Practical Industrial Cyber Security Enhancements

Tues 19th Nov. 2019    30mins  14:30pm - 15:00pm

Cevn@Vibertsolutions.com  www.vibertsolutions.com  +44 (0)7909 992786

linkedin.com/in/vibertprofile  //twitter.com/cevnv
• Consultant

• Best Industrial Cyber Security Consultants 2017/ 2019

• 35+ yrs experience OT/ICS/MES/Physical/Cyber.

• Chartered IT Professional.

• Member IET, ISA, MESA, ISSA, InstMC, BCS, ISACA, IoD....
Chair of the Institute of Measurement and Control’s Industrial Cyber Special Interest Group

Member of the UK Cyber Alliance committee. We are building the new UK Cyber Council funded by DCMS/Gov UK.

Member of the National Cyber Security Centre (NCSC)’s Industrial Cyber Community of Interest group.

Member of MESA Manufacturing Cyber working group
The UK Cyber Security Alliance to create the new UK Cyber Security Council
OT ICS Cyber Security Activities

- Surveys and Audits
- Governance, Policies & Procedures
- Risk Assessments
- Compliance and Framework studies
- Integrity and Access Controls
- Intrusion Monitoring and Prevention
- Command and Control Management
- Vulnerability Management
- Training and Briefings
- ........and ....common sense strategies.....
Hands Up !!

Who, in your organisation, is personally responsible for Health and Safety?

Who, in your organisation, is personally responsible for Cyber Security?
"There are now three certainties in life
- there’s Death, Taxes, and foreign intelligence service on your system,“
– Head of MI5 Cyber

“There are two kinds of companies...
There are those who've been hacked... and those who don't know they've been hacked.....”
FBI Chief – James Comey

Cybersecurity at the Heart of the 4th Industrial Revolution.
Over the next 10 years, digital transformation is expected to unlock an estimated $10 trillion of value for business and wider society.
Davos
“There are more 18 year old males using Facebook than there are 18 year old males living on Earth today.”
Cyber Attacks are increasing because...???

LinkedIn breach affected around 117 million.

DropBox security breach exposed 69 million accounts.

Equifax breach 143 million accounts

\[
117 \times 2.50 = 300M
\]

Account sell price.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>iTunes</td>
<td>$8</td>
</tr>
<tr>
<td>Groupon.com</td>
<td>$5</td>
</tr>
<tr>
<td>GoDaddy.com</td>
<td>$4</td>
</tr>
<tr>
<td>Facebook</td>
<td>$2.50</td>
</tr>
<tr>
<td>Twitter</td>
<td>$2.50</td>
</tr>
</tbody>
</table>
What IT, Computers, Networks, IOT, IIOT in a large office facility is at risk?

Office Networks
Office Backups
Computer Server Room
Computer Server Room Fire Suppression
PA Public Address System
Access Control Network
Card Reader and Biometrics
Security Control Room
Reception Computer Terminals
Printers everywhere
WiFi repeaters
Door Control systems
TV on-demand networks

CCTV Network
CCTV Cameras
Backup Power Supply Generators Room
UPS Backup Systems
Fire Detection and Alarm Systems
Fire System Network
Building Management Systems
Building Management
HVAC Systems
Gate Control Systems
Vehicle Stopper Control Systems
Vending Machines and networks
The National Cyber Security Centre is part of GCHQ and aims to **make Britain the safest place to live and work online**.

NCSC has defended the UK against more than 600 cyber attacks in the past year – bringing the **total number to almost 1,800** – significant number from Nation States.
The Industrial IT World

Safety == Security
LIVE

BREAKING NEWS

MASSIVE CYBER ATTACKS

12:49 CRITICAL NATIONAL INFRASTRUCTURE DISABLED BY CYBER ATTACKS

Could it happen??
In previous years we were missing **Stories relevant** to Industrial Cyber .... But now..

