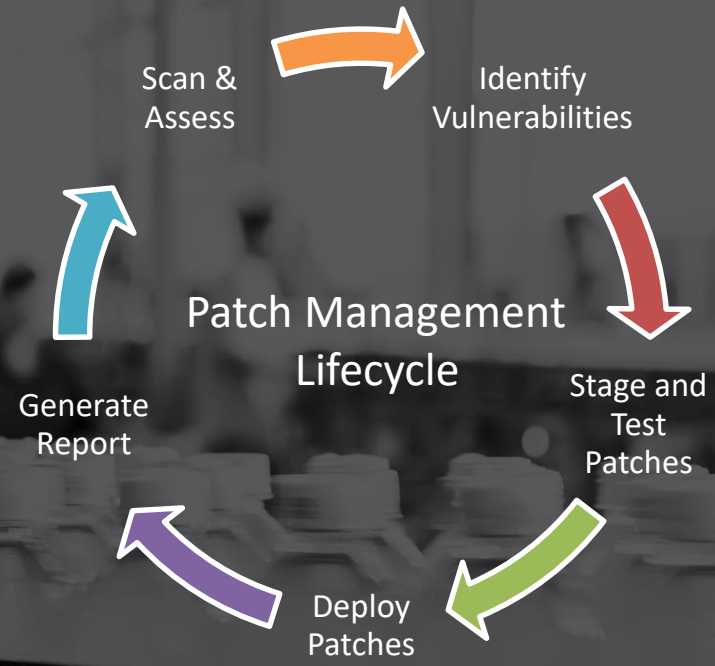
Production or Patching?

Mature companies choose both.



GRANTEK

August 3rd, 2017

Chris Hamilton
Director, Industrial IT/OT and Cyber Security

Agenda

- Introduction – Chris Hamilton
- Introduction – Grantek Systems Integration
  - Limited in presentation: More detail available in emailed deck
- Threats – Then and Now
  - Deep Dive – WannaCry and NotPetya
- ICS Network Design
  - ISA95 Levels / CPwE
  - Secure Vendor Remote Access
- Patching and OS Lifecycle Management
- What's really out there today?
  - How does this relate to Manufacturing and Critical Industry?
  - Why is all this such a concern to me?
- Do you know what's on your network, and what can you do to find out?

Reminder: Email questions to the address in the top bar

Introduction

Chris Hamilton
Director, Industrial IT and Cyber Security
Grantek Systems Integration

Business vCard:
https://inigoapp.com/m/public/profile/BA474E2155530713FFCC3E4A74A5A283?sh=1459781285

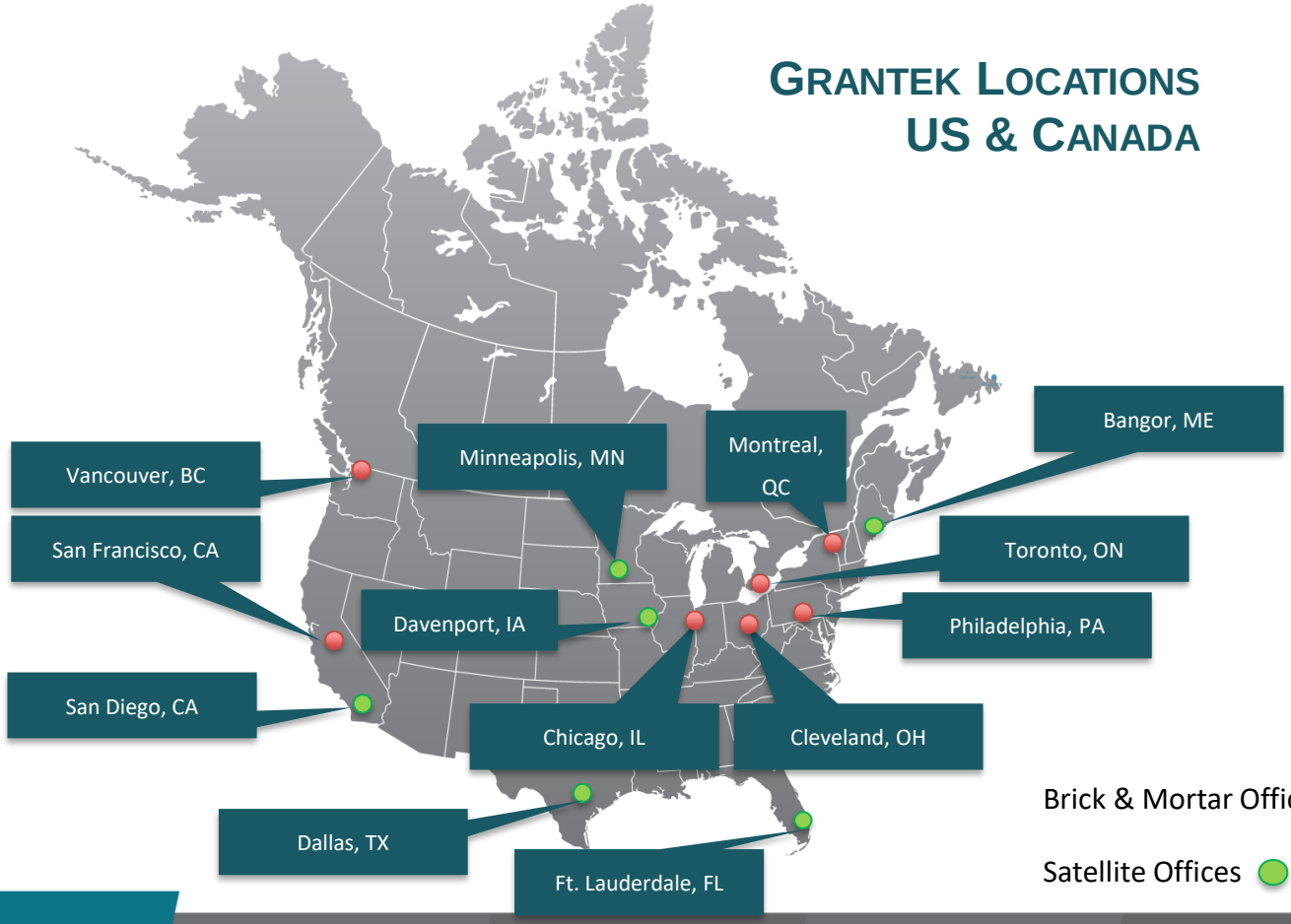
- 10+ years in Controls and Automation
- 15 years in IT systems architecture and cyber security
- MESA Cyber-Security Co-Chair
- Consulting – Bridging the *political* IT / OT gap
- Technical Experience:
  - Network Design and Cyber Security
  - IIoT - Technology Enablement
  - Virtualization and Hyperconvergence
  - Applications and Dataflow Security – in motion and at rest
  - ISA-95 “Shop Floor to Top Floor” OSA

Introduction – Grantek Systems Integration

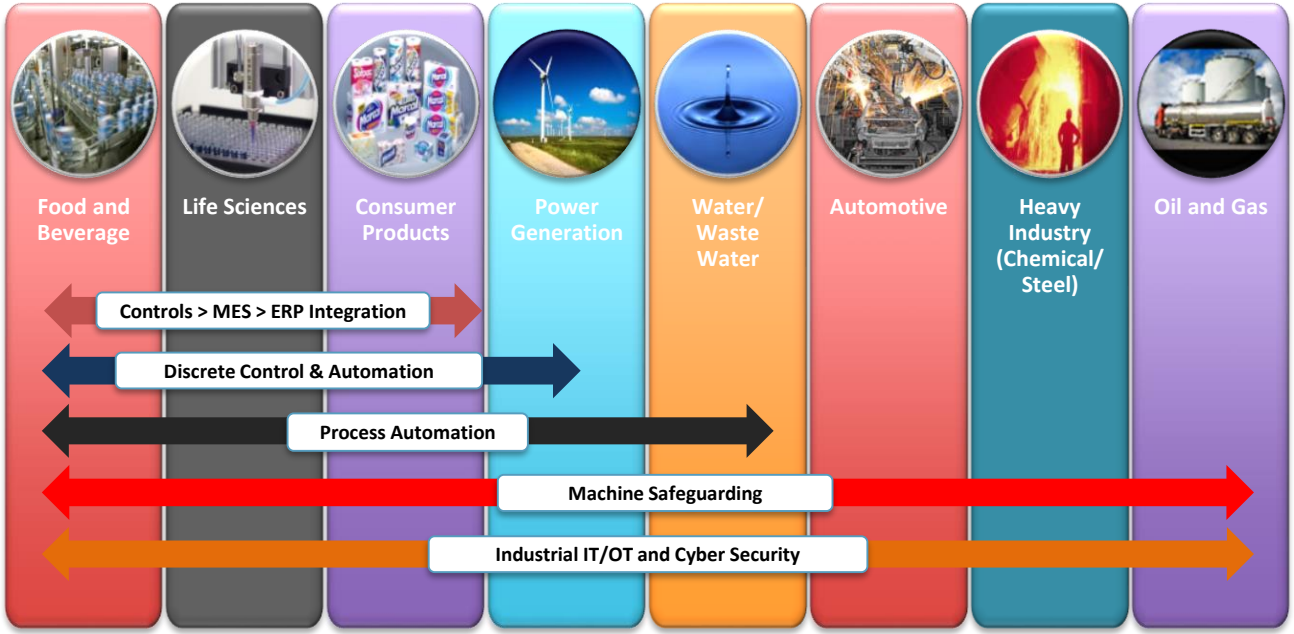
- System Integrator & Business Solution Provider
- Over 35 years experience
- Strong North American presence
- Over 200 employees
- From the plant floor to the boardroom

GRANTEK

GRANTEK LOCATIONS US & CANADA



Industries Served



Strategic Partnerships

MESA INTERNATIONAL
GOLD KEYSTONE SPONSOR

inductive automation
CERTIFIED PREMIER INTEGRATOR

sepasoft
CERTIFIED PREMIER INTEGRATOR

Rockwell Automation
Solution Partner
Enterprise
Machine Safety
Process
Control
Information
Industrial IT

SAP

OSIsoft.

