAT) team at Kaspersky Labs is published with a few new takeaways:
• Globally they have observed about 2800 victims of Dragonfly.

• Most victims are in the industrial / machinery building sector.
• It appears that the campaign originated at the end of 2010.

2014-09-15 Belden announces the outcome of a study8, which it commissioned Joel Langill of RedHat Cyber to undertake, in order to discover more about Dragonfly. This study reveals:
• The three targets of the trojanised software are primarily suppliers to the pharmaceutical sector, not the energy sector.
• Dragonfly bears some resemblance to the Epic Turla attack, which [according to Langill] targeted the IP of pharmaceutical companies.
• The Industrial Protocol Scanner of Dragonfly searches for devices on TCP ports 44818 (Omron, Rockwell Automation), 102 (Siemens) and 502 (Schneider Electric). These protocols and products have a higher installed base in packaging and manufacturing applications typically found in consumer packaged goods industries, such as pharmaceutical rather than the energy industry.
• [Consequently] the [current] target is most likely the pharmaceutical sector, not the energy sector.

2015-02-12 Fast-forwarding to 2015, there is no doubt more to be revealed about Dragonfly and its successful exploits in ICS.

BlackEnergy2

The BlackEnergy toolkit is malware used for criminal purposes and first saw the light of day in 2007. Originally crafted for the creation of botnets for use in DDoS, it has evolved in several different directions and is today used for spamming, theft of bank credentials, password theft, state-on-state cyber-terrorism, and in one of its latest guises, for industrial espionage through scada systems.

Because the toolkit is widely available and used by many different groups for different purposes, it is not easy to attribute its usage in the ICS space to a particular group. Its application in theft of IP via scada systems was first reported in August 2014.

Aka / associated with / in the same family as: Sandworm, BKDR_BLACKEN.A and BKDR_BLACKEN.B, Blakken, Fonten

Timeline

2014-10-08 ICS_CERT releases a TLP Amber alert (ICS-ALERT-14-281-01P) to its US-CERT secure portal.

2014-10-14 iSIGHT Partners, which has been analyzing Sandworm (BlackEnergy2) and working closely with Microsoft, reports9 on the discovery of a zero-day vulnerability affecting all supported versions of Microsoft Windows, Windows Server 2008 and 2012, and Microsoft releases a patch for this vulnerability (CVE-2014-4114). Key aspects of the iSIGHT report:

• The campaign's purpose is cyber espionage.
• The campaign is attributed to the Sandworm team.
• The campaign is tightly targeted, with victims being Nato, Ukrainian government organisations, a Western European government organization, energy sector firms (specifically in Poland), European telecommunications firms and a US academic organization.

• Although the Sandworm team had been targeting Nato and others before this latest assault, attacks using this zero-day vulnerability started in June 2014.

2014-10-16 Trend Micro's TrendLabs reports new findings10, the most important of which is that one of the attack vectors is via GE Intelligent Platform's CIMPLICITY HMI solution suite.

2014-10-21 iSIGHT Partners reports11 additional information related to the scada attack vector, noting that additional files suggest that Siemens WinCC scada is also being used as an attack vector.

2014-10-29 ICS-CERT publishes an alert12 concerning an ongoing malware campaign using a variant of the BlackEnergy malware. Key points from the report:
• The campaign has compromised numerous ICS.
• The campaign has been ongoing since at least 2011.
• Multiple companies have identified the malware on Internet-connected HMIs from the product families GE Cimplicity, Advantech/Broadwin WebAccess and Siemens WinCC.
• Any companies that have been running Cimplicity since 2012 with their HMI directly connected to the Internet could be infected.

2014-11-03 Kaspersky labs' Securelist publishes a detailed report13 on BlackEnergy2. From a control and instrumentation perspective, the key takeaway of the report is that a set of victims discovered that Siemens' "ccprojectmgr.exe" [WinCC] was responsible for downloading and executing BlackEnergy between March 2014 and July 2014.

