



Member
CyberExchange

Practical Industrial Cyber Security Improvements Workshop.

Improvement Strategies, Project Engagement Approaches and Integrated Security & Safety.



VIBERT SOLUTIONS



VIBERT SOLUTIONS

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



[linkedin.com/in/vibertprofile](https://www.linkedin.com/in/vibertprofile)



[//twitter.com/cevnv">//twitter.com/cevnv](https://twitter.com/cevnv)

Vibert Solutions

This Workshop.....

Cevn and Ade



- Practical Industrial Improvements Programmes Introduction.
- **Lightning Workshop** – Create your own Improvement Programme.
- Team Presentation – 5 minutes in front of the Board
- Open Discussion forum
- Close

Running this workshop with able assistant **Ade Isaac**

Vibert Solutions Ltd.



Industrial Cyber Security Consultants and Advisors

- Consultants, Solutions, Speakers, Trainers, Coaches
- Our Teams advise companies in many countries and in most industry verticals.
- Security, Cyber, C2, MES, SCADA, Risk Management, Governance, Compliance, Industrial Networks, Consultancy and Training.
- 30+ yrs experience in Industrial Information and Control Systems.
- Board NED Advisor. Director. Chartered IT Professionals.
- CITP, MIET, MISA, MISSA, MInstMC, MBCS, MISA, MISSA, MISACA, MloD
- Vibert Solutions advises, consults, trains and presents to C-suite, boards, senior management or shop-floor teams at manufacturers, offices, integrators, industry, CNI and mission critical facilities in all aspects of industrial information and control systems security and compliance.



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



[linkedin.com/in/vibertprofile](https://www.linkedin.com/in/vibertprofile)



[//twitter.com/cevnv](https://twitter.com/cevnv)

Vibert Solutions

Cyber Security Capabilities

- Surveys and Audits
- Security Framework Developments
- Governance, Policies & Procedures
- Risk Assessments
- Compliance and Framework studies
- Integrity and Access Controls
- Incident Investigations
- Intrusion Monitoring and Prevention (Local and Global Industrial SOCs)
- Command and Control Management (ConOps)
- Vulnerability Management – external links
- Training and Briefings
- Simulation and Strategizing
- Maintenance and Controls
-andcommon sense strategies.....



VIBERT SOLUTIONS



VIBERT SOLUTIONS

Vibert Solutions



Chair of the Institute of Measurement and Control (InstMC)
Industrial Cyber SIG – launched this year.....

Join the SIG !



Member of the UK Cyber Alliance building the new UK Cyber
Council funded by Gov UK.



Member of MESA Manufacturing Cyber working group



© Katelee Arrowsmith/SWNS.com/MailOnline

Nuclear

Cyber



Industrial

CNI



ALES



VIBERT SOLUTIONS

Vibert Solutions

Cyber
Cevn



Analyst
Cevn



Community
Cevn



Vibert Solutions

Membership Get qualified Events Policy & Influence Develop your people Deliver & teach qualifications


Content hub Building up the defence

ARTICLE

Building up the defence

14 Mar 2019 5 min read

EMAIL SHARE TWEEET SHARE SHARE



The cyber physical bad guys are now attacking internet of things (IIOT) and the industrial internet of things (IIOT), says Cevn Vibert, Industrial Cyber Security Consultant and Educator. As the bad guys get better and better at attacking, so we must constantly get better at defending. There is evidence that the good guys have not properly started to improve their security stance yet, so this is a serious call-to-action.

Our modern society is built on automation, control systems and their management. The things mentioned often in the internet of things (IIOT) and the industrial internet of things (IIOT), are becoming smarter and more ubiquitous. If you think about all the automation-controlled things that have contributed to your day and try to list them, you may be surprised and perhaps a little worried to know that everything from the power grid to planes and care suppliers to cashpoints are being invisibly attacked.

Critical national infrastructures are under pressure from government, regulators and

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

Recent Papers



InstMC Precision Magazine 2019

(ISC)² BLOG

Home Archives **Subscribe**

SSCP Spotlight: Mario Barrowell | Main | Breached Data: Keeping it Secret Doesn't Make it Go Away

06 December 2017

EXPLORING INDUSTRIAL CYBER PHYSICAL SECURITY ENHANCEMENT



By Cevn Vibert, ICS Industrial Cyber Physical Security Advisor

Cevn will be hosting the session Grass Roots Industrial Control Security at ICS2 Secure Summit UK, between 12th and 13th December 2017.

The industrial cybersecurity market is facing rapid changes as more threats are discovered, more impact is felt by end-users and cybersecurity vendors vie for leadership.

My session will highlight both alerts and advice for end-users of automation and control systems (ICS/OT), as well as selected advisory notes for practitioners of Industrial Cyber Physical Security. Strategic methodologies and programmes of activities for mitigation of impacts on IIOT, IOT and how holistic integrated security can provide comprehensive situational awareness will additionally be provided. Multiple types of security are addressed, together with some mythical attack and defense scenarios. The history of industrial cyber-attacks are mentioned briefly, to counterpoint the prevalent myths of defense, and finally some alerts to the cyber arms race.

End-users face increased pressure to improve their security stance, and I will discuss some successful methods for implementing these improvements including a "stairway", a "jigsaw" and an "A-Team".

The cyber physical bad guys are now attacking IOT and IIOT. They are constantly getting better at attacking, so the good guys must also constantly get better at defending. There is much evidence that most good guys have not even properly started to improve their security stance yet, so my session will be a serious call-to-action too.

https://blog.isc2.org/isc2_blog/2017/12/exploring-industrial-cyber-physical-security-enhancement.html

If you're not sure where to start, here are some essential tips for keeping your business safe from cyber crime.

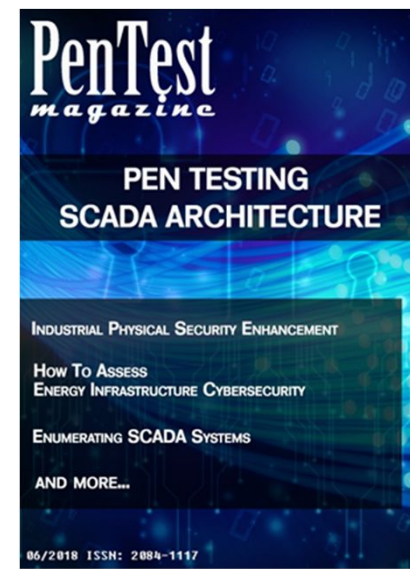


Identify All Possible Threats

"Cyber Risk Reviews must consider IT in your facilities such as AirCon, Lifts, Doors, Alarms & CCTV, not just networks" – Cevn Vibert, Industrial Cyber Security Advisory Director at Vibert Solutions

The first step in protecting your business is to run a cyber security audit. This will not only allow you to see where you are currently, but also identify any threats that are putting your business at risk.

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



<https://pentestmag.com/product/pentest-pen-testing-scada-architecture/>

Vibert Solutions in the industry ?



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

Wave the Flags. Socialise.
Enjoy. Promote.

Management of
Change. Build Resilience







Hands Up !!



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

Who, in your organisation, is **personally** responsible for Cyber Security?



Common Sense Methodologies



What is your objective?..

Cyber Standards and Frameworks..

Safety?

Do you use one or more of these?

Are you compliant?

Just continuous improvement?