COGNEX
AUTOMATION SOLUTION PROVIDER
ASP

SICK

ABB Robotics
Partner

CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL
CISSP

CISCO PARTNER
Registered

vmware PARTNER
PROFESSIONAL SOLUTION PROVIDER

PANDUIT
Business Partner

GRANTEK

CPG | Food | Beverage | Life Sciences & Pharma | Energy & Renewable Energy

Grantek Strategic Initiatives

To enable Grantek to succeed by providing thought leadership, strategic guidance and technological enablement.

Smart Manufacturing

Enabling Operational Excellence via Digital Integration

- *MES / ERP*
- *Operational Management (ISA95)*
- *Compliance (Quality, FSMA, Serialization)*

Safety

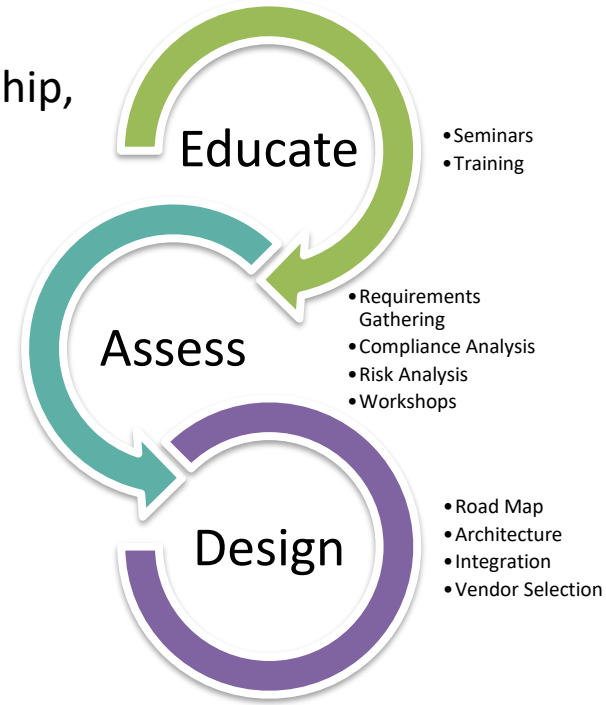
Increasing Productivity Through Smart Safety Solutions

- *Machine Safety*
- *Corporate Safety*
- *Risk Management*

Industrial IT/OT & Cyber Security

Providing the Foundation for Manufacturing Connectivity, Availability and Security

- *Cyber Security*
- *IIoT (Industrial Internet of Things)*
- *Physical Infrastructure Assessment*
- *Network ICS/Cyber-Physical Systems*

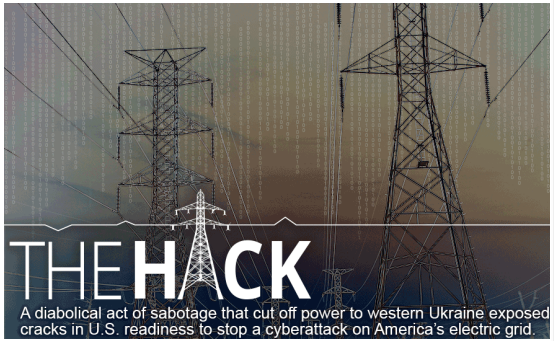


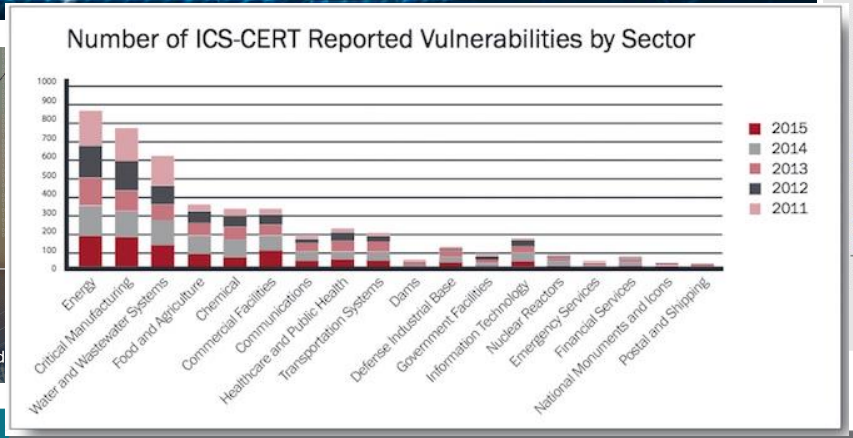
Agenda

- Introduction – Chris Hamilton
- Introduction – Grantek Systems Integration
  - Limited in presentation: More detail available in emailed deck
- Threats – Then and Now
  - Deep Dive – WannaCry and NotPetya
- ICS Network Design
  - ISA95 Levels / CPwE
  - Secure Vendor Remote Access
- Patching and OS Lifecycle Management
- What's really out there today?
  - How does this relate to Manufacturing and Critical Industry?
  - Why is all this such a concern to me?
- Do you know what's on your network, and what can you do to find out?

Threats - Then and Now

Manufacturing has changed; it has evolved.






May / June 2015

Homeland Security

ICS-CERT MONITOR

Contents

Incident Response Activity
Onsite Assessment Summary
Situational Awareness
ICS-CERT News
Recent Product Releases
Open Source Situational Awareness Highlights
Coordinated Vulnerability Disclosure
Upcoming Events

National Cybersecurity and Communications Integration Center

Incident Response Activity

Notable Incident

In the course of incident response and assessments, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) works with organizations that often lack adequate security measures, best practices/policies, documentation, and personnel. Cybersecurity can be a difficult proposition for the critical infrastructure community, and it is not the position of ICS-CERT to regulate or criticize the shortcomings of any organizations. Instead, ICS-CERT provides guidance and support to organizations in the form of assessment services and tools, subject matter expertise and analytic support, no-cost training, and other resources for use in strengthening cybersecurity against today's threats. Our mission is to assist critical infrastructure asset owners in reducing the risk of cyber attacks. The below incident scenario details an example of our onsite assistance for an organization dealing with a cyber intrusion. The writeup is intended to provide insight into some common deficiencies that exist across many organizations today. ICS-CERT encourages organizations to make cybersecurity a priority and not wait until a significant incident has occurred.

A critical infrastructure asset owner recently engaged the ICS-CERT to evaluate the organization's control systems environment for possible advanced persistent threat (APT) activity. It had been discovered during previous incident response efforts that the bridge between the corporate and processing network had been compromised. Concerned about the integrity of the processing environment, the asset owner requested ICS-CERT support to analyze the systems for possible adversary activity and then, secondarily, evaluate the overall security posture.

Industry Breaches - 2012

- *The Saudi Aramco Breach (August 2012)*
  - Malware partially wiped or totally destroyed the hard drives of **35,000** Aramco computers
  - IT Response: Quickly disconnect its systems (physically) from each other and the internet
  - Financial and business systems went down (nobody got paid)
  - Independent legacy oil manufacturing systems continued to function
  - What happens when these manufacturing systems are ***connected?***

The Old World: Islands of Automation

Imagine the modern office, and then turn everything off, Kubecka said. "No emails, no phones, nothing," she said. While oil production—drilling and pumping—remained unaffected because those were automated, the rest of the business went old-school. Everything was on paper, whether it was managing supplies, tracking shipment, or handling contracts with partners and governments. Employees used typewriters and fax machines. The IT staff had to figure out where to go to buy the fax machines, she said.

Rashid, Fahmida Y. "Inside The Aftermath Of The Saudi Aramco Breach." Dark Reading. N.p., n.d. Web. 28 Jan. 2016.

Industry Breaches - 2014

- Why Should You Care?
  - Amidst the growing and changing attacks on the cyber front, many of the fundamentals have not changed.
  - It is still true that most exploited vulnerabilities – 99% in fact, according to Verizon's 2015 DIBR (Data Breach Investigations Report) -- **came over a year after that exploit had been discovered and patched.**
  - The importance of patching will continue to be critical to a secure infrastructure.

In 2014…

99.9%
OF THE EXPLOITED VULNERABILITIES WERE COMPROMISED MORE THAN A YEAR AFTER THE CVE WAS PUBLISHED.

"2015 Data Breach Investigations Report (DBIR)." Verizon Enterprise Solutions. N.p., n.d. Web. 28 Jan. 2016.