2014-11-21 Siemens publishes an Industrial Security Alert recommending users to update SIMATIC WinCC to the latest release [which addresses the ICS-CERT alert]. The company also issues a detailed Security Advisory SSA-134508: Vulnerabilities in SIMATIC WinCC, PCS 7 and WinCC in TIA Portal.14

2015-02-12 As the year progresses we expect there will be further revelations of this group targeting owners of scada systems – either to extract information about those systems or as a backdoor into their corporate systems for espionage and worse.

German blast furnace incident

In mid-December 2014 the German Federal Office for Information Technology (BSI) published its report2 on the state of IT security in 2014, in which it describes a targeted attack on a German steel plant. The malware entered the company's office network via sophisticated phishing and social engineering vectors and from there gained access to the production network. The plant experienced an increased frequency of individual components and of production units. Ultimately this led to a situation in which the control system was unable to bring the blast furnace to a safe state and massive damage occurred.

Unfortunately, BSI has so far revealed very little about the incident. However, at least one industry commentator has suggested that it can probably be attributed to either Dragonfly or BlackEnergy.15

Points to ponder

Are we to take these attacks at face value and assume they are purely industrial espionage, or are they the first phase of a search and destroy mission in which the stolen information on control system

topologies and OPC tags is used to cause not only economic hardship for targets through loss of IP, but also loss of production capacity and injury to personnel through subsequent sabotage?

We subtitled this article, “Complacency could kill careers, co-workers and companies”, so let’s wrap it up by turning our backs on technicalities and facing some of the consequences of failing to adequately secure an IT installation.

Career killer

After the Sony hack, which revealed to the world at large, amongst other items, the content of 5000 of her private emails, Amy Pascal was fired as co-chair of Sony’s movie studios. It would not stretch the bounds of belief to imagine that one or more senior IT members also found themselves looking for a new career.

Co-worker killer

The German blast furnace incident must be a huge wake-up call to all IT practitioners who oversee C&I networks. Five thousand cubic metres of charge at around 1500°C is an immense amount of energy to lose control of. In November 2013, a blast furnace being commissioned at Bhushan Steel in India exploded killing at least one worker and injuring many more. As a result of the incident, three top officials of BSL, including its chief operating officer (COO), were arrested on charges of negligence.

Company killer

On its own, cyber espionage can destroy a company. Key intellectual property that is stolen can leave industry-leading companies with no unique selling proposition once their IP such as developments, detailed designs, engineering drawings, recipes, process steps, operating parameters, customer list and source code etc. are revealed to unscrupulous competitors. All it takes is one incident and a company can be forced into bankruptcy and closure.

On 17 June 2014, Code Spaces, a site that provided code hosting services which were ultimately hosted on Amazon’s Elastic Compute Cloud, was subjected to a DDoS. Reportedly the attacker demanded a significant ransom. The company failed to agree to the ransom and attempted to lock the intruder out, to which his response was to wipe all the company’s files on Amazon’s Cloud infrastructure. According to a statement published at the time on its website, “We finally managed to get our panel access back but not before he had removed all EBS [Amazon Elastic Block Store] snapshots, S3 [Amazon Simple Storage Service] buckets, all AMI’s [Amazon Machine Images], some EBS instances and several machine instances. In summary, most of our data, backups, machine configurations and offsite backups were either partially or completely deleted.”

Immediately after this devastating attack, the company announced, “Code Spaces will not be able to operate beyond this point, the cost of resolving this issue to date and the expected cost of refunding customers who have been left without the service they paid for will put Code Spaces in an irreversible position both financially and in terms of ongoing credibility.”