GDPR

NIS D

NIST

NIST 800-53

BS31111

HSE og-0086

ISO27001

IEC62443

ANSSI

Cyber Essentials

Cyber Essentials+

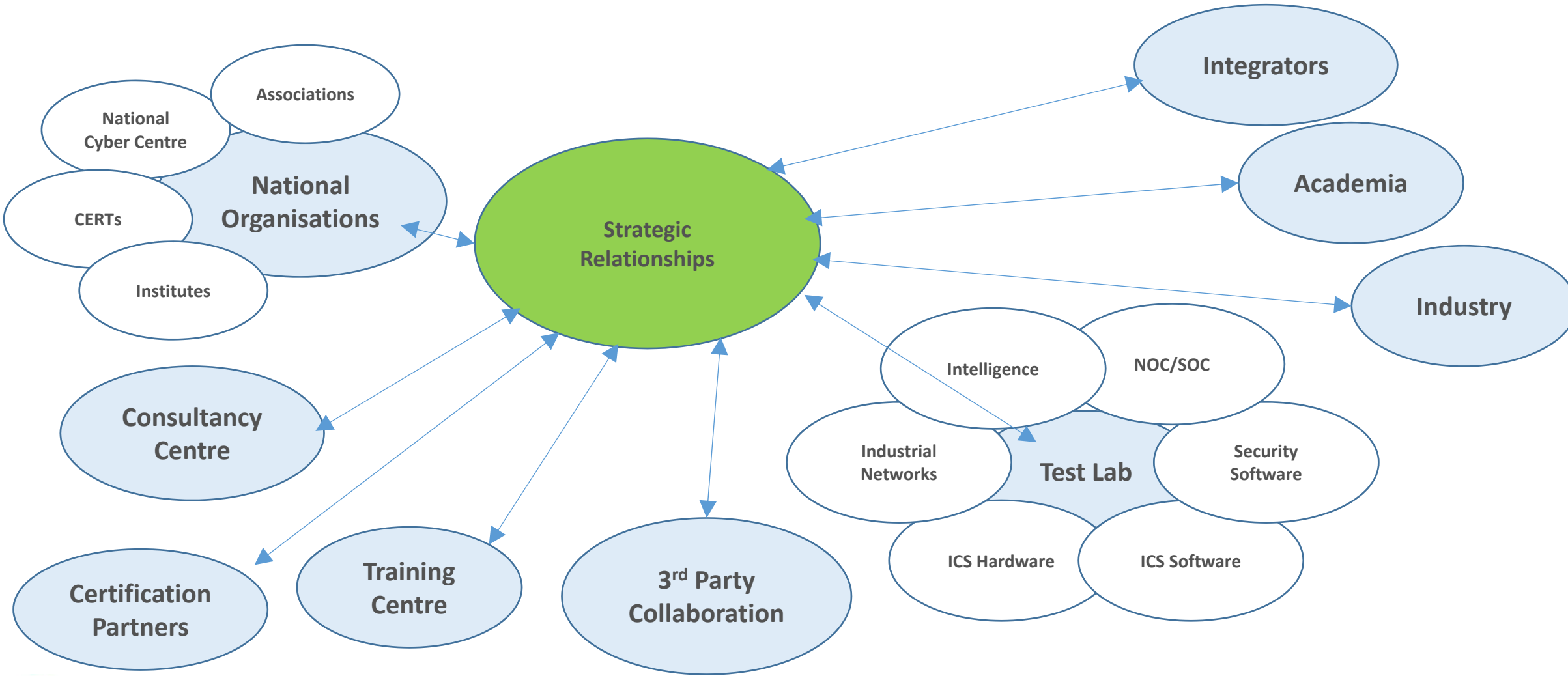


Strategy of Improvement Projects and Programmes

- Who needs strategy?
 - Balances of 'Threats/Risks/Impacts' to 'Profitable Business Operations'
 - Is this part of Business-as-Usual for the Board of Directors?
 - **Remember – The Bad Guys don't stop getting better.**
-
- How do you start to improve? – **The Staircase**
 - What products and vendors are useful? – **The Jigsaw**
 - Who will make the improvements? – **The A-Team**