Industry Reports - 2016

Verizon DBIR

Number of breaches per threat action category over time

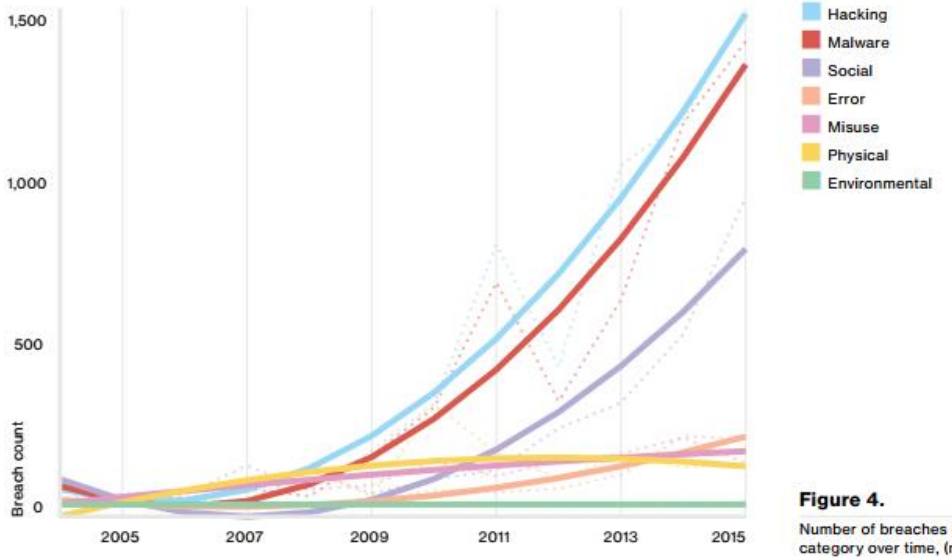
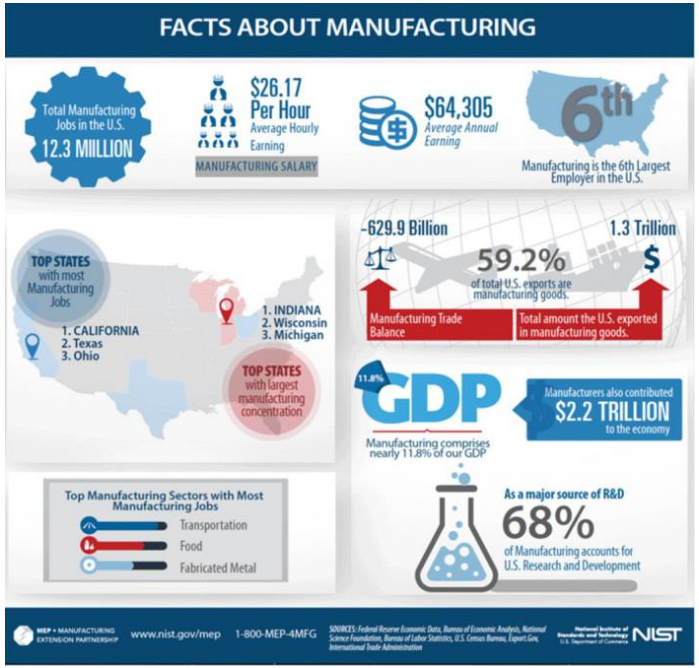


Figure 4.
Number of breaches per threat action category over time, (n=9,009)

2016 Data Breach Investigations Report

89% of breaches had a financial or espionage motive.

National Institute of Standards and Technology



- The Cybersecurity Framework was published in February 2014 following a collaborative process involving industry, academia and government agencies, as directed by a presidential executive order
  - January 2017 update
  - Regulation to be added to all critical infrastructure sectors
  - Manufacturing expected to follow suite

https://www.nist.gov/mep/cybersecurity-resources-manufacturers

Cybersecurity Strengthens U.S. Manufacturers

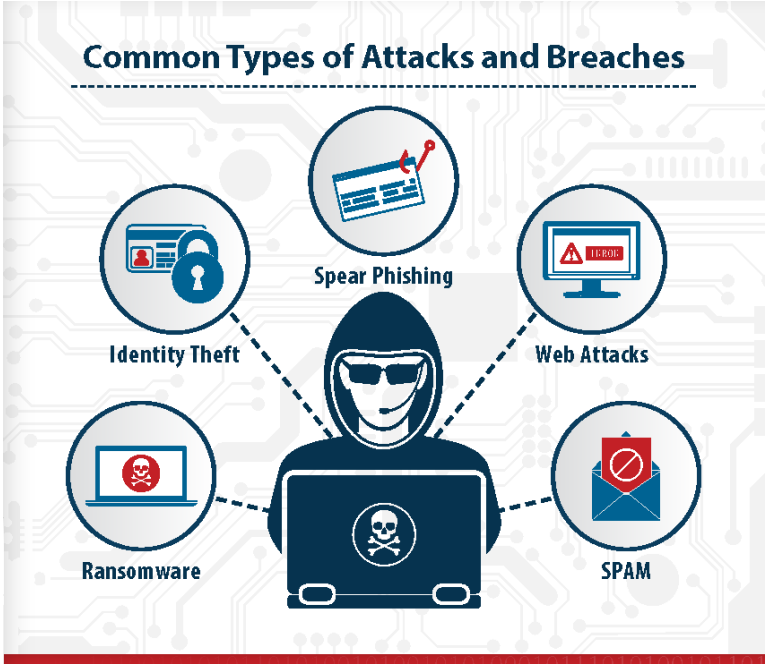
Reality of Cyberattacks and Breaches

55% of small and mid-sized business have experienced a data breach or cyberattack.

43% of all spear-phishing attacks are targeted at small businesses.

60% of impacted businesses are left severely impaired.

$38K is the average cost for a small business to overcome a data breach.



https://www.nist.gov/mep/cybersecurity-resources-manufacturers

Cybersecurity Strengthens U.S. Manufacturers

Defense Suppliers: Compliance

Manufacturers in the DoD supply chain have until **December 31, 2017** to be in compliance with new DFAR cybersecurity requirements.

Learn more at **nist.gov/mep/cybersecurity**

Enhance Your Cybersecurity

Whether you're a manufacturer implementing a cybersecurity program, or a DoD supplier looking to achieve compliance, the MEP National Network can help you with your cybersecurity needs.

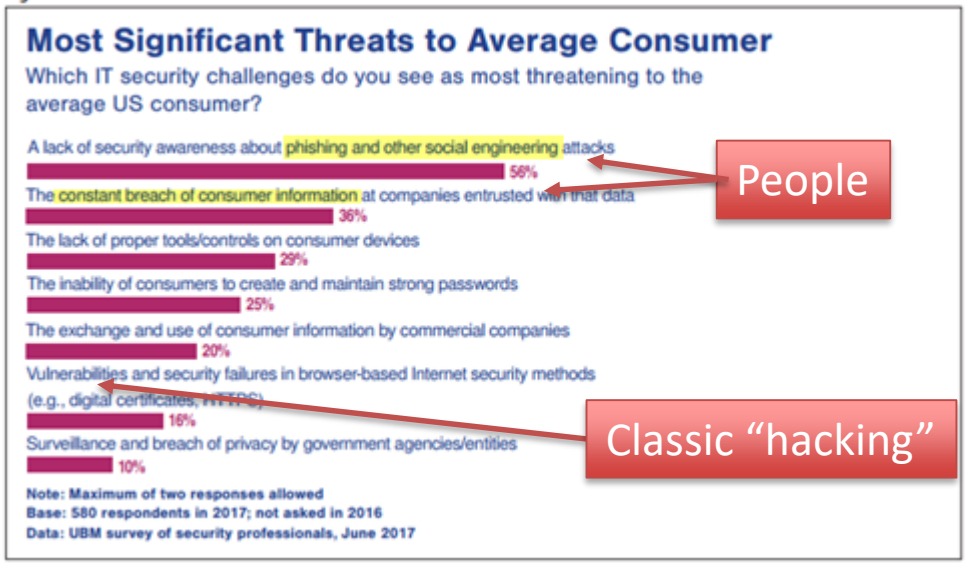
Contact your local MEP Center or learn more at **nist.gov/mep/cybersecurity**

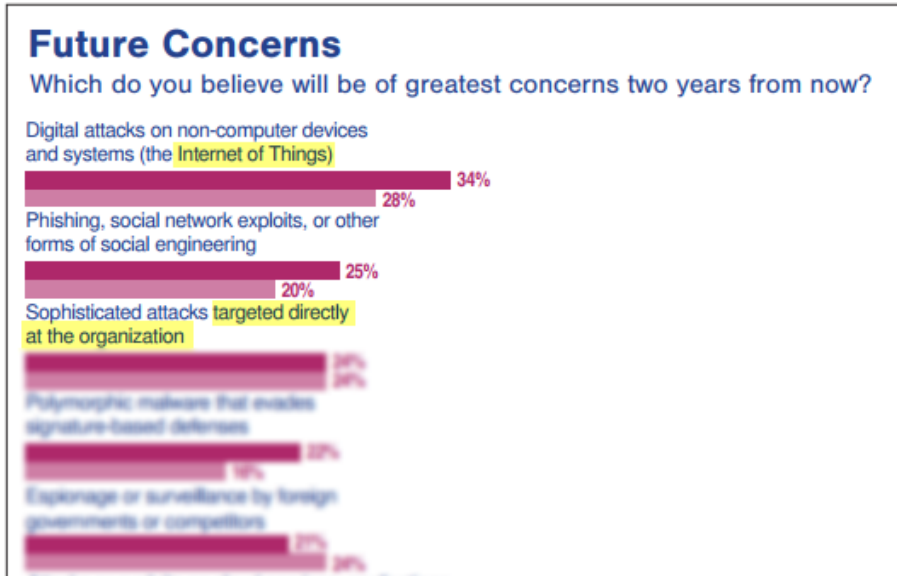
https://www.nist.gov/mep/cybersecurity-resources-manufacturers


JULY 22-27, 2017
MANDALAY BAY / LAS VEGAS, NV
WWW.BLACKHAT.COM #BHUSA
black hat
USA 2017
www.blackhat.com
July 2017
2017 Black Hat Attendee Survey
Portrait of an Imminent Cyberthreat
Cyber attacks on US enterprises and critical infrastructure are coming soon, according to some of the industry's most experienced and highly informed security professionals. And in most cases, defenders are not prepared.

Black Hat - 2017

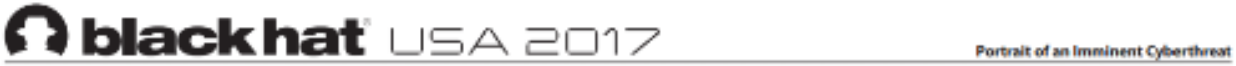
Figure 13





blackhat USA 2017

Black Hat - 2017



Most information security professionals believe that the US critical infrastructure will be breached by a cyber attack within the next two years. Most also believe that their own enterprises will be breached in the next 12 months. And most believe that the defenders of those infrastructures are not ready to respond.

July 2017

Agenda

- Introduction – Chris Hamilton
- Introduction – Grantek Systems Integration
  - Limited in presentation: More detail available in emailed deck
- Threats – Then and Now
  - Deep Dive – WannaCry and NotPetya
- ICS Network Design
  - ISA95 Levels / CPwE
  - Secure Vendor Remote Access
- Patching and OS Lifecycle Management
- What's really out there today?
  - How does this relate to Manufacturing and Critical Industry?
  - Why is all this such a concern to me?
- Do you know what's on your network, and what can you do to find out?