http://www.instrumentation.co.za/8303a

Takeaways

1. Antivirus systems typically respond to known attack vectors, not zero-day exploits. Campaigns like Stuxnet, Dragonfly and BlackEnergy2 were active for typically two years or more before being exposed. Based on past performance, this means that your ICS infrastructure may already be compromised by 2016's, 2017's or 2018's killer APT.
2. Just because there are no obvious signs of malware in your ICS (computers that fail to boot, high traffic volumes, etc.), it does not mean that your system is not already controllable by an outsider group.
3. No company or organisation is too big or too small to avoid being a potential targeted victim of a malware campaign that steals intellectual property and / or sabotages plants and processes.
4. If your scada system becomes the target, or worse still, the victim, of one of these campaigns your job security and career path will be affected.
5. If your plant becomes victim to malware and consequent sabotage, as in the German case quoted above, senior management of all designations and certainly of the IT and engineering divisions could face arrest, compensation claims and possibly years behind bars.
6. If you are living in the misguided belief that your cloud-based service provider is protecting your data and backups, you have work to do.
7. Your company may not survive the destruction of all of its software, data assets and backups.
8. Don't write emails with the premise that they are confidential. If each and every one of them was published in the public domain, would their contents cause you embarrassment?

Glossary Term	Information
3DES	In cryptography, Triple DES (3DES) is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block[8].
APT	An advanced persistent threat (APT) is a set of stealthy and continuous computer hacking processes, often orchestrated by human(s) targeting a specific entity. APT usually targets organisations and/or nations for business or political motives. APT processes require a high degree of covertness over a long period of time. The "advanced" process signifies sophisticated techniques using malware to exploit vulnerabilities in systems. The "persistent" process suggests that an external command and control system is continuously monitoring and extracting data from a specific target[8].
Botnet	A botnet is a collection of Internet-connected programs communicating with other similar programs in order to perform tasks. This can be as mundane as keeping control of an Internet Relay Chat (IRC) channel, or it could be used to send spam email or participate in distributed denial-of-service attacks[8].
Command and Control server	A malware's originator can control the activity of malicious programs on a compromised computer via one or more host servers. The server(s) that the malicious software interacts with (sends data to and receives instructions from) is known as the command-and-control (C2) server.
DCOM	Distributed Component Object Model (DCOM) is a proprietary Microsoft technology for communication among software components distributed across networked computers. DCOM, which originally was called "Network OLE", extends Microsoft's COM, and provides the communication substrate under Microsoft's COM+ application server infrastructure[8].
DDoS	A distributed denial-of-service (DDoS) attack occurs when multiple systems flood the bandwidth or resources of a targeted system, preventing that resource from being able to timeously or adequately perform its normal tasks.
ICS-CERT	The [US] Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) operates within the National Cybersecurity and Integration Center (NCCIC), a division of the Department of Homeland Security's Office of Cybersecurity and Communications (DHS CS&C). NCCIC/ICS-CERT is a key component of the DHS Strategy for Securing Control Systems[8].
National Cyber Awareness System	The National Cyber Awareness System is America's first cohesive national cybersecurity system for identifying, analysing, and prioritising emerging vulnerabilities and threats. It is managed by the US-CERT[8].
OPC classic	Originally called OPC for process control, this connectivity standard became the Esperanto of industrial communications protocols allowing multiple dissimilar devices to communicate with computers via a common protocol. The classic version, which dates back to the mid-1990s, was built on Microsoft's COM/DCOM technology.
OPC Unified Architecture	OPC Unified Architecture (OPC UA) was designed to operate cross-platform (and hence independent of Microsoft components and services) and to provide an extensible architecture incorporating secure communications.
Phishing	Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and some times, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting public[8].
TLP	The Traffic Light Protocol (TLP) is a set of designations used to ensure that sensitive information is shared with the correct audience. It employs four colours [red, amber, green, white] to indicate different degrees of sensitivity and the corresponding sharing considerations to be applied by the recipient(s)[8].
Trojanised software	Legitimate software, such as drivers and application updates, to which a malicious payload has been added. Supplier sites for updates and downloads can unknowingly become sources of trojanised software.
Watering hole attack	A computer attack strategy identified in 2012 by RSA Security, in which the victim is a particular group (organisation, industry, or region). In this attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with malware. Eventually, some member of the targeted group gets infected. Relying on websites that the group trusts makes this strategy efficient, even with groups that are resistant to spear phishing and other forms of phishing[8].
Zero-day vulnerability	A zero-day vulnerability is a vulnerability in a computer application or operating system of which the developers and users are unaware.