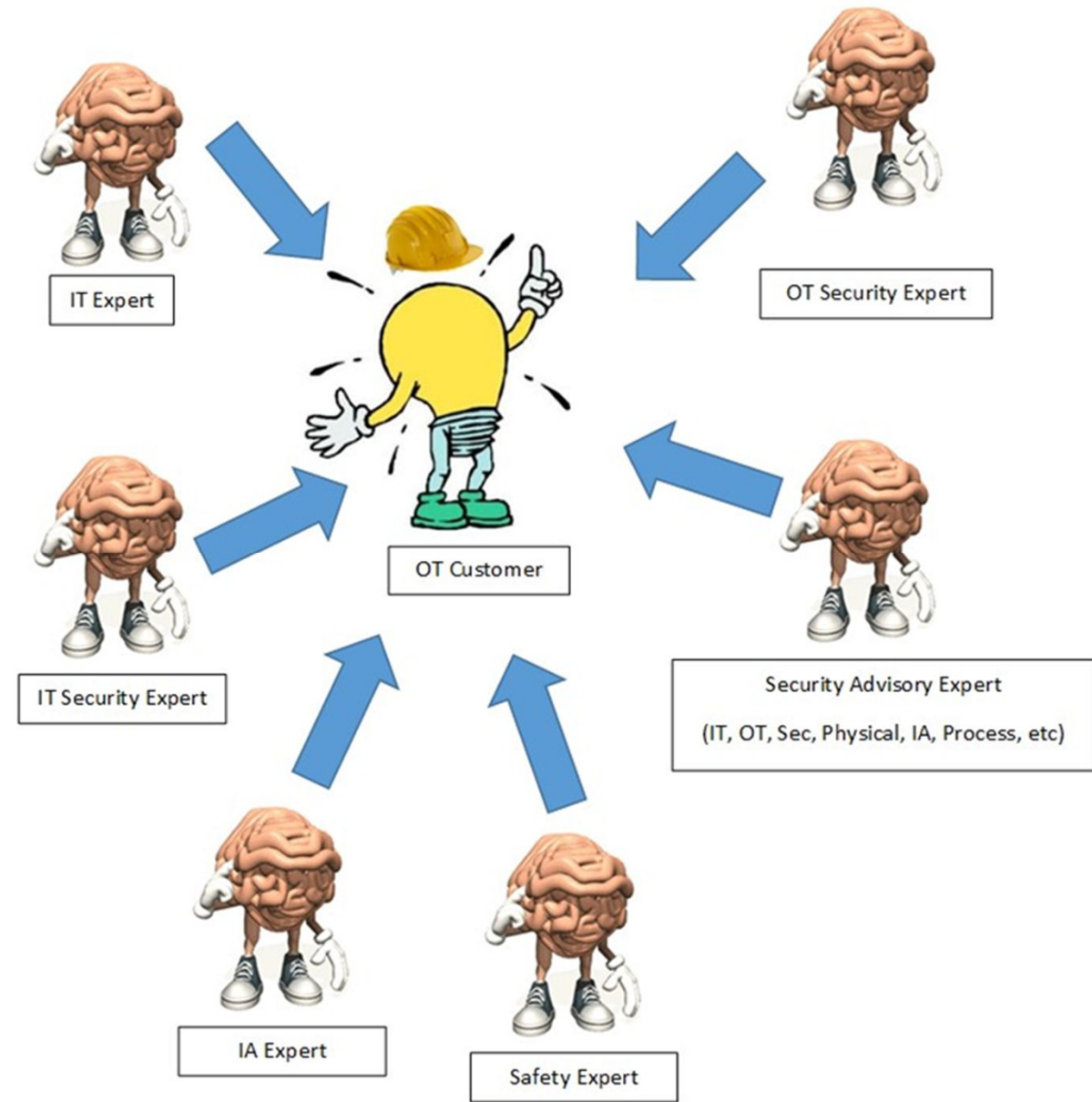


Strategic Relationships



The A-Team

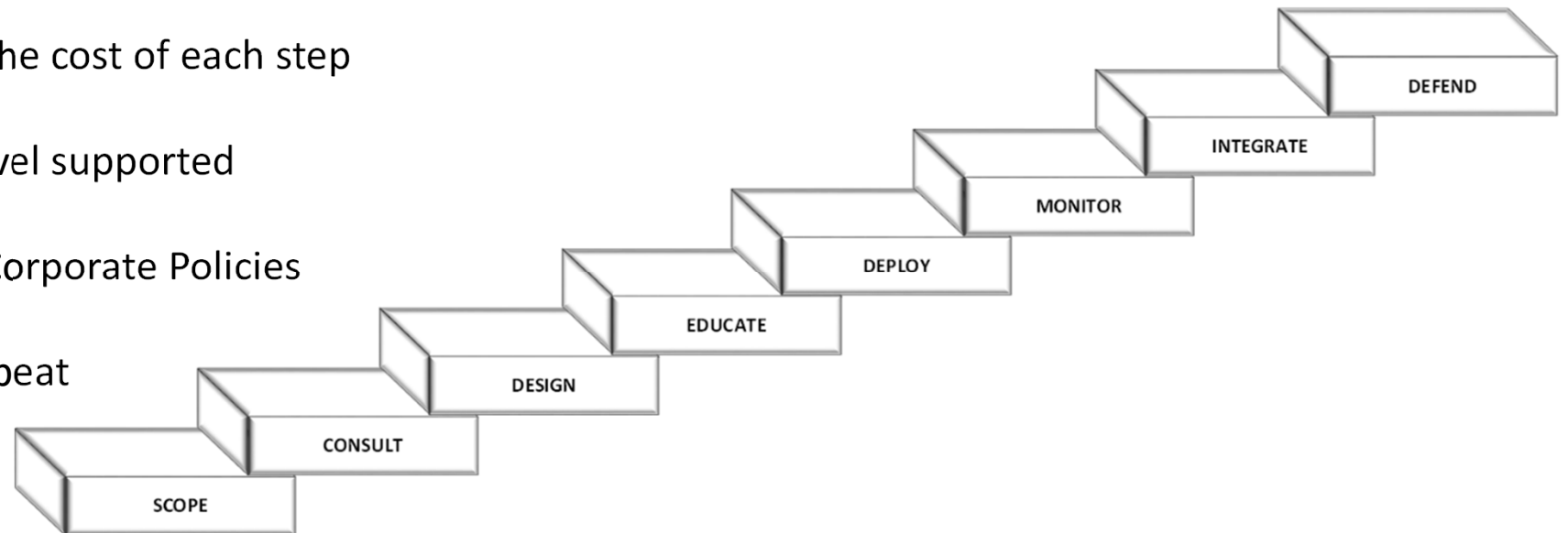
- The Team is the core
- Multi-role people
- Champions (social)
- Champions (technical)
- Financial budget holders
- Key decision makers
- Internal and External members
- Success is not simple



The Staircase

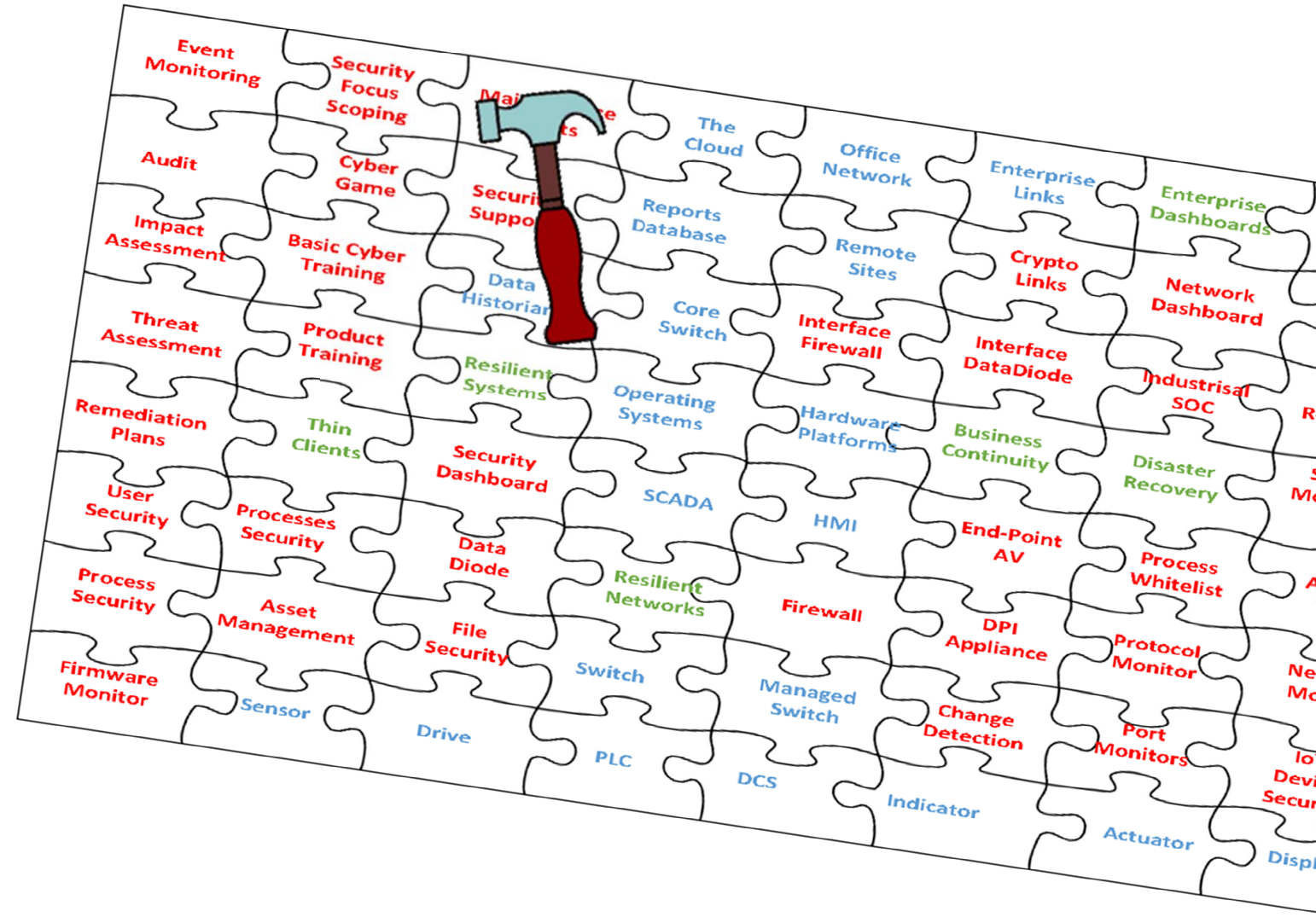
The Staircase

- Standard procedure not magic!
- Lots of help available internally and externally
- Build partners as integrated parts of the 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 staircase, then Repeat

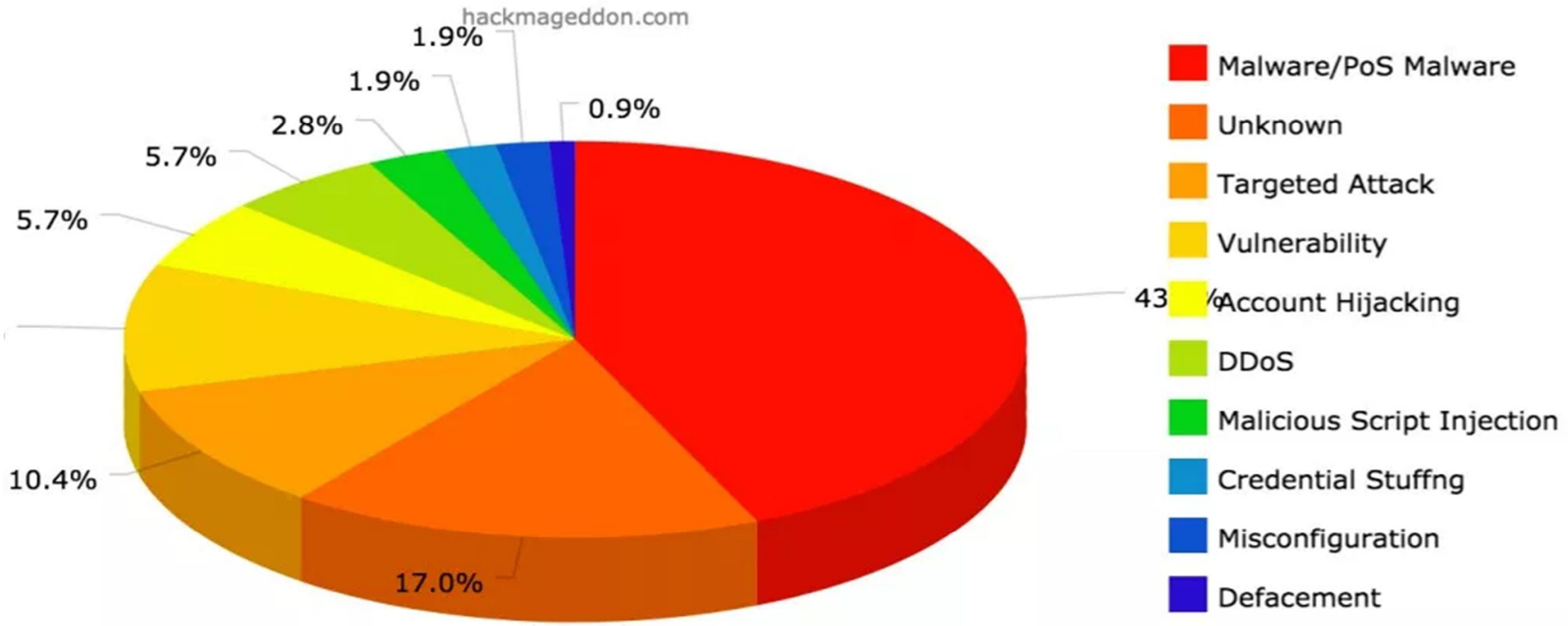


The Jigsaw – products/vendors/partners

- If it don't fit then don't just smash it in!
- Understand your requirement
- Review the market
- Keep reviewing and changing
- The market is embryonic in some areas
- Less may be more
- Nothing is perfect – try for “good” first.