- WannaCry
- Petya
- NotPetya
- Ukraine1
- Ukraine2
- BlackEnergy

### Cybercampaigns
- Stuxnet
- DroppingElephant
- DragonFly
- Triton
- Equation
- Norsk Hydro
- Shamoon wiper
- StoneDrill
- CrouchingYeti
- Industroyer
- Carbanak
- RedOctober
- BlackEnergy2
- Andromeda
- DarkHotel
- ShadowBrokers
- Mirai
- Gaus
- ZeuS
- Havex
- PetulantPenguin
- Turla
- BlackEnergy
- Ukrainian

---

Cybercampaigns.net and apt.securelist.com for APT Groups

- BlackEnergy2
- Triton
- Norsk Hydro
- LockerGoga
- Industroyer
- KillDisk
- EnergeticBear / CozyBear
- Slammer and Conficker Worm
- PetulantPenguin
- Agora+ for Canvas and Metasploit

---

Dallas Emergency Sirens
- Kemuri Water
- Flame
- EnergeticBear / CozyBear
- Slammer and Conficker Worm
- PetulantPenguin
- Andromeda
- DarkHotel
- ShadowBrokers
- Mirai
- Gaus
- ZeuS
- Havex

---

German Steelmill
- NightDragon
- Maersk
- Duqu
- StoneDrill
- CrouchingYeti
- Industroyer
- Carbanak
- RedOctober
- BlackEnergy2
- Andromeda
- DarkHotel
- ShadowBrokers
- Mirai
- Gaus
- ZeuS
- Havex
- PetulantPenguin

---

Vibert Solutions
A recent Kaspersky survey has discovered that two-thirds (67%) of industrial organizations do not report cybersecurity incidents to regulators.
Office Networks
Office Backups
Computer Server Room
Computer Server Room Fire Suppression Systems
PA Public Address System
Access Control Network
Card Reader and Biometrics devices
Security Control Room
Reception Computer Terminals
Printers
WiFi repeaters
Door Control systems
TV on-demand networks
CCTV Network
CCTV Cameras
Backup Power Supply Generators Room
UPS Backup Systems
Fire & Gas Detection and Alarm Systems
Fire System Network
Building Management Systems
Building Management Networks
HVAC Systems
Lift/Crane Control Systems
DeSal Control Systems
Stabiliser and Ballast systems
Emergency Shutdown systems
Office Networks
Office Backups
Computer Server Room
Computer Server Room Fire Suppression
PA Public Address System
Access Control Network
Card Reader and Biometrics
Security Control Room
Reception Computer Terminals
Printers everywhere
WiFi repeaters
Door Control systems
TV on-demand networks
CCTV Network
CCTV Cameras
Backup Power Supply Generators Room
UPS Backup Systems
Fire Detection and Alarm Systems
Fire System Network
Building Management Systems
Building Management
HVAC Systems
Gate Control Systems
Vehicle Stopper Control Systems
Vending Machines and networks
Example industrial network

Industrial IT System Architectures
The Industrial World...... vendor examples
Exploits – now easier to use

Is your site listed on **SHODAN**?........
Are your trusted suppliers listed?........

**GLEG SCADA pack,**
**MetaSploit**
**CANVAS**

Compromise “Test” Tools

<< FREE AND EASY !! >>
Cyber Myths debunked - based on findings

Myth: **We are disconnected.**
Fact: Many systems have 10+ connections to the World.

Myth: **Firewall protected.**
Fact: Many firewalls set to allow ‘any’ on inbound.

Myth: **Hackers don’t understand our Unusual/Legacy Systems.**
Fact: Increase of hackers specifically attacking you due to kudos of accomplishment.

Myth: **We are an unlikely target.**
Fact: Can be collateral due to proliferation of attacks and supply chain. Nation-state variants.

Myth: **Safety/backup systems will protect us.**
Fact: Safety/backup systems just as likely to be hit. Often similar technology systems used.
Industrial Cyber Standards and Regulations are evolving

**CAF 3**  NCSC Cyber Assessment Framework

**OG-86**  HSE - Cyber Security for Industrial Automation and Control Systems (IACS) EDITION 2


**NERC CIP 002-009**  Cyber Security Standards for Critical Infrastructure Protection

**ISO/IEC 2700x**  Information Security Standards

**NIST**  Cyber Security Framework (CSF)

**ANSSI**  Cyber Security for Information Systems (France)

**BSI**  Cyber Security for Information Systems (Germany)

**NIS-D**  NIS Directive  - Networks and Information Systems (EU)

....and.. Corporates/Enterprise’s own home-brewed standards.....
**Objective A: Managing security risk**

Appropriate organisational structures, policies, processes are in place to understand, assess and systematically manage information systems supporting essential functions to the network and systems.