Reminder: Email questions to the address in the top bar

Recent cyber threats: WannaCry

- Who was affected?
  - Infected an estimated 300,000 computers worldwide in a weekend (Avast)
- How did it spread?
  - Primarily over the open internet
  - SMBv1 EternalBlue exploit attributed to the NSA. Patched by Microsoft March 14th, 2017

Recent cyber threats: WannaCry

- What stopped it?
  - A security researcher inadvertently found the “kill switch”
  - Microsoft released an unprecedented patch for Windows XP to curb the spread.
  - *Note: Systems unable to reach the “kill switch” domain name continued unencumbered.*
- How did victims recover?
  - Restore from backup, or rebuild
- What could have prevented it?
  - **PATCHING**. A patch for the exploit was released 2 months before WannaCry was seen in the wild.

Recent cyber threats: WannaCry

David Zahn, GM of the PAS Cybersecurity Business Unit explained for IIoT World: “For the longest time, facilities have trusted security controls like security by obscurity, system complexity, air gapping, and perimeter-based cybersecurity to protect ICS. WannaCry is another example of how these safeguards are not sufficient. Companies that rely upon industrial control systems (ICS) to operate need to implement solutions that help answer simple cybersecurity questions such as what are my cyber assets, where do I have vulnerabilities, has an unauthorized change occurred, can I recover quickly if a system is compromised, and more. Sadly, these are hard questions to answer as industrial process companies have limited visibility into nearly 80% of the cyber assets in an industrial process facility.”

https://grantek.com/wannacry-ransomware-cryptoworm-what-it-means-to-the-industrial-world/

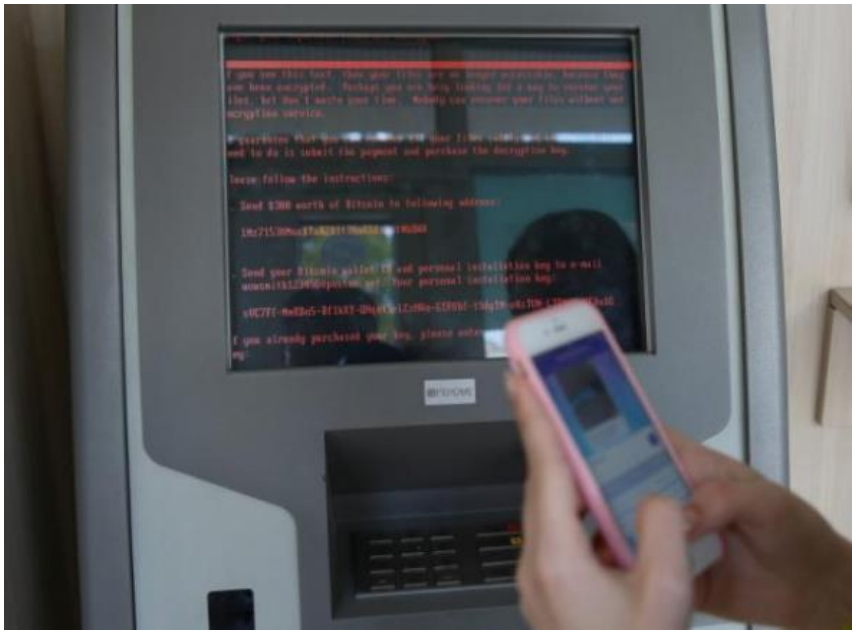
NotPetya – June 27, 2017

aka SortaPetya, Petna, ExPetr, GoldenEye, Nyetya, Diskcoder.C

Who was affected?

- First identified in Ukraine, quickly spread to major European firms
- Infected ~300,000 systems in <24hours

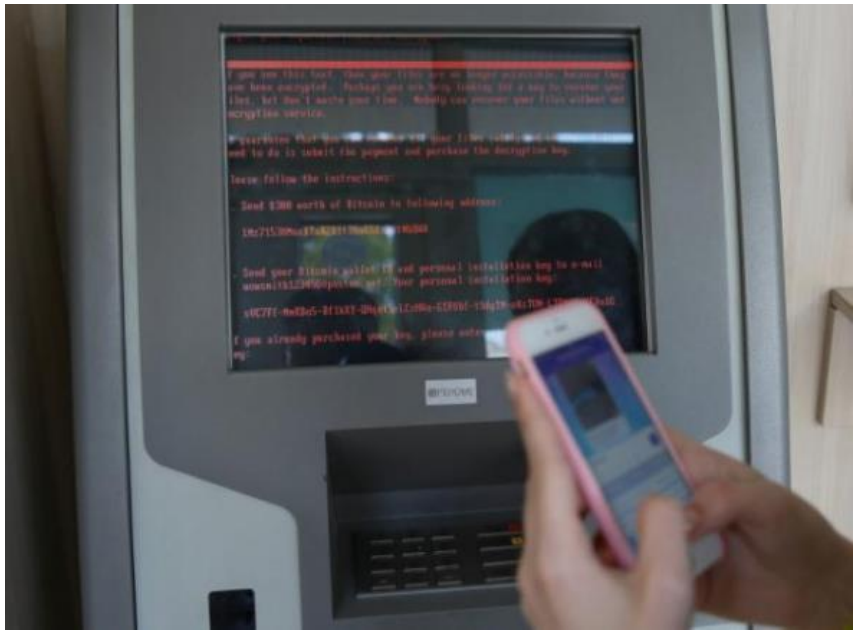
- How did it spread?
  - Very sophisticated use of multiple security tools and exploits
  - Release into the wild
    - Largely unknown
    - Ukrainian accounting software MeDoc implicated
  - Lateral movement
    - SMBv1 exploit: EternalBlue was patched in MS17-010 on March 14th
    - Mimikatz: Targeted IT systems by stealing cached Remote Desktop credentials - *NOT patchable*. Detectable by Anti Virus



NotPetya – June 27, 2017

aka SortaPetya, Petna, ExPetr, GoldenEye, Nyetya, Diskcoder.C

- What stopped it?
  - System isolation and network IPS/IDS
  - Patching and Antivirus updates
  - Intense effort and hours of time invested by IT and engineering teams
- How did victims recover?
  - Restore from backup, or rebuild
- What could have prevented it?
  - Reactive: ICS-CERT on the next slide
  - Proactive: **Increased ICS maturity and cyber-stewardship culture**



NotPetya – June 27, 2017

aka SortaPetya, Petna, ExPetr, GoldenEye, Nyetya, Diskcoder.C

MITIGATION

ICS-CERT recommends that users take defensive measures to minimize the risk associated with the Petya malware. Specifically, users should consider the following:

- Apply the Microsoft patch, MS17-010.
- Disable SMBv1 on every system connected to the network. Information on how to disable SMBv1 is available from Microsoft(link is external). While many modern devices will operate correctly without SMBv1, some older devices may experience communication or file/device access disruptions.
- Microsoft recommends(link is external) blocking all traffic on Port 139/TCP and 445/TCP to prevent propagation. Microsoft has also recommends that their users can also disable remote WMI and file sharing.
- Review network traffic to confirm that there is no unexpected SMBv1 network traffic. The following links provide information and tools for detecting SMBv1 network traffic and Microsoft's MS17-010 patch:
  - SMB—Audit Active Usage using Message Analyzer(link is external)
  - Wireshark download
  - MS17-010 SMB RCE Detection(link is external).
- Isolate or protect vulnerable embedded systems that cannot be patched from potential network exploitation.
- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks and devices behind firewalls, and isolate them from the business network.

https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-181-01C

NotPetya – June 27, 2017

aka SortaPetya, Petna, ExPetr, GoldenEye, Nyetya, Diskcoder.C

MITIGATION

ICS-CERT recommends that users take defensive measures to minimize the risk ass d w the t ware. Specifically, users should consider the following:

- Apply the Microsoft patch, MS17-010.
- Disable SMBv1 on every system connected to the n rk. rm on h to able SMBv1 is available from Microsoft(link is external). While many modern devices will oper e c ectly w ou MBv1 ome older devices may experience communication or file/device access disruptions.
- Microsoft recommends(link is ernal) cking all traf on Po 139/TCP and 445/TCP to prevent propagation. Microsoft has also recommends that their users so d ble remote W and file sharing.
- Review network ic to con h th her nexpected SMBv1 network traffic. The following links provide information and tools for detecting Bv1 iwa traf rosoft's MS17-010 patch:
  - MB- udi tive Us e using Message Analyzer(link is external)
  - k do
  - M 7-0 SMB RCE Detection(link is external).
- Isolate or otect vulnerable embedded systems that cannot be patched from potential network exploitation.
- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks and devices behind firewalls, and isolate them from the business network.

https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-181-01C

REACTIONARY

NotPetya – June 27, 2017

aka SortaPetya, Petna, ExPetr, GoldenEye, Nyetya, Diskcoder.C

NotPetya is a **cyberweapon**, not ransomware

- Encrypted files not considered recoverable
- Execution of attack was not intended to make money
- Because DeOS attacks destroy all data, a definitive post-mortem analysis is not likely

NotPetya – June 27, 2017

aka SortaPetya, Petna, ExPetr, GoldenEye, Nyetya, Diskcoder.C

- What can prevent ***the next*** one?
  - A mature patch management policy
    - Managed, tested, applied!
  - Mature OS and Software lifecycle management
    - Windows Server 2003
  - Account management / access policies
    - Disallow saving of credentials
    - Block reuse of passwords across systems
  - Disable unused services
    - Disable SMBv1
    - Disable remote execution in environments where it is not needed
  - Antivirus with updates!
    - Within hours the major AV companies had released updates capable of detecting and **stopping** the execution of NotPetya.

NotPetya – Financial Ramifications

aka SortaPetya, Petna, ExPetr, GoldenEye, Nyetya, Diskcoder.C

- Nuance says it expected its revenue for the third quarter will be in the $494 million to $498 million range, down from the original expectation of $509 million to $513 million.
- "Not Petya signaled a new paradigm shift as attackers are willing to launch attacks specifically to disrupt and destroy IT assets and data," says Mac McMillan, president of the security consultancy Cynergistek

http://www.bankinfosecurity.com/nuance-latest-notpetya-victim-to-report-financial-impact-a-10138

NotPetya – Financial Ramifications

NotPetya impact detailed in SEC 10-K filing

In its annual 10-K filing with the US SEC (Securities and Exchange Commission), FedEx says no data was stolen from its or TNT's network, but "TNT operations and communications were significantly affected."