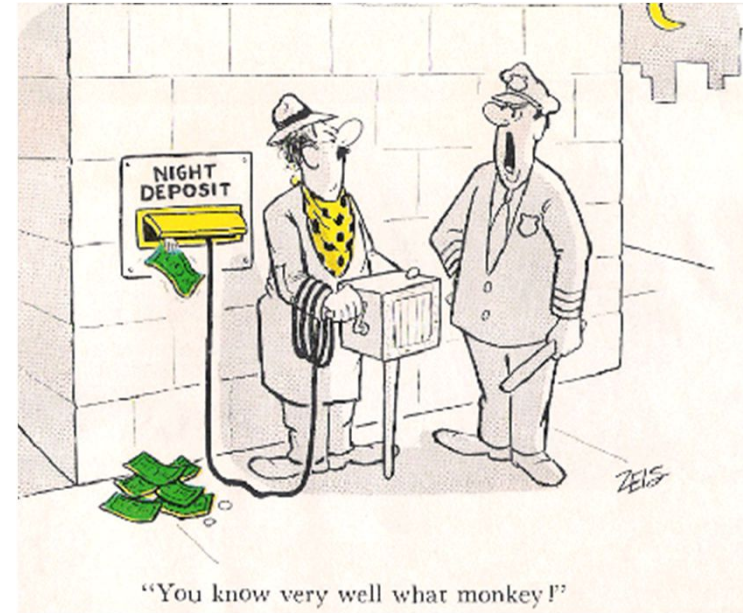
Attack Techniques (September 2018)



Basic Mitigations

- Surveys and Risk Assessments
- Gap Analysis to Frameworks
- Integrity Controls – whitelisting/lockdowns
- Anti-Malware
- Incident Investigation
- Intrusion Monitoring and Prevention
- Command and Control Management
- Vulnerability Management
- Training
- Simulation
- Maintenance and Controls

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



Reach out for help...



<https://www.ncsc.gov.uk/>

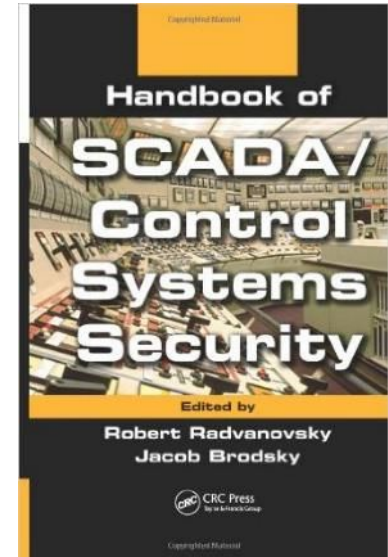
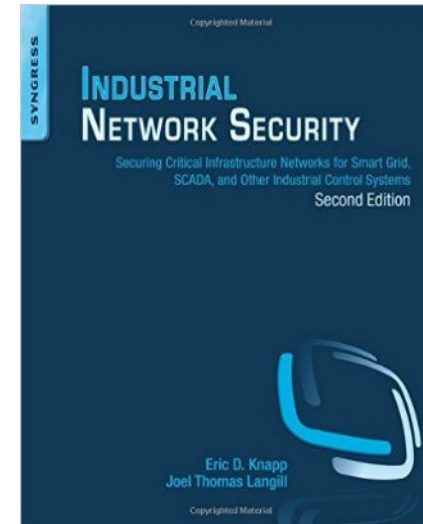
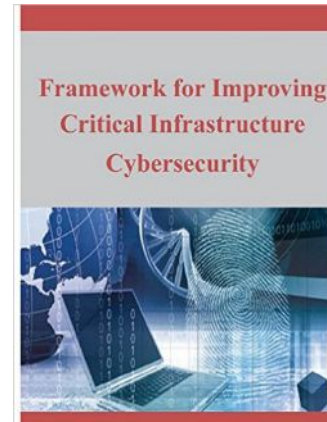
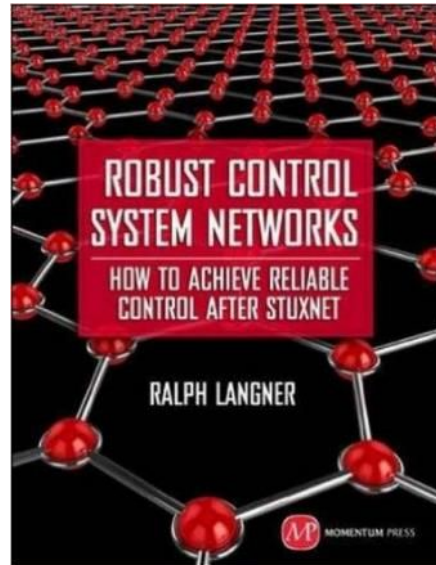
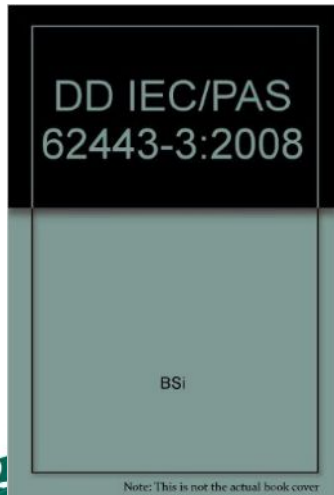
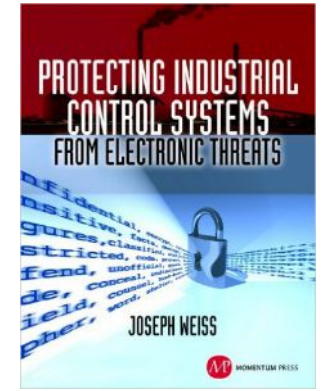
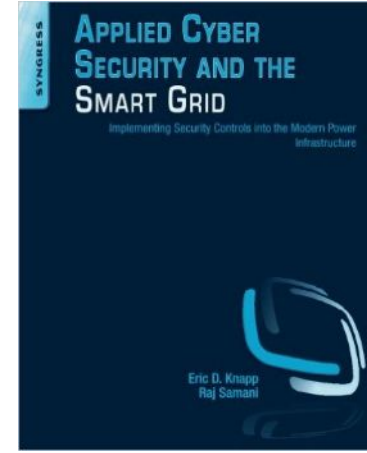
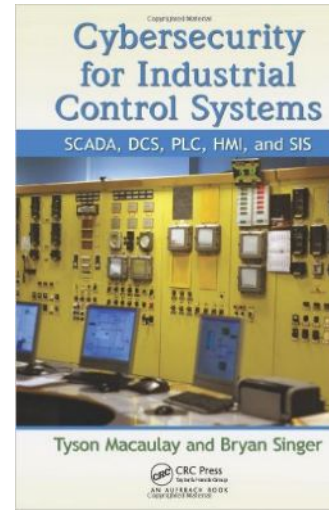
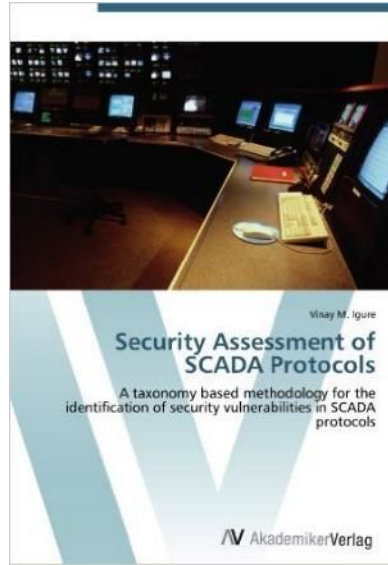
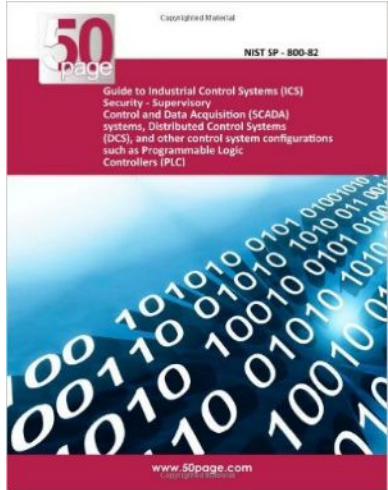
<https://www.ncsc.gov.uk/topics/cyber-threats>

<https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes>



Vibert Solutions

ICS Security Books



Think like a **hacker**...
to secure industrial control systems.