**Objective B: Protecting against cyber attack**

Proportionate security measures are in place to protect the network and information systems supporting essential functions from cyber-attacks.

**Objective C: Detecting cyber security events**

Capabilities exist to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential functions.

**Objective D: Minimising the impact of cyber security incidents**

Capabilities exist to detect potential security problems and track the effectiveness of existing security operation of essential functions, including the restoration of those functions where necessary.

**D.1 Response and recovery planning**

Putting suitable incident management and mitigation processes in place.

**D.2 Lessons learned**

Learning from incidents and implementing these lessons to improve the resilience of essential functions.
Common Sense Methodologies

... Where to start?
Successes

- Exec Supporter/s
- Business Aligned to Changes to come on the Stairway
- All Departments working together on the journey.
- Internal and External Partners on the A-Team
- Frameworks, Jigsaw, Compliance, Best Practice, Governance
- Management of Change. Build Resilience
Security Strategy, Projects and Programmes

• Is Security part of Business-as-Usual for the Board of Directors?

• Remember – The Bad Guys don’t stop getting better – you need Strategy...

• How do you learn and share? - Strategic Relationships

• How do you start to improve? – Security Staircase

• What products, partners and vendors are useful? – Security Jigsaw

• Who will make the improvements? – Security A-Team
Raising Awareness
Sharing Experience
Cyber Games
Basic Mitigations

‘Threats /Risks/ Impacts’

‘Profitable Business Operations’
Predictions from 2017...2018..2019...

- Disclosing Attacks becomes mandatory. ✓
- Nation-State Alliances form. ✓
- Cyber and Safety no longer in silos. ✓
- Supply-Chain security mandatory. X
- ICS Cyber Insurance becomes “real”. X
- The Kaspersky/Huawei Effect grows. ✓
- OT Security Market thins. ✓
- Real attacks on Industrial Safety Systems. ✓
- ICS Specific Malware Exploits grow. ✓
- AI OT Cyber Security grows. ✓
- Growth of Security-By-Design. ✓
- Nation State ICS probing grows. ✓
Quantum Computing

Google has calculations more than 3,000,000 times as fast as the world's fastest computer

Big Data

Artificial Intelligence

Machine Learning

Autonomous bots
Be Safe......
Keep others Safe.....

We look forward to being on YOUR Security A-Team.

Thank you ......
- CNI
- Tier 1 Primes & Tier 1 Integrators

**The Cyber Knowledge Plimsol Line**

- Systems Integrators
- Academia
- Supply Chain/VARs
- Vendors
- Tier 2, 3, 4, 5 Suppliers
- End-Users

**The UK Cyber Capability Iceberg**

- Experience
- Training
- Certification
- Threat Awareness
- Purpose
- Requirement
- Budget

- No Hands-on Experience
- Minimal Training
- Minimal Certification
- No Threat Awareness
- Occasional Requirement
- Little Budget
Cyber Management

Security Questions for the Organisation

Does the institution participate in an incident, threat, vulnerability notification and sharing service?

What is the industry best practice and how does the institution compare?

What can be done to successfully implement information security governance?

Does the board understand the institution's dependence on information?

Does the institution recognize the value and importance of information?

Does the institution have a security strategy?
Round-Table Questions..Questions..Questions...

Chatham House Rules – Non-Attribution!

Compliance?  Policies?
Audits?  Procedures?
Scans?  Assets?
Surveys?  Segregation?
Briefings?  UK/EU/US?
Workshops?  27001?
Training?  62443?
Board Advisory?  Tools?
State of the Nation?  Physical Security?
Essentials?  Wireless?
Threats?  Gov?
Vulnerabilities?  GCHQ?
Consequences?  Certification?
Risks?  Predictions?
Governance?  Assistance?
Consulting?
ICS Security Books
Cyber Management Business Benefits

**RISKS**

- security standards;
- privacy legislation;
- spam legislation;
- trade practices legislation;
- intellectual property rights, software licensing;
- record keeping requirements;
- environmental legislation and regulations;
- health and safety and accessibility legislation;
- social responsibility standards.