FedEx says it restored IT systems and services right after the incident, but "customers are still experiencing widespread service and invoicing delays," nearly three weeks after NotPetya hit its network.

"We cannot yet estimate how long it will take to restore the systems that were impacted, and it is reasonably possible that TNT will be **unable to fully restore all of the affected systems and recover all of the critical business data** that was encrypted by the virus," FedEx wrote in its 10-K filing.

FedEx has disclosed the following costs and damages:

- loss of revenue resulting from the **operational disruption** immediately following the cyber-attack;
- loss of revenue or increased bad debt expense due to the **inability to invoice** properly;
- loss of revenue due to **permanent customer loss**;
- remediation costs to restore systems;
- increased operational costs due to contingency plans that remain in place;
- investments in enhanced systems in order to prevent future attacks;
- cost of incentives offered to customers to restore confidence and maintain business relationships;
- **reputational damage** resulting in the failure to retain or attract customers;
- costs associated with potential **litigation** or **governmental investigations**;
- costs associated with any data breach or data loss to third parties that is discovered;
- costs associated with the potential **loss of critical business data**;
- longer and more costly integration (due to increased expenses and capital spending requirements) of TNT Express and FedEx Express; and
- other consequences of which we are not currently aware but will discover through the remediation process.

https://www.bleepingcomputer.com/news/security/fedex-says-some-damage-from-notpetya-ransomware-may-be-permanent/

NotPetya – Financial Ramifications

In June 2017, TNT Express **worldwide operations were significantly affected** due to the infiltration of an information technology virus known as Petya. For further information about the cyber-attack, see the section titled "TNT Express Cyber-Attack" included in Item 7 of this Annual Report on Form 10-K ("Management's Discussion and Analysis of Results of Operations and Financial Condition").

Our information technology teams have been focused on the recovery of critical systems and continue to make progress in resuming full services and restoring critical systems. Currently, we are focused on **restoring remaining operational systems as well as finance, back-office and secondary business systems**. At this time, we **cannot estimate how long** it will take to restore the systems that were impacted and it is reasonably possible that TNT Express will be **unable to fully restore** all of the affected systems and recover all of the critical business data that was encrypted by the virus.

Given the recent timing and magnitude of the attack, in addition to our initial focus on restoring TNT Express operations and customer service functions, we are still evaluating the financial impact of the attack, but it is likely that it will be material. **We do not have cyber or other insurance** in place that covers this attack. Although we cannot currently quantify the amounts, we have experienced loss of revenue due to decreased volumes at TNT Express and incremental costs associated with the implementation of contingency plans and the remediation of affected systems. Additional consequences and risks associated with the cyber-attack that could negatively impact our results of operations and financial condition are described in the corresponding risk factor included in this MD&A. In addition to financial consequences, the **cyber-attack may materially impact our disclosure controls and procedures and internal control over financial reporting** in future periods.

NotPetya – Financial Ramifications

DEERFIELD, III., July 6, 2017 – Mondelēz International today provided an update to its prior disclosure on the June 27th global cyber-attack that impacted our business.

We are pleased that we are making good progress in restoring our systems across the enterprise. Since the time of the incident, our teams have done remarkable work to continue to operate the business, manufacture our products, serve customer needs and progress the recovery activities. We believe the issue has been contained and a critical majority of the affected systems are up and running again.

Given the timing of this significant global attack, despite our best efforts, we experienced **disruption in our ability to ship and invoice** during the last four days of our second quarter. There are a few markets where we have permanently lost some of that revenue due to holiday feature timing, but we expect we will be able to recognize the majority of these delayed shipments in our third quarter results.

Our preliminary estimate of the **revenue impact of this event is a negative 300 basis points on our second quarter growth** rate.

We are still assessing the full financial impact of this event, in addition to performing our normal quarter-end financial close process. Based on our current assessment of the situation, our recovery progress, and the underlying trends in our business, we are reaffirming our full- year organic revenue growth outlook of "at least 1 percent growth". We expect to incur incremental one-time costs in both our second and third quarters as a result of this issue, but our underlying margin progress continues to be in line with our outlook ofmid-16 percent for the full-year.

A further update on these matters, our second quarter results and our full-year outlook will be provided in our second quarter investor earnings call and webcast in August.

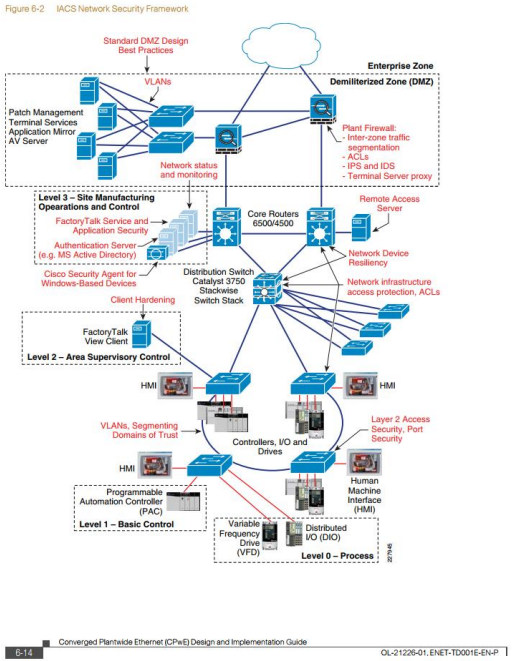
Agenda

- Introduction – Chris Hamilton
- Introduction – Grantek Systems Integration
  - Limited in presentation: More detail available in emailed deck
- Threats – Then and Now
  - Deep Dive – WannaCry and NotPetya
- ICS Network Design
  - ISA95 Levels / CPwE
  - Secure Vendor Remote Access
- Patching and OS Lifecycle Management
- What's really out there today?
  - How does this relate to Manufacturing and Critical Industry?
  - Why is all this such a concern to me?
- Do you know what's on your network, and what can you do to find out?

Secure Network Design - DiD

Risk mitigation: *Defense in Depth*

- Leverage IT-Approved User Access
- Keep ICS Protocols in the Manufacturing zone
- Control Application use (remote and local)
- Protocol Conversion (No direct traffic, common protocols or ports between zones)
- Single path in and out

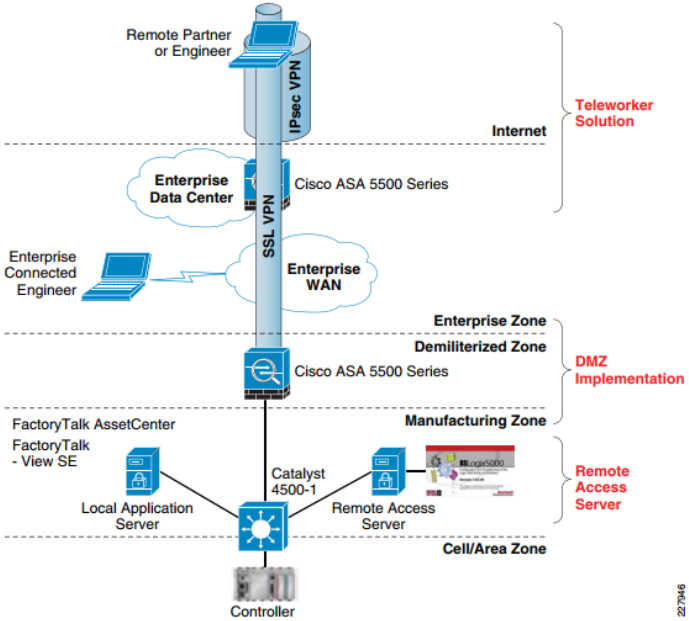


Secure Network Design – Remote Access

Remote Access

- Provide clear alternatives to “roll-your-own” point solutions
  - MANY solutions are shown at trade shows which give the OEM full control (and full risk) over RA
  - These solutions are touted as *convenient* and *secure*
- Provide clear policy to OEMs/Vendors so they understand how to request remote access to your plant
- Review drivers and business risk with PMs and those who interact with 3rd party vendors on projects – increase safety culture

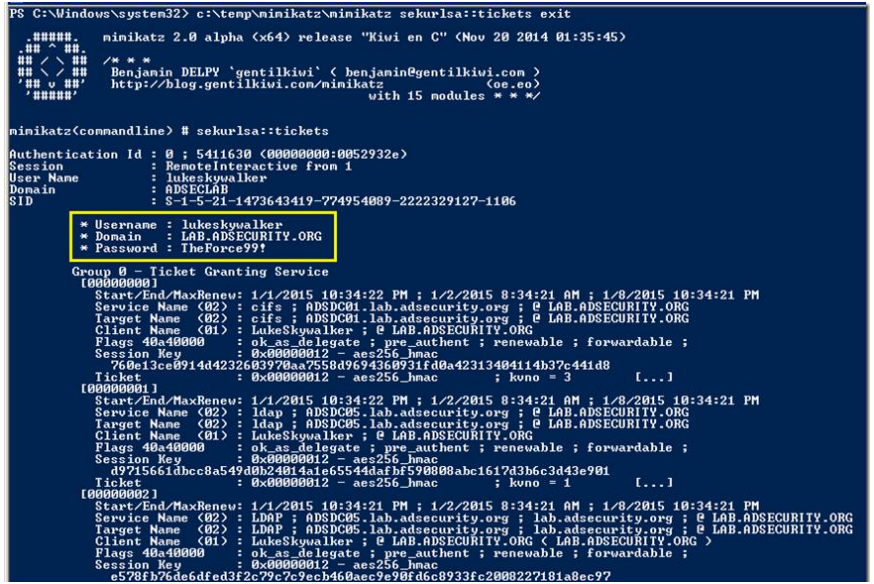
Figure 6-3 Simplified Remote Access



Secure Network Design – Remote Access

Not-Petya point

- Malware stole passwords from the Windows Credential Manager via a modified version of mimikatz (available for free on GitHub)
- It specifically looked for TSCLIENT (remote desktop) and matched the credentials with recent RDP sessions – allowing it to spread across networks