SCADAhacker.com



- Home
- Training
- Library**
- Resources
- Tools
- Dashboard
- Newsletter
- Blog
- About
- Contact

Donate



Contents

Library of Resources for Industrial Control System Cyber Security

★ = New/Updated Content Q1-2016

[Revision History](#)

ICS Vulnerabilities

- Year in Review ([2014](#) | [2013](#) | [2012](#) | [2011](#) | [2010](#))
- [Industrial Control Systems Assessments 2014 - Overview and Analysis](#)
- [Incident Response Summary Report - 2009-2011](#)
- [Distinguishing Internet-facing ICS Devices using PLC Programming Information](#)
- [2015 Cyber Security Report](#)
- [Common Control System Vulnerabilities \(2005\)](#)
- [Common Cybersecurity Vulnerabilities Observed in ICS \(2009\)](#)
- [Common Cybersecurity Vulnerabilities in ICS \(2011\)](#)
- [Common Cybersecurity Vulnerabilities Observed in Control Systems \(2008\)](#)
- [Leveraging Ethernet Card Vulnerabilities in Field Devices](#)
- [ICCP: Threats to Data Security and Potential Solutions](#)
- [Hacking Embedded Devices](#)
- [Cyber Incidents Involving Control Systems](#)
- [Safety vs Security \(2006\)](#)
- [Vulnerability Analysis of Energy Delivery Control Systems](#)

- ICS-CERT pdf ★
- ICS-CERT pdf ★
- ICS-CERT pdf
- AFIT pdf R3
- Control Engr pdf ★
- DHS pdf
- DHS pdf
- DHS pdf
- DoE pdf
- DigitalBond pdf R1
- EPRI pdf R4
- pdf R1
- INL pdf R5
- INL pdf
- INL pdf R4

- [Assessment Guidance](#)
- [Assessment Tools](#)
- [Best Practices](#)
- [Case Studies](#)
- [Cheat Sheets](#)
- [eBooks](#)
- [Government](#)
- [ICS Basics](#)
- [ICS Cyber Events](#)
- [ICS Protocols & Networks](#)
- [ICS Supplier Security](#)
- [Reference](#)
- [ICS Vulnerabilities](#)
- [Incident Response](#)
- [Insider Threats](#)
- [Multimedia](#)
- [News](#)
- [On-Line Tools](#)
- [OPC Security](#)
- [Open-Source Intelligence](#)
- [Risk Management](#)
- [Roadmaps](#)
- [Software](#)
- [Spreadsheets](#)
- [Standards](#)
- [Threat Intelligence](#)
- [Users Guides & Manuals](#)
- [Websites](#)
- [White Papers & Articles](#)

security and risk management strategies.



The ISF Standard of Good Practice for Information Security



The ISF Benchmark and Benchmark as a Service



Information Risk Assessment Methodology 2 (IRAM2)



Supplier Security Evaluation Tool (SSET)



Information Security Governance Diagnostic Tool



Security Function Diagnostic Tool



Supply Chain Assurance Framework (SCAF)



The ISF Maturity Model Accelerator Tool

S-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICSJWG

INFORMATION PRODUCTS

TRAINING

FAQ

Standards and References

This page provides an extensive bibliography of references and standards associated with ICS security. The list is categorized as follows with web links provided where applicable:

- [Cyber Security Policy Planning and Preparation](#)
- [Establishing Network Segmentation, Firewalls, and DMZs](#)
- [Patch, Password, and Configuration Management](#)
- [Control System Cyber Security Training for Engineers, Technicians, Administrators](#)
- [Establishing and Conducting Asset, Vulnerability, and Risk Assessments](#)
- [Control System Security Procurement Requirements Specification](#)
- [Placement and Use of IDSs and IPDSs](#)
- [Authentication, Authorization, and Access Control For Direct and Remote Connections](#)
- [Securing Wireless Connections](#)
- [Use of VPNs and Encryption in Securing Communications](#)
- [Establishing a Secure Topology and Architecture](#)
- [Applying and Complying with Security Standards](#)
- [Ensuring Security when Modernizing and Upgrading](#)

Cyber Security Policy Planning and Preparation

- National Institute of Standards and Technology (NIST) [Cybersecurity Framework](#) (title 48 CFR, part 101-11.6, NIST SP 800-171 Rev 2, May 2013)
- NIST SP 800-82 Rev 2, [Guide to Industrial Control Systems \(ICS\) Security](#), May 2010
- NIST SP 800-53 Rev 4, [Recommended Security and Privacy Controls for Federal Information Organizations](#), April 2013.
- ANSI/ISA-62443-2-1 (99.02.01)-2009 - [Security for Industrial Automation and Control Systems](#) - Establishing an Industrial Automation and Control Systems Security Program ([www.ansi.org](#))

Additional Information



Simulation Games

Typical Scenarios



Exciting!
Educational

**** New !! ****

IT and ICS networks

Order for your teams. Game and/or Events.
cevn@vibertsolutions.com +44(0)7909 992786



Vibert Solutions

Business Case.....



Business Case for Industrial Automation & Control System (IACS) Security Programme

An Approach.

Ade Isaac



Business Case for IACS Security Programme

- **Why Cybersecurity Management is Important**

- Protect our business from the impact of a cybersecurity incident
- Potential for cyber security incident to lead to a major accident and the impact to our business will vary
- However, these impacts need to be understood and managed accordingly if our business is to be able to operate as expected

- **Regulatory Requirements**

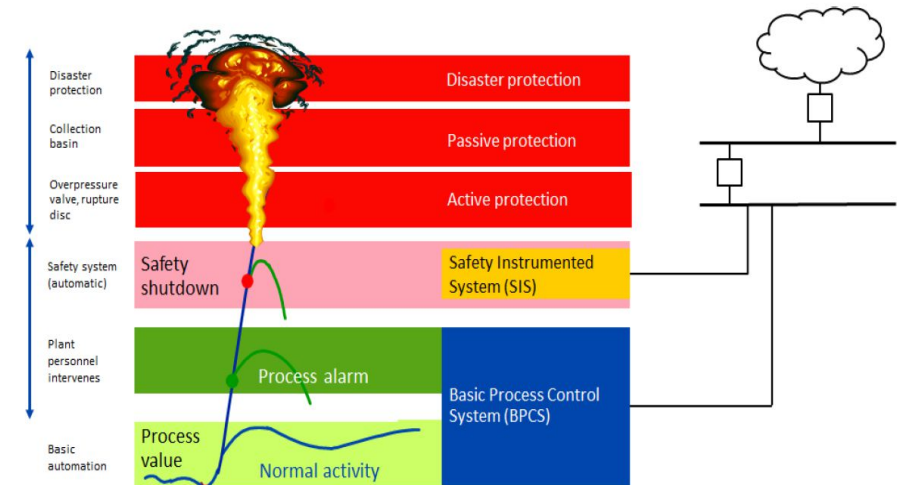
- NIS Directive (If in Scope) : Focus on operators of essential services (OES) security of supply
- UK Health and Safety Executive (HSE): Focus on Major accident hazard

- **Process Safety and Cyber Security**

- Traditional hazard and operability studies (HAZOPs) and layer of protection analysis (LOPAs) has generally excluded the potential for cyber related attacks to cause process safety incidents.
- What if a malicious actor or malicious code were able to enter and compromise the control system and safety instrumented system? This could result in the loss of three layers of protection based on a single initiating event or attack. **Such attacks have happened.**

- **Increased Security incidents involving IACS**

- Recent Examples
- Triconex Safety System on one of “Company XYZ” plant and in the program mode similar to the above plant at the time of the incident.