Glossary references
1. Wikipedia, http://en.wikipedia.org/, [2015-02-12].
2. ICS-CERT, https://ics-cert.us-cert.gov/, [2015-02-12].
3. US_CERT, Frequently Asked Questions, https://www.us-cert.gov/faq, [2015-02-12].
4. US-CERT, Traffic Light Protocol (TLP) Matrix and Frequently Asked Questions, https://www.us-cert.gov/tlp, [2015-02-12].

Article references

1. ICS-CERT, Alert (ICS-ALERT-14-281-01B) Ongoing Sophisticated Malware Campaign Compromising ICS, 2014-12-10, http://tinyurl.com/ldzw6m6, [2015-02-12].
2. Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2014, 2014-12, http://tinyurl.com/ns4sy2g, [2015-02-12].
3. National Vulnerability Database, Vulnerability Summary for CVE-2013-5671, 2014-05-12, http://tinyurl.com/jwzuxt2, [2015-02-12].
4. F-Secure, Havex Hunts for ICS/SCADA Systems, 2014-06-23, http://tinyurl.com/p65plco, [2015-02-12].
5. Symantec Security Response, Dragonfly: Cyberespionage Attacks Against Energy Suppliers, 2014-07-07, http://tinyurl.com/kauk4q4, [2015-02-12].
6. FireEye, Havex, It's Down With OPC, 2014-07-17, http://tinyurl.com/ogxd3ty, [2015-02-12].
7. Kaspersky Lab, Energetic Bear: more like a Crouching Yeti, 2014-07-31, http://tinyurl.com/pnmjj9y, [2015-02-12].
8. BusinessWire, Belden Research Reveals Dragonfly Malware Likely Targets Pharmaceutical Companies, 2014-09-15, http://tinyurl.com/pbljj9e, [2015-02-12].
9. iSIGHT Partners, iSIGHT discovers zero-day vulnerability CVE-2014-4114 used in Russian cyber-espionage campaign, 2014-10-14, http://tinyurl.com/mzsjsjk, [2015-02-12].
10. Trend Micro, Sandworm to Blacken: The SCADA Connection, 2014-10-16, http://tinyurl.com/oy5oan3, [2015-02-12].
11. iSIGHT Partners, Sandworm Team – Targeting SCADA Systems, 2014-10-21, http://tinyurl.com/m4b7at3, [2015-02-12].
12. ICS-CERT, Alert (ICS-ALERT-14-281-01B) Ongoing Sophisticated Malware Campaign Compromising ICS (Update B), 2014-12-10, http://tinyurl.com/ldzw6m6, [2015-02-12].
13. Kaspersky Lab, BE2 custom plugins, router abuse, and target profiles - New observations on BlackEnergy2 APT, 2014-11-03, http://tinyurl.com/nf8t3ok, [2015-02-12].
14. Siemens, SSA-134508: Vulnerabilities in SIMATIC WinCC, PCS 7 and WinCC in TIA Portal, 2014-11-21, http://tinyurl.com/o2j9fmb, [2015-02-12].
15. ICS-SANS, ICS CP/PE (Cyber-to-Physical or Process Effects) case study paper – German Steel Mill Cyber Attack, 2014-12-30, http://tinyurl.com/k9lwbpw, [2015-02-12].

About the author

Andrew Ashton has electrical, mechanical and business qualifications and has been active in automation and process control since the early 1980s. Since 1991 he has headed up a company that has developed formulation management systems for the food, pharmaceutical and chemical manufacturing industries and manufacturing solutions involving the integration of various communication technologies and databases. Developed systems address issues around traceability, systems integration, manufacturing efficiency and effectiveness. Andrew is a contributing editor for SA Instrumentation and Control.