**REWARDS**

- Increased predictability
- reduced uncertainty of business operations
- Protection from civil and legal liability
- Structure to optimize the allocation of resources
- Assurance of security policy compliance
- Foundation for effective risk management.
- A level of assurance that critical decisions are not based on faulty information
- Accountability for safeguarding information.
Security Enhancement Strategic Relationships

Together…. We are Stronger!
The Security A-Team

- The Team is the core
- Multi-role people
- Champions (social)
- Champions (technical)
- Financial budget holders
- Key decision makers
- Internal and External members
- Success is not simple
The **Security Staircase**

**The Security Staircase**

- Standard procedure not magic!
- Lots of help available internally and externally
- Build partners as integrated parts of the Security A-Team
- Use common sense and keep learning
- Do not under-estimate the cost of each step
- Must be Director CxO level supported
- Must be aligned to the Corporate Policies
- Climb then Repeat
Security Strategy, Projects and Programmes

Stairway to Security

**Scope.**
- Audits.
- Initial Threat Appetite.
- Focus/Focii of interest.
- ConOps – Operational Manuals.
- Initial Risks.
- Scope.
- Initial Contacts.
- Stakeholders.
- Required Outputs.

**Consult.**
- Methodology.
- Tools.
- Interviews.
- Threats.
- Risks.
- System Reviews.
- Business Operations.
- Policy Reviews.
- Audit Reviews.
- RAG analysis.
- Gap analysis.
- Mitigations report.
- CISO sign-off Mits.

**Design.**
- Network Architectures.
- Operational Procedures.
- Training Courses.
- Team Briefings.
- Guides.
- Policy Inclusions.
- Audit Inclusions.
- Design statements.
- SOC/NOC Integration Links.
- Mitigation Compliance.
- Review/Rework Timeline.

**Educate.**
- Training Courses for Teams.
- Build xFn Security Groups.
- Promote Security by Design.
- Education Media.
- Education 5 year Schedule..
- Link Teams to Peer Groups.
- Update blog/news feeds.
- Link with Academia.

**Integrate.**
- Integration with NOC function.
- Integration with SOC function.
- Integration with externals.
- Integration with xFn Teams.

**Deploy.**
- Deploy Designed Mitigations.
- Test results.
- Review Change Programs.
- Integrate Teams.
- Deploy Audit Mechanisms.
- Link Remote Management.
- Promote Changes.

**Monitor.**
- Monitor Systems for Threats.
- Tune system for false positives.
- Interviews teams for effectiveness.
- Gain initial CISO system approval.

**Defend.**
- Shadow full system defence.
- Carry out routine trials.
- Reiterate improvement program.
- 5 year schedule for re-work.
- 10 year planning cluster.

Initial Concerns.....
Risks, Threats, Impact Assessments

Security Assessments

- Wide range of methods
- Many tools open source
- Need an experienced head
- Can do much on your own
- Can be certified – ISO27001 Certification
- Most is common sense but inter-relationship meaning is learned.
- Useful to link assessments with Safety, People, Operations, etc.
- Essential to achieve full team buy-in for success.
- **This is not a one-off event!**
Security Jigsaw – products/vendors/partners

• If it don’t fit then don’t force it!

• Understand your requirements

• Review the market

• Keep reviewing and changing

• The market is embryonic

• Less may be more

• Nothing is perfect – try for “good” first.
Cyber Security Basic Mitigations

- Surveys and Risk Assessments
- Integrity Controls – whitelisting/lockdowns
- Anti-Malware
- Incident Investigation
- Intrusion Monitoring and Prevention (IDS/IPS)
- Command and Control Management (SOC/GSOC/NOC)
- Vulnerability Management/Intel – external links
- Training – … in all its forms....
- Simulation and Strategizing
- Maintenance and Controls

Cyber Essentials/SANS top 20/CERT advice/…….common sense .?.....
Recent Papers

https://www.bcs.org/content-hub/building-up-the-defence/

https://www.tripwire.com/state-of-security/featured/securing-sme-online-world/


https://pentestmag.com/product/pentest-pen-testing-scada-architecture/
The Business Challenge
Infineum (Exxon and Shell JV) has several Process Controlled (PCS) sites around the globe running a variety of vendor control systems. Infineum recognised the security enhancement and coordination benefits of providing a Global Security Operations Centre (GSOC) bringing together the current site security capabilities.