Source: aeSolutions Integrating ICS Cybersecurity with PSM
By Cusimano & Gruhn – April 18, 2016

Recent Example of Industrial Cyber Attacks

- **Equipment damage:** In 2014, hackers gained access to a steel mill in Germany and disrupted the operation of the safety system, causing massive damage to the blast furnace.
- **Service Outage:** In 2015, hackers infiltrated the control system of a Ukrainian power company and took control of the electricity distribution network. Approximately 80,000 homes were left without electricity for up to six hours.
- **Potential Plant Explosion:** In 2017, Saudi Arabian petroleum plant was hit with malware (Trisis) that tried to cause an explosion. The attack which was detected in August 2017, appears to have been designed to cause safety controllers to stop working by forcing a malfunction in the **Triconex' Safety System** i.e. targeting the safety override system, which could have caused an explosion that could have destroyed the entire plant.

Perceived “Company XYZ” Cybersecurity Risk – Risk Register

Targeted Asset(s)	Threat Agent	Threat Type	Likelihood	Consequence	Unmitigated Risk
Process Control and Safety Systems	External - Intentional sophisticated or Internal - Intentional sophisticated	Targeted malware attack	Possible / Likely	Critical Event: illness or Injury resulting in Multiple fatalities. Asset Damage or Financial loss >\$100M Regulatory action, including prosecution; request for significant improvement or temporary cessation of operations, significant fine.	25
Process Control and Safety Systems	External - Intentional unsophisticated Or Internal - Intentional unsophisticated	Targeted malware attack	Possible / Likely	Major Event: illness or Injury resulting in one fatality Asset Damage or Financial loss \$10M to \$100M Regulatory action, including prosecution; request for significant improvement or temporary cessation of operations, significant fine.	20
Process Control and Safety Systems	Internal - Unintended mistake Or External – General	General virus / Malware	Likely	Minor harm to company public reputation Notification will be required to the Regulator	10

Likelihood					
Chance	Virtually improbable and unrealistic	Conceivably possible, but very unlikely to occur	Unusual but possible	Quite possible or not unusual	Likely to occur
Frequency	Event could occur at some time greater than 100 years	Event could occur at some time within 10 to 100 years	Has occurred or is expected to occur within 5 to 10 years	Has occurred or is expected to occur within 1 to 5 years	Event expected to occur more than once per year

- Regulatory Requirements: Duty holder responsibility is to ensure the prevention and mitigation of major accident risk in workplaces.
- The risk shown above is based on the reason that our means of reducing risk of major accident often required application of process control and safety system. Therefore, our major hazard risk reduction depend on these systems functioning correctly.
- the risk shown can prevent “Company XYZ” from being able to achieve objectives stated in their mission statement

	Safety	Environment	Financial	Reputation		Likelihood				
						1 Improbable	2 Rare	3 Unlikely	4 Possible	5 Likely
Impact	↓ Medical Treatment, Minor Health Effects, First Aid Case, or Less	No off site impact	Potential equipment or asset damage or financial loss < \$100K USD	No harm or slight client concern	1 Trivial	1	2	3	4	5
	Medical Treatment with Restricted Duty or Medium Health Effects	One odor or noise complaint from event	Potential equipment or asset damage or financial loss \$100K to \$1M	Minor harm to the Company's public reputation or client concern	2 Minor	2	4	6	8	10
	Serious illness or injury resulting in days away from work (LTI); or a permanent partial Disability	On-site or off-site environmental release to soil/ground or multiple odor or noise complaints from event	Potential equipment or asset damage or financial loss \$1M to \$10M	Harm to the Company's reputation limited to the local area via local public media reports or local industry news, significant client concern	3 Moderate	3	6	9	12	15
	Illness or injury resulting in one fatality, or permanent full disability	On-site or off-site environmental release to surface water	Potential equipment or asset damage or financial loss \$10M to \$100M	Harm to the Company's reputation extends to the region through regional or national public media outlets or national industry or financial news, multiple significant client concerns	4 Major	4	8	12	16	20
	↓ Illness or injury resulting in multiple (2+) fatalities.	Major off-site impact (vapor cloud explosion, fire, major toxic gas release, major off-site environmental release, wildlife kill)	Potential equipment or asset damage or financial loss >\$100M	Harm to the Company's reputation extends internationally through public media outlets or negative publicity in international industry or financial news, global client concerns	5 Critical	5	10	15	20	25



“Company XYZ” IACS Security - Current Position

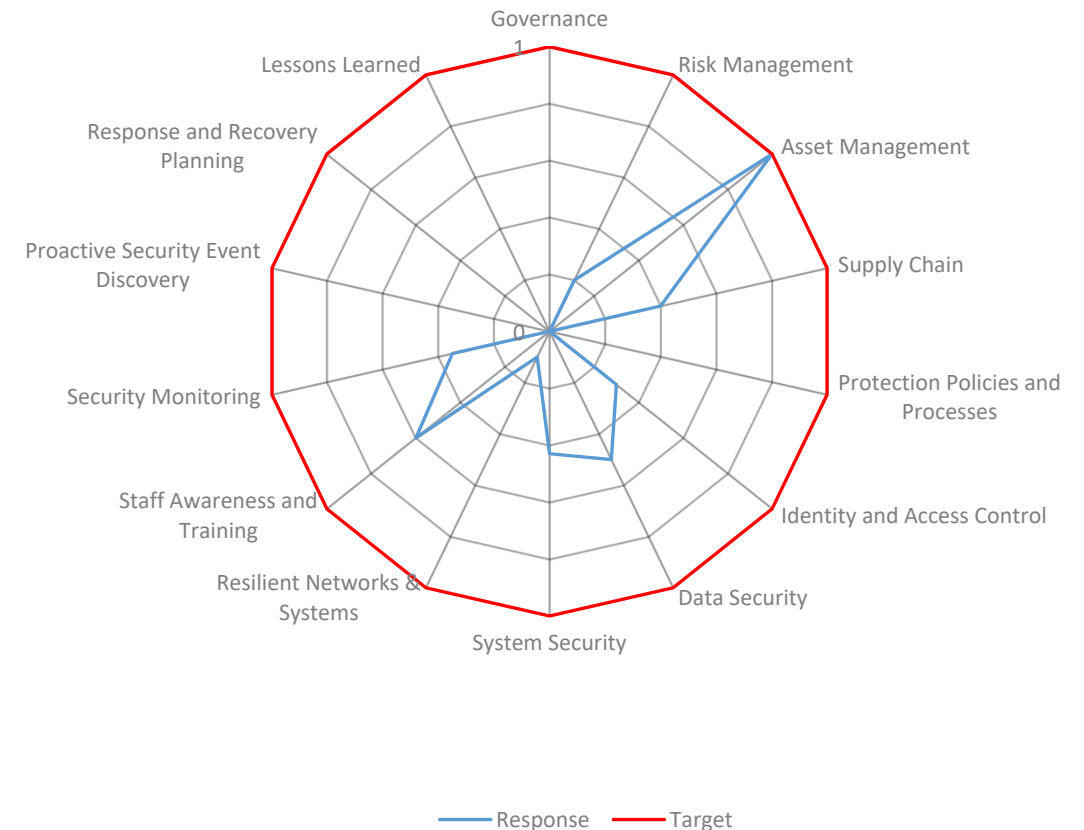
• IACS Cybersecurity Posture Assessment

- Typically conducted by External Specialist or competent personnel within the company
- Identification and Involvement of Key Stakeholders - This includes, but is not limited to: Senior Management| Company Head of HSE | C&I Technical Authority | Head of IT | Head of Supply Chain | Head of HR & Communication | Head of Security | Legal |Operations Managers | Maintenance Manager | C&I Engineers| IT Security Personnel | Third Party Contractors
- Assessment carried out based on recognised Cybersecurity Framework. Free tools such as US Department of Homeland Security ICS Cybersecurity Evaluation Tool (CSET) could also be used
- Produced Company Overall Assessment Result
- Timeframe typically 1 to 3 months depending on company structure.