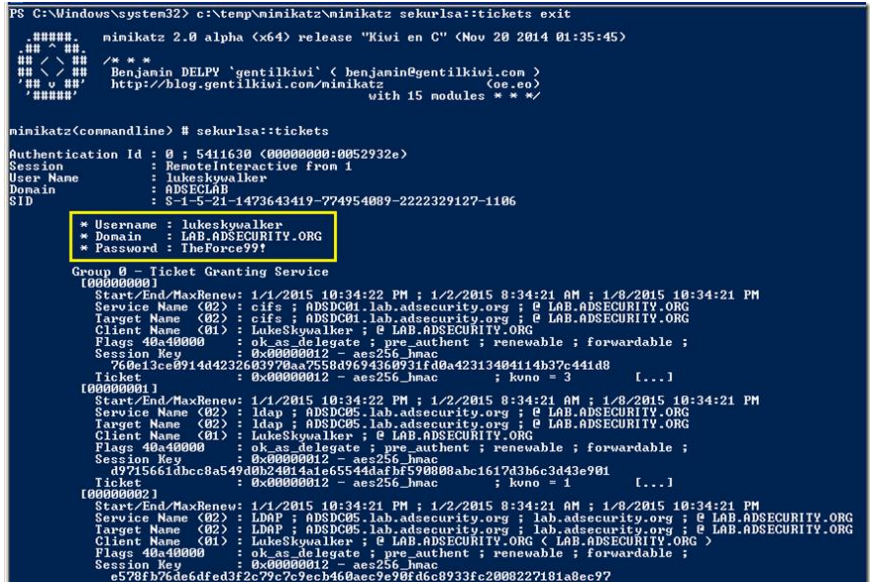


https://adsecurity.org/?page_id=1821

Secure Network Design – Remote Access

Malware Protection

- DO NOT reuse passwords
- DiD – leverage different account names and passwords across zones
- **Most simply: DO NOT save passwords!!**



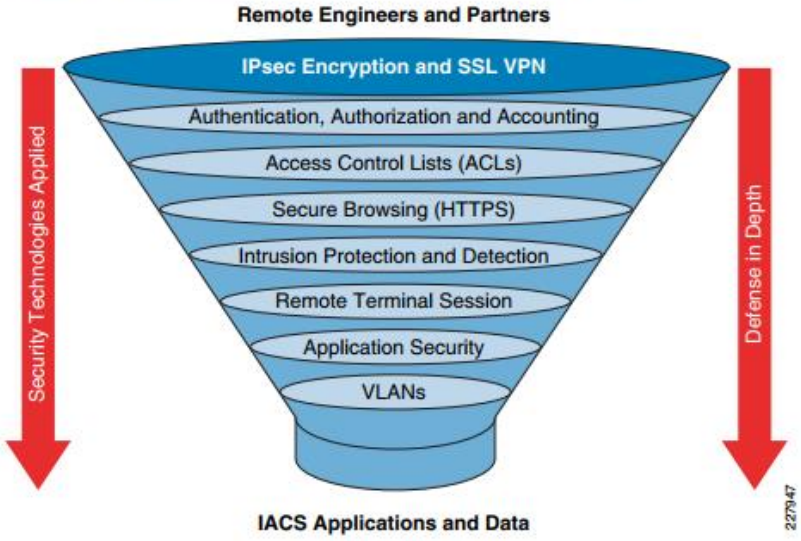
https://adsecurity.org/?page_id=1821

Secure Network Design – Remote Access

How to mitigate risks?

- Leverage IT-Approved User Access
- Keep ICS Protocols in the Manufacturing zone
- Control Application use (remote and local)
- Protocol Conversion (No direct traffic, common protocols or ports between zones)
- Single path in and out

Figure 6-4 Defense-in-Depth Approach for Secure Remote Access



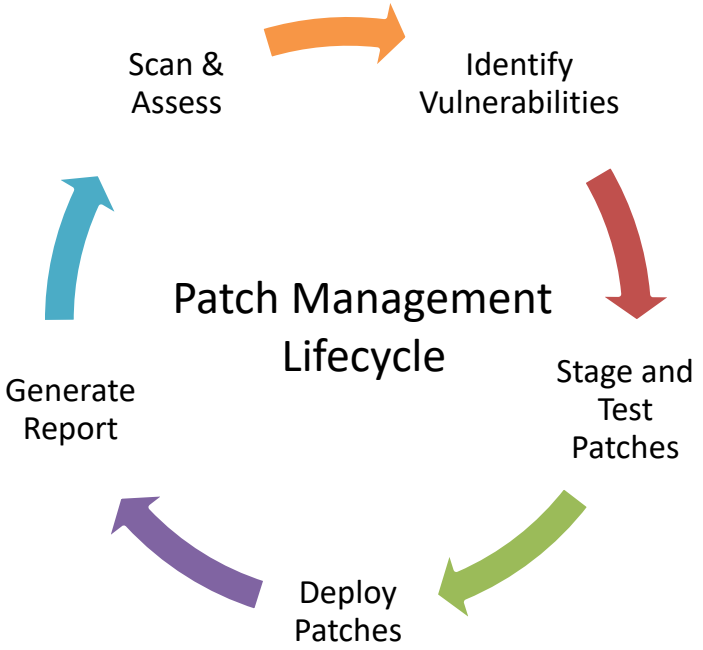
Agenda

- Introduction – Chris Hamilton
- Introduction – Grantek Systems Integration
  - Limited in presentation: More detail available in emailed deck
- Threats – Then and Now
  - Deep Dive – WannaCry and NotPetya
- ICS Network Design
  - ISA95 Levels / CPwE
  - Secure Vendor Remote Access
- Patching and OS Lifecycle Management
- What's really out there today?
  - How does this relate to Manufacturing and Critical Industry?
  - Why is all this such a concern to me?
- Do you know what's on your network, and what can you do to find out?

Patching and LCM

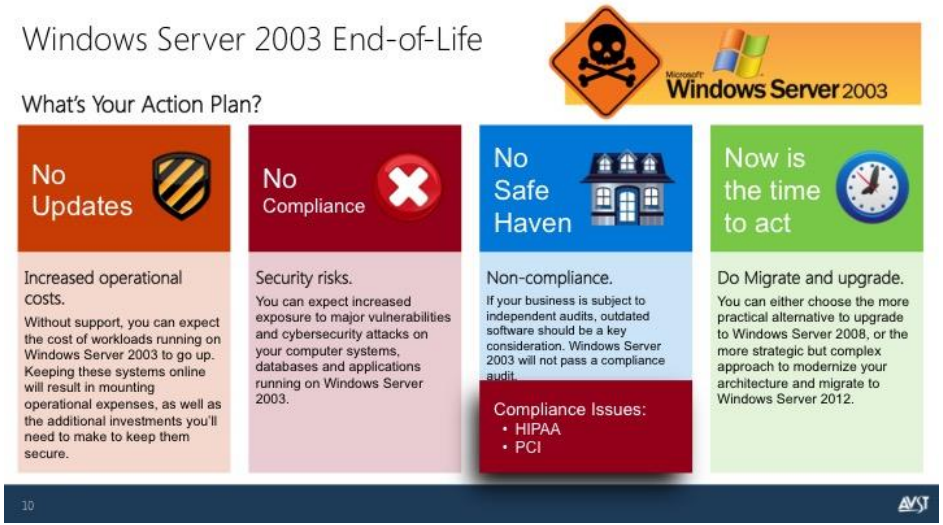
Why manufacturing avoids patching

- Long system life (10-20 years)
- Classically “protected” by limited connectivity
- Immediacy of industry
- Lack of planning
- Lack of system knowledge
- Lack of testing
- Difficulty of scheduling downtime
- Numerous vendors providing different solutions – complex landscape
- Cost of patching / new systems



Patching and LCM

Risks of running EOL Operating Systems



End-Of-Extended-Support Dates:

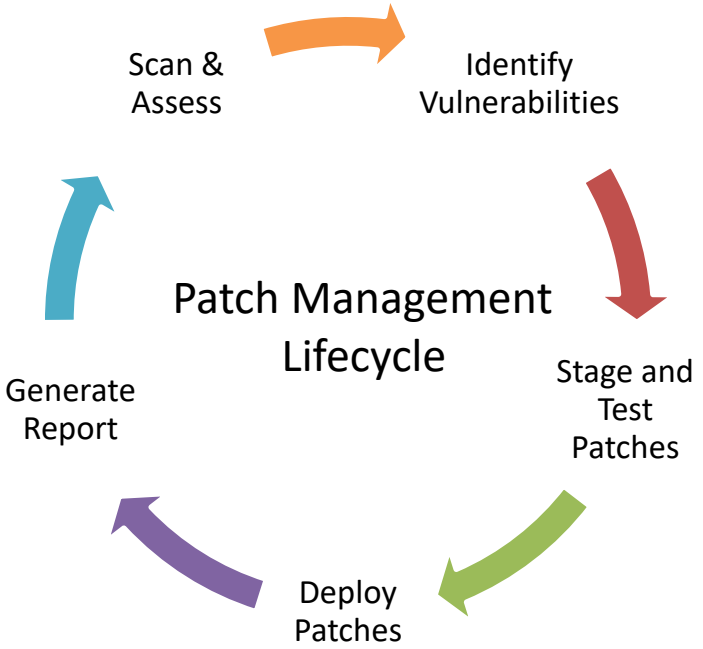
- Windows 2000: July **2010**
- Windows XP: April **2014**
- Windows Server 2003 R2: July **2015**
- Windows 7: January 2020
- Windows Server 2008 R2: January 2020
- Windows Server 2012 October 2023