Vibert Solutions were asked to provide Subject Matter Expertise with both Process Control and Cyber Security experience together with Governance and Risk Assessment capabilities.

The Solution
Vibert Solutions provided assistance to a range of project challenges aligned with the GSOC Program. Tasks such as; to assess current state of compliance with industry standards; to act as Customer Subject Matter Expert; to link across Process Control, Project Management and Vendor groups; and to provide both Technical Design, Governance and Human input based on experiences, within highly controlled critical national infrastructures, to the Infiniun GSOC solution.

The project phase completed with high levels of success and acclaim from senior management and is being extended to further plants.

The Business Challenge
A Gas Pipeline has a number of pipeline control systems managed through Control Centres in different countries. The provision of Security and Network Operations Centre (SOC) and (NOC) capabilities is essential to ensuring security for pipeline operational and safety management.

Vibert Solutions were asked to provide Subject Matter Expertise with both Process Control and Cyber Security experience together with Governance and Risk Assessment capabilities.

The Solution
Vibert Solutions provided assistance to a range of project challenges aligned with the Gas Pipeline Control Systems Program. Tasks such as; to assess current state of compliance with industry standards; to act as Customer Subject Matter Expert; to link across Process Control, Project Management and Vendor groups; and to provide both Technical Design, Governance and Human input based on experiences, within highly controlled critical national infrastructures, to the Gas Pipeline solution.

SOS Security and People's University
Loss of systems, information, knowledge and competitive advantage is a major risk for Norwegian companies. Most have thought about the idea of securing themselves, but unfortunately it usually stops at the idea. Assistance was provided for practical cyber security enhancements. The assistance was tailored to be suitable for business leaders at all levels who want advice and tips on how to enhance cyber security. The work covered a taste of current threats, technologies and services to reduce threats, and an introduction to countermeasures and security strategies.

European Gas Pipeline
The Business Challenge
A Gas Pipeline has a number of pipeline control systems managed through Control Centres in different countries. The provision of Security and Network Operations Centre (SOC) and (NOC) capabilities is essential to ensuring security for pipeline operational and safety management.

Vibert Solutions were asked to provide Subject Matter Expertise with both Process Control and Cyber Security experience together with Governance and Risk Assessment capabilities.

The Solution
Vibert Solutions provided assistance to a range of project challenges aligned with the Gas Pipeline Control Systems Program. Tasks such as; to assess current state of compliance with industry standards; to act as Customer Subject Matter Expert; to link across Process Control, Project Management and Vendor groups; and to provide both Technical Design, Governance and Human input based on experiences, within highly controlled critical national infrastructures, to the Gas Pipeline solution.

Maritime Workshop
Collaborative workshop for industrial and IT cyber security expertise. Education, design reviews, planning, risks and governance workshop. Vessel and architecture aspect reviews.

Prominent UK Asset
Assistance was provided for industrial cyber security expertise, Risk Assessments, Governance Audits and Physical Security reviews.

Assistance was provided for industrial cyber security go-to-market strategies with business plans and industrial cyber security market knowledge.

SOS Security and People's University
Loss of systems, information, knowledge and competitive advantage is a major risk for Norwegian companies. Most have thought about the idea of securing themselves, but unfortunately it usually stops at the idea. Assistance was provided for practical cyber security enhancements. The assistance was tailored to be suitable for business leaders at all levels who want advice and tips on how to enhance cyber security. The work covered a taste of current threats, technologies and services to reduce threats, and an introduction to countermeasures and security strategies.