• IACS Maturity - Concept/Identification phase

- Recognise need to protect property, assets, services, or personnel in cyber security terms
- Start developing the security program

"Company XYZ" Assessment Overall Result Mapped to NCSC CAF Assessment

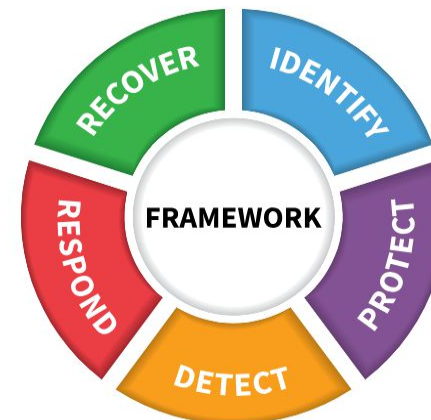


Proposed IACS Cyber Security Programme (CSP) & Strategy

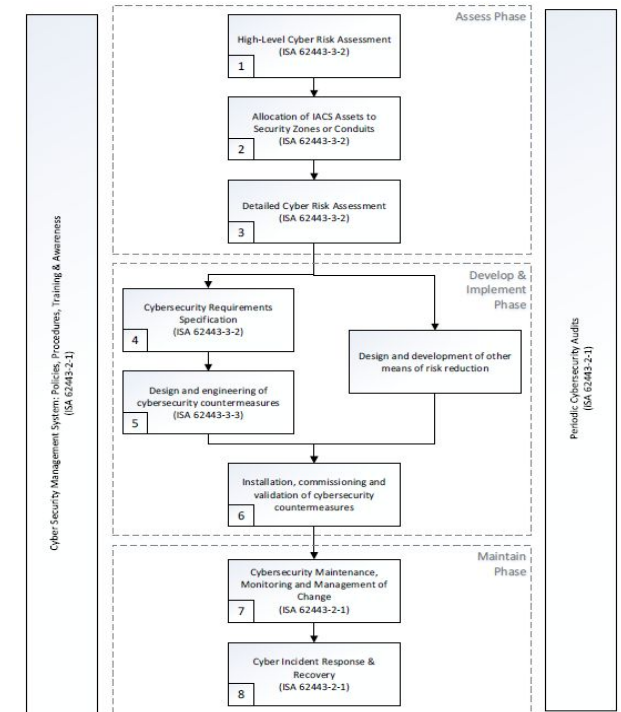
- The aim of the programme is to improve the company cybersecurity capabilities, so that the organisation is better able to manage the risk of cyber incidents. Due to the nature of threats, the proposed program is a continuous process.
- This risk mitigation programme will address the cybersecurity challenges the company faces and ensure compliance with HSE/NCSC recommended cybersecurity principles. This will be delivered in four parts:
 - Part 1: Assess Current Company IACS Security Posture - Complete
 - **Part 2: Assess and Define – Identifying, Understanding and Managing IACS Security Risks**
 - Part 3: Design & Implement
 - Part 4: Operate and Maintain

Strategy and Asset Selection

- Implement/test the new Cybersecurity Programme – Select an asset
 - Prove the programme prior to devoting a large amount of resources / time/budget
- Selection are based on:
 - Manned vs Unmanned Installations
 - Production Throughput
 - Regulatory Inspection (UK)
 - Location (Proximity to Society)
 - Accessibility & Media attention
- **Proposed to test the program at the “Y Site”**



NIST Cybersecurity Framework



Proposed ISA 62443 IACS Cybersecurity Lifecycle
Submitted by John Cusimano 04/15/2015

- Identify & Implement Good Practice and Quick wins on other assets and carryout preliminary cybersecurity activities on those assets such as
 - Asset Identification
 - Document site IACS inventory and Configuration



CSP Part 2: Assess & Define – Resources & Activities

Part 2 Activities

- Establish Governance Model & Reporting Structure
- Set up organisation for managing IACS Security
- Asset Identification : Asset Inventory, System Architecture Diagrams, Network Diagrams
- Prepare for Risk Assessment: Criticality Assessment, Gap Assessment, Vulnerability Assessments, Threat Intelligence
- Establish IACS Security Strategy, Policies, Standard and Procedures
- Implement Quick wins
- Provide Competency and/or awareness training to Key Stakeholders / employees / Contractors across all sites
- Carryout Risk Assessments
- Develop Risk Reduction Strategy (time-bound plan) to address any intolerable risks

Estimate Duration for Part 2

- XXX days

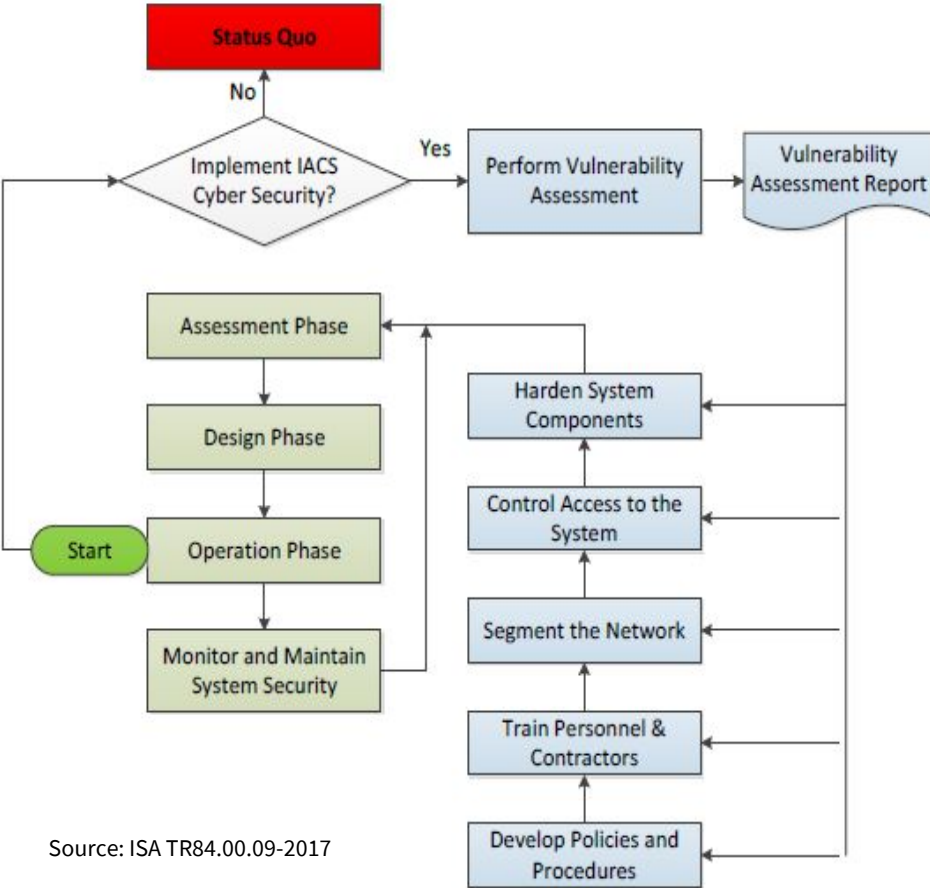
Proposed New Resources Requirements

- IACS Cyber Security Programme Project Engineer
 - Recruited or Appointed
- External Assistance – Multi vendor support



Order of Magnitude Cost Estimate – Part 2

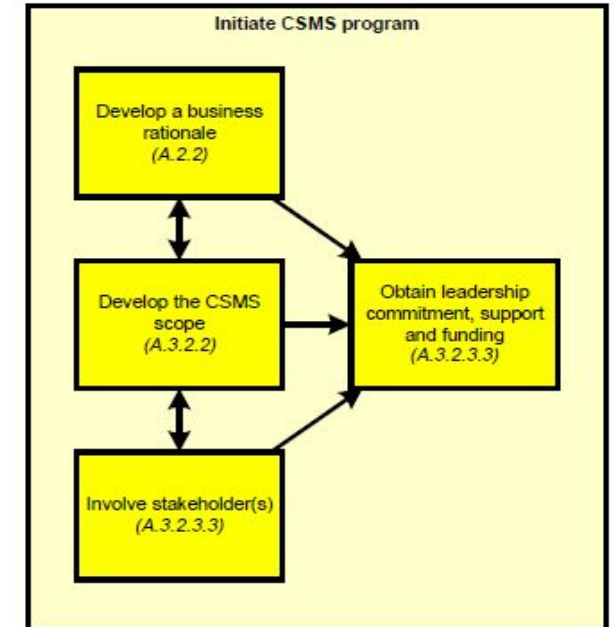
- IACS Cybersecurity Specialist Vendor - ££££££