Patching and LCM

Concern	Resolution
Long system life (10-20 years) Lack of system knowledge Numerous vendors providing different solutions – complex landscape	Solve by: Proper documentation
Immediacy of industry Lack of planning Lack of testing Difficulty of scheduling downtime	Solve by: Proper planning and process
Cost of patching / new systems	Solve by: Proper planning and budget
Classically “protected” by limited connectivity	Not true in today’s connected world

Patching and LCM

- Assess
  - Understand what you have today
  - Audit this against known risks like EOL software/OSs and CVEs
- Design
  - Work within your company and partners to create a management policy for patching
    - Understand risks – Production Downtime, Backups, etc
    - Understand timeline – patching may “lag” behind the enterprise, that is not an excuse for “not doing it” at all
- Implement
  - Proactively schedule patching during maintenance windows on a yearly basis
  - Ensure vendor/internal body tests all patches
  - Ensure backups are viable (restore rehearsal)
  - Ensure rollout is communicated between plant personnel, other vendors and corporate IT

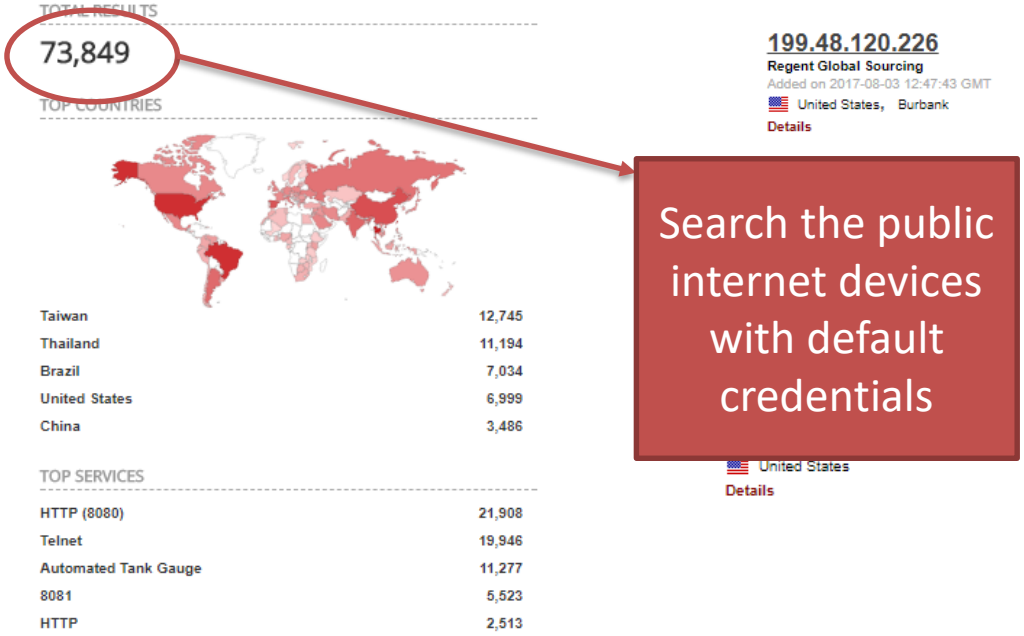


Agenda

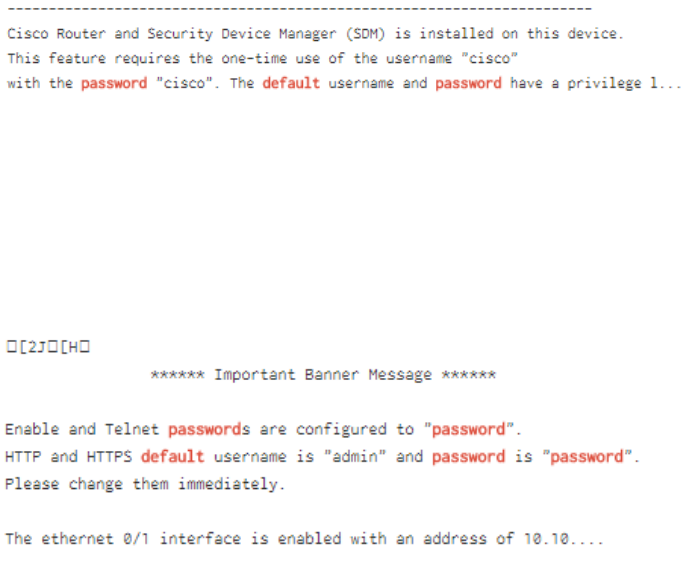
- Introduction – Chris Hamilton
- Introduction – Grantek Systems Integration
  - Limited in presentation: More detail available in emailed deck
- Threats – Then and Now
  - Deep Dive – WannaCry and NotPetya
- ICS Network Design
  - ISA95 Levels / CPwE
  - Secure Vendor Remote Access
- Patching and OS Lifecycle Management
- What's really out there today?
  - How does this relate to Manufacturing and Critical Industry?
  - Why is all this such a concern to me?
- Do you know what's on your network, and what can you do to find out?

Reminder: Email questions to the address in the top bar

What's out there today?



Search the public internet devices with default credentials



What's out there today?

TOTAL RESULTS

5,288

TOP COUNTRIES

United States	3,343
Canada	498
Spain	211
Taiwan, Province of China	121
Australia	117

Rockwell Devices "ENBT"

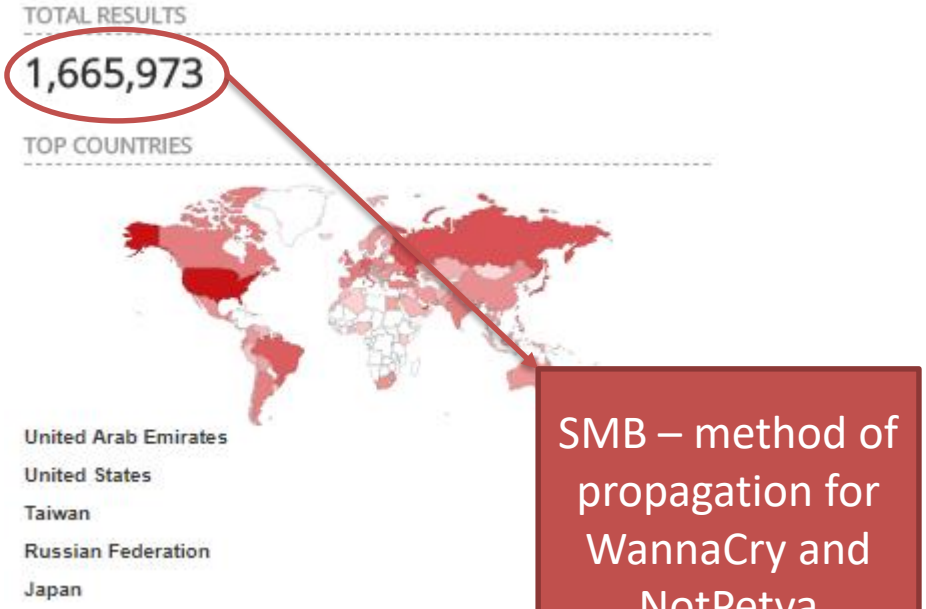
166.155.245.50
50.sub-166-155-245.myvzw.com
Verizon Wireless
Added on 2017-06-01 09:33:07 GMT
United States
Details

```
Product name: 1756-ENBT/A
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x005e8f60
Device type: Communications Adapter
Device IP: 10.174.82.128
```

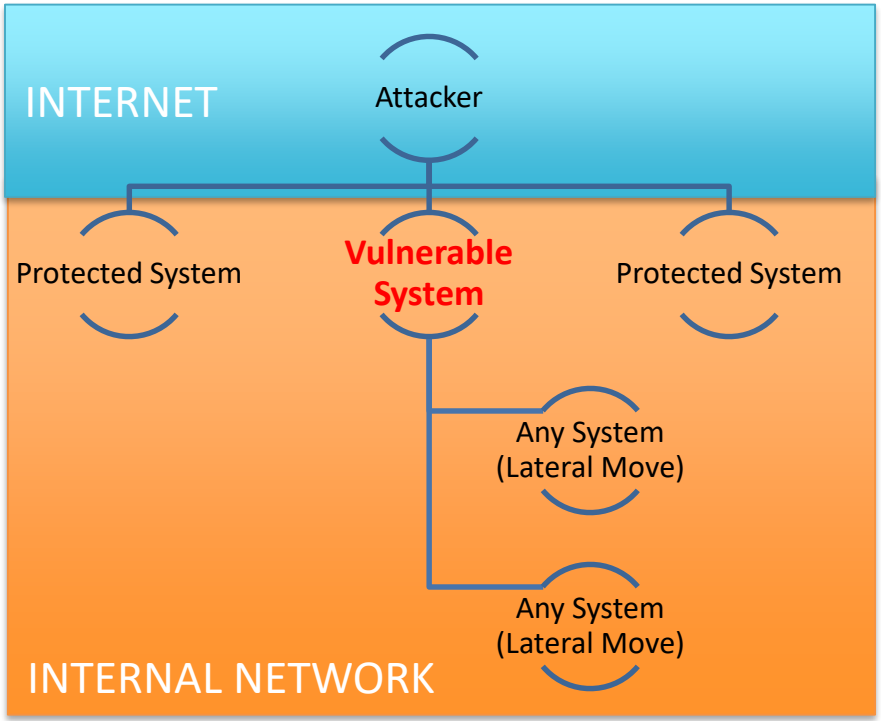
74.198.185.43
Rogers Cable
Added on 2017-06-01 14:51:17 GMT
Canada
Details

```
Product name: 1769-L35E Ethernet Port
Vendor ID: Rockwell Automation/Allen-Bradley
Serial number: 0x4039335d
Device type: Communications Adapter
Device IP: 192.1.1.190
```