European Gas Pipeline
The Business Challenge
A Gas Pipeline has a number of pipeline control systems managed through Control Centres in different countries. The provision of Security and Network Operations Centre (SOC) and (NOC) capabilities is essential to ensuring security for pipeline operational and safety management.

Vibert Solutions were asked to provide Subject Matter Expertise with both Process Control and Cyber Security experience together with Governance and Risk Assessment capabilities.

The Solution
Vibert Solutions provided assistance to a range of project challenges aligned with the Gas Pipeline Control Systems Program. Tasks such as; to assess current state of compliance with industry standards; to act as Customer Subject Matter Expert; to link across Process Control, Project Management and Vendor groups; and to provide both Technical Design, Governance and Human input based on experiences, within highly controlled critical national infrastructures, to the Gas Pipeline solution.
SYNOPSIS

There are rapidly increasing threats to Manufacturing, Industry, Critical National Infrastructure and Office Infrastructures. Where do you start to address these threats? Is it a mountain or a molehill? What is Shamoon, Dancing Bear, Night Dragon, Triton and Petulant Penguin and how do we deal with them? What are your strategies as a company? How do you make those step changes in security improvements?

Are you a Manufacturer, an SME, a Port, Airfield, Factory, Ship, Energy or Transport Provider? Do you make things or deal with people, plant, devices, food, waste, water, fuel, chemicals or hazards?

Are you a large office with Access Control, Perimeter protection, Air Conditioning, CCTV, Machinery or any devices or systems that has a network of some kind?

Is it all secure? Really secure? Do you know about the latest threats?
Is your Health and Safety plan linked to your Cyber Security plan?
What are the threats, likelihoods, impacts, consequences, mitigations?
Are you compliant? Do you have a plan? How do you improve in a manageable way?

If you are unsure, want to learn more, or network with others in the same boat, then lets talk.
Some of the Conference Themes Today

- Blockchain
- Governance
- AI
- PPP Partnerships
- Cyber in Buildings
- Collaboration
- Crisis Management
- Continuity
- Quantum threat
- NIS-D
- Risk Management
- Integrated Safety and Security (Holistic Integrated Security)
- Lifestyle Change not Projects

If you are unsure, want to learn more, or network with others in the same boat, then let's talk.
Objective A: Managing security risk
Appropriate organisational structures, policies, and processes are in place to understand, assess and systematically manage security risks to the network and information systems supporting essential functions.

A.1 Governance
Putting in place the policies and processes which govern your organisation’s approach to the security of network and information systems.

A.2 Risk management
Identification, assessment and understanding of security risks. And the establishment of an overall organisational approach to risk management.

A.3 Asset management
Determining and understanding all systems and/or services required to maintain or support essential functions.

A.4 Supply chain
Understanding and managing the security risks to networks and information systems which arise from dependencies on external suppliers.
Objective B: Protecting against cyber attack

Proportionate security measures are in place to protect the network and information systems supporting essential functions from cyber attack.

B.1 Service protection policies and processes
Defining and communicating appropriate organisational policies and processes to secure systems and data that support the operation of essential functions.

B.2 Identity and access control
Understanding, documenting and controlling access to networks and information systems supporting essential functions.

B.3 Data security
Protecting stored or electronically transmitted data from actions that may cause an adverse impact on essential functions.

B.4 System security
Protecting critical network and information systems and technology from cyber attack.

B.5 Resilient networks and systems
Building resilience against cyber attack.

B.6 Staff awareness and training
Appropriately supporting staff to ensure they make a positive contribution to the cyber security of essential functions.
Objective C: Detecting cyber security events
Capabilities exist to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential functions.

C.1 Security monitoring
Monitoring to detect potential security problems and track the effectiveness of existing security measures.

C.2 Proactive security event discovery
Detecting anomalous events in relevant network and information systems.

Objective D: Minimising the impact of cyber security incidents
Capabilities exist to minimise the adverse impact of a cyber security incident on the operation of essential functions, including the restoration of those functions where necessary.

D.1 Response and recovery planning
Putting suitable incident management and mitigation processes in place.

D.2 Lessons learned
Learning from incidents and implementing these lessons to improve the resilience of essential functions.