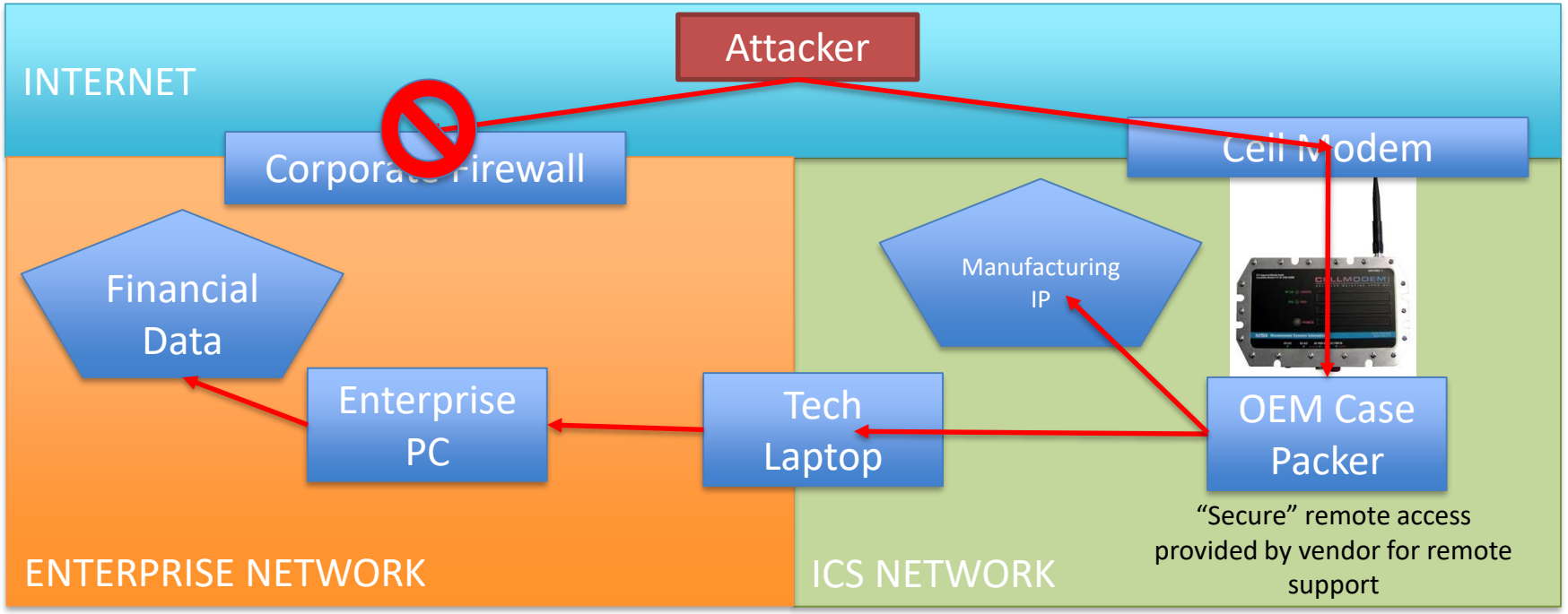
What's out there today?



SMB – method of propagation for WannaCry and NotPetya



Poorly controlled Remote Access



Risk Mitigation

All is not lost!

- Assess: What do you have out there today!? Where are your biggest risks?
- Design: Ensure your systems are securely connected. Including vendors
- Enforce: Implement patching and LCM policies *with* corporate IT and engineering to secure your sites. Budget and understand costs
- BACKUP, backup, backup! (and test)

Don’t be this sad kitten!

What are the global stakes today, you ask?

- A well executed cyber attack could cause damages around the world ranging from $53.1 billion to **$121.4 billion**

- Lloyd's of London

Counting the cost: Cyber exposure decoded

July 17th 2017 Press Release

Superstorm Sandy, the second costliest tropical cyclone on record, is generally considered to have caused economic losses between $50 billion and $70 billion

https://www.lloyds.com/news-and-insight/press-centre/press-releases/2017/07/cyber-attack-report

Agenda

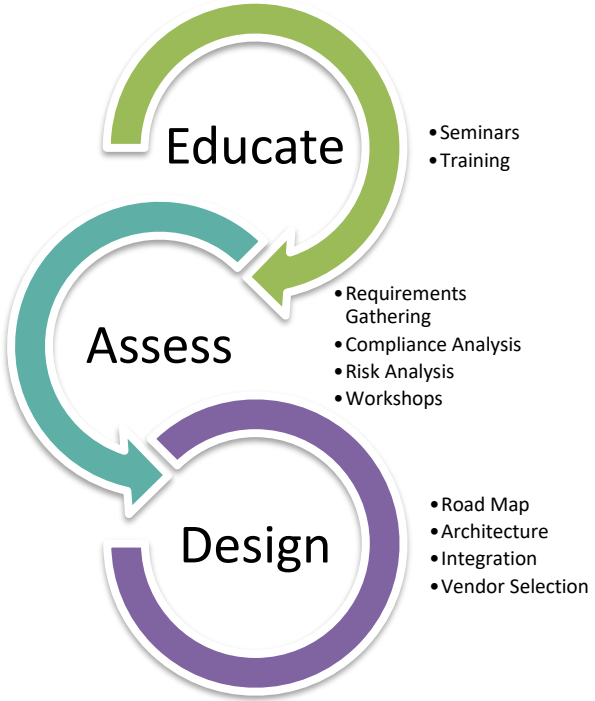
- Introduction – Chris Hamilton
- Introduction – Grantek Systems Integration
  - Limited in presentation: More detail available in emailed deck
- Threats – Then and Now
  - Deep Dive – WannaCry and NotPetya
- ICS Network Design
  - ISA95 Levels / CPwE
  - Secure Vendor Remote Access
- Patching and OS Lifecycle Management
- What's really out there today?
  - How does this relate to Manufacturing and Critical Industry?
  - Why is all this such a concern to me?
- Do you know what's on your network, and what can you do to find out?

Reminder: Email questions to the address in the top bar

Do you know what's on your network?

Phase 1 - Assessments/Audits/Requirements Gathering:

- ICS Network Logical Assessment
- ICS Physical Infrastructure Assessment
- ICS Compute/Virtualization Assessment
- ICS Cyber Security Assessment
- IIOT (Industrial Internet of Things) Readiness Assessment



Do you know what's on your network?

- Selected Assessments
  - ICS Logical Network
  - ICS Physical Infrastructure
  - ICS Compute/Virtualization
- Additional Discussion
  - Controls/SCADA life-cycle
  - Vendor Remote Access
  - Corporate Pi Connectivity

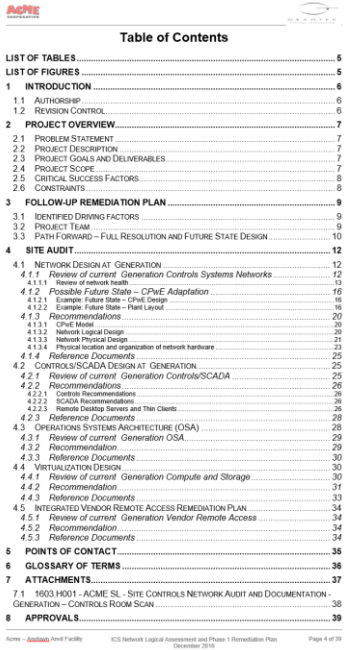
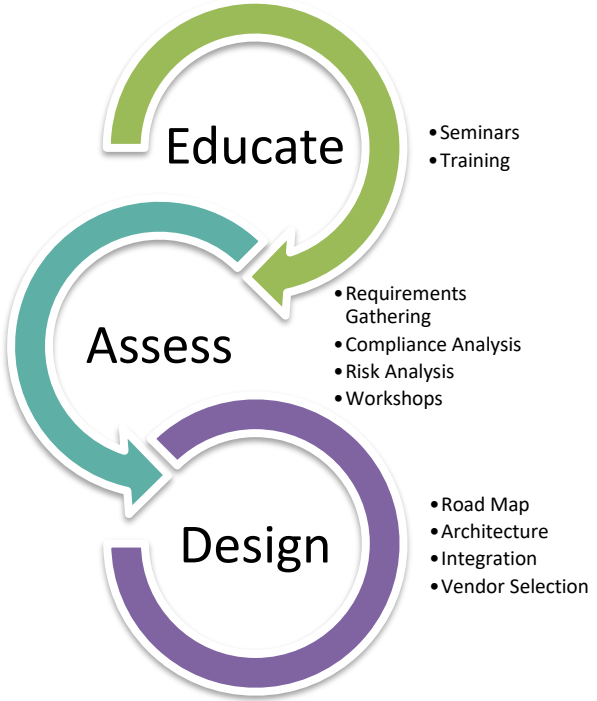
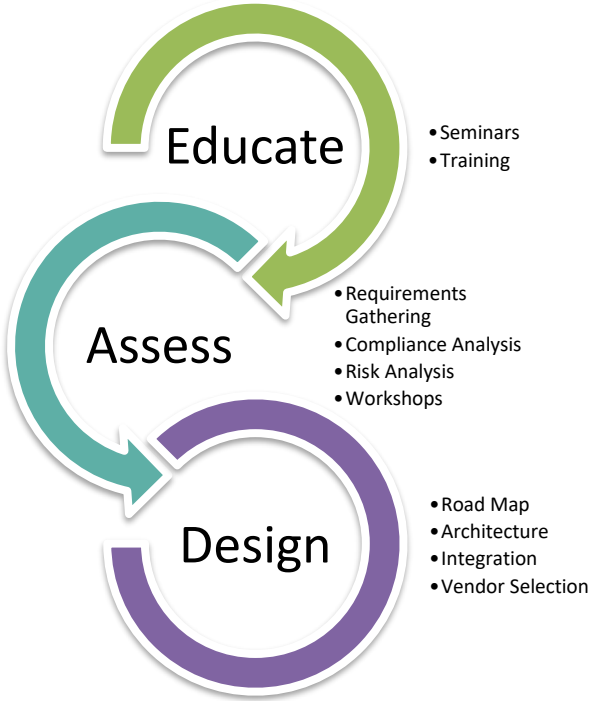


Table of Contents



Thank You!


Educate
•Seminars
•Training
Assess
•Requirements Gathering
•Compliance Analysis
•Risk Analysis
•Workshops
Design
•Road Map
•Architecture
•Integration
•Vendor Selection