Source: ISA TR84.00.09-2017

IACS Security Business Case - Conclusion

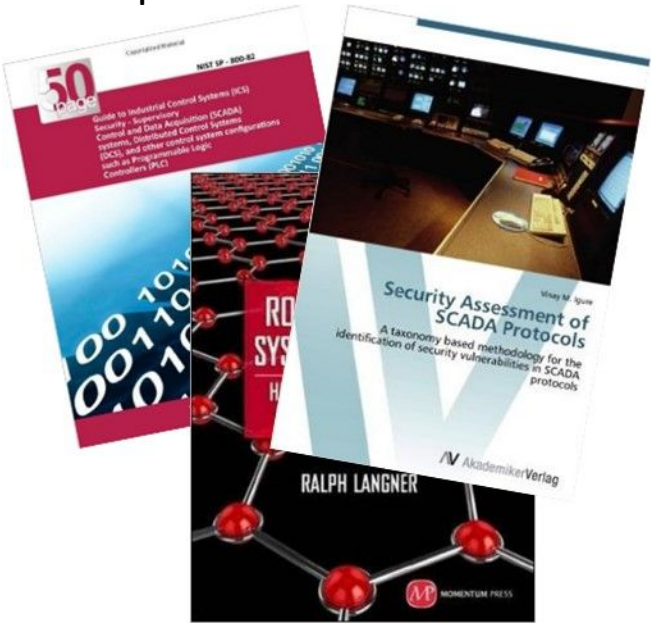
- The goal is to develop a cost-effective CSP that leverage existing business processes and organisation e.g. IT / Operations Processes and Procedures
- CSP is a combination of cross asset activities and individual asset activities
- Whilst Return on Investment (ROI) is difficult to quantify when it comes to Cyber, the CSP will be a fine balance of risk versus cost
- Organisation Resource Requirements: Increased responsibilities for stakeholders, increased competency and awareness required, additional resource(s) and funding will be required to achieve a CSP.
- The development of a management system for IACS security is a journey that may take months or years to achieve
- Overall aim of this Business Case is to obtain commitment, support, and funding for “Company XYZ” CSP



Source: IEC 62443-2-1 (Annex B)



Expert Books and Articles



Expert Websites



Raising Awareness Sharing Experience Cyber Games Basic Mitigations

Educational Games



'Threats
/Risks/
Impacts'

'Profitable
Business
Operations'

SECURITY 101



Strategy Recap.....



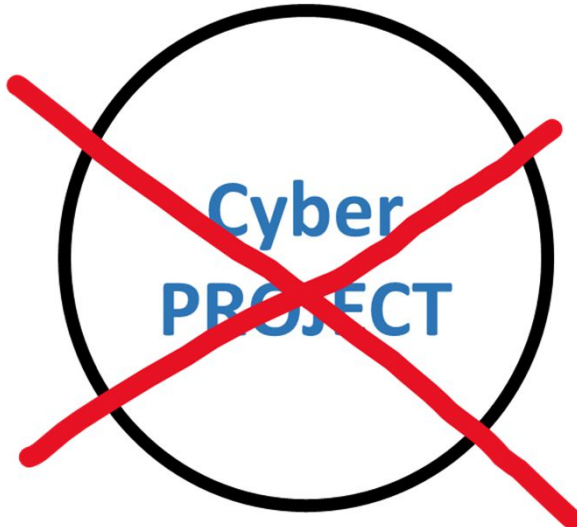
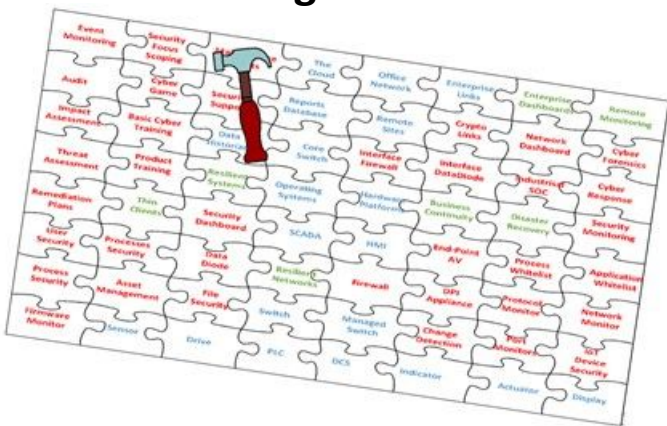
Security Methodologies

Lifestyle Change
Not
Programmes or Projects

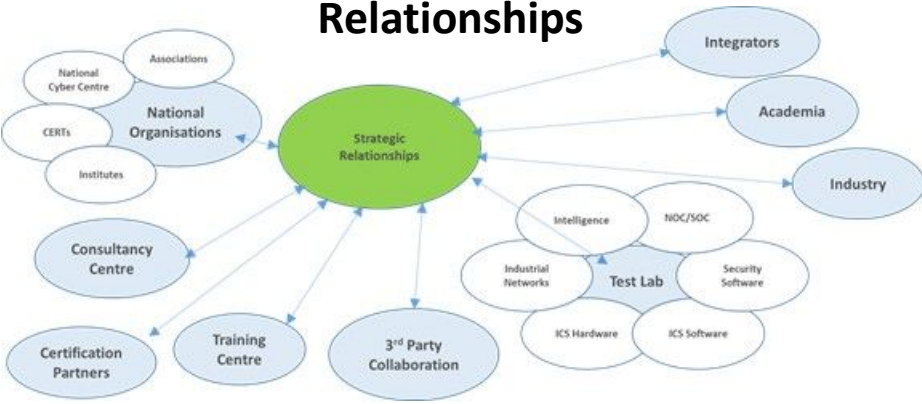
Audits



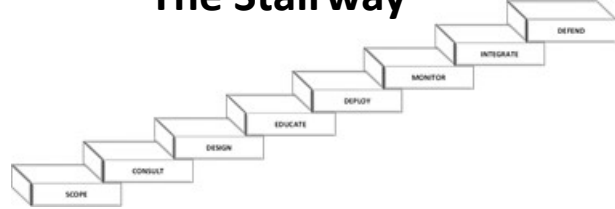
The Jigsaw



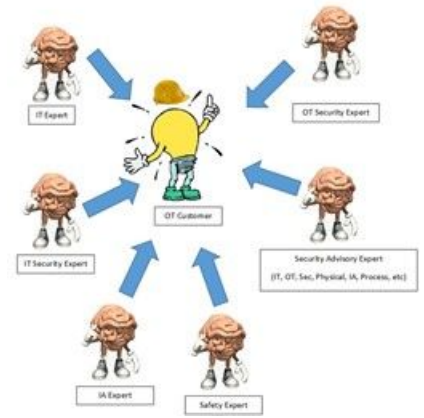
Relationships



The Stairway



The A-Team



Thanks What's Next..... ?????

- What did you learn?
- How can **you** improve **your** security?
- What are you going to do next?
- Do you need help?
- We look forward to being on YOUR Security A-Team.

Cevn@Vibertsolutions.com www.vibertsolutions.com 07909 992786



[linkedin.com/in/vibertprofile](https://www.linkedin.com/in/vibertprofile)



[//twitter.com/cevnv](https://twitter.com/cevnv)

The Workshop next....



Practical Industrial Cyber Security/Safety Improvements Workshop.

Improvement Strategies, Project Engagement Approaches and Integrated Security & Safety Training.



VIBERT SOLUTIONS



VIBERT SOLUTIONS

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



[linkedin.com/in/vibertprofile](https://www.linkedin.com/in/vibertprofile)



[//twitter.com/cevnv](https://twitter.com/cevnv)

Vibert Solutions

Company/Team Name:

Company/Team Name:

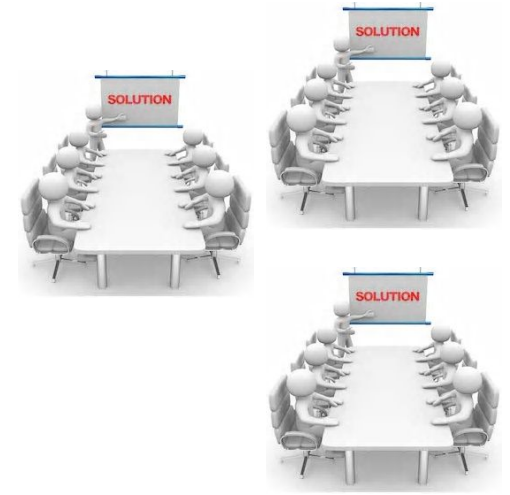
Company/Team Name:

Company/Team Name:

Company/Team Name:

Company/Team Name:

Company/Team Name:



Strategy Recap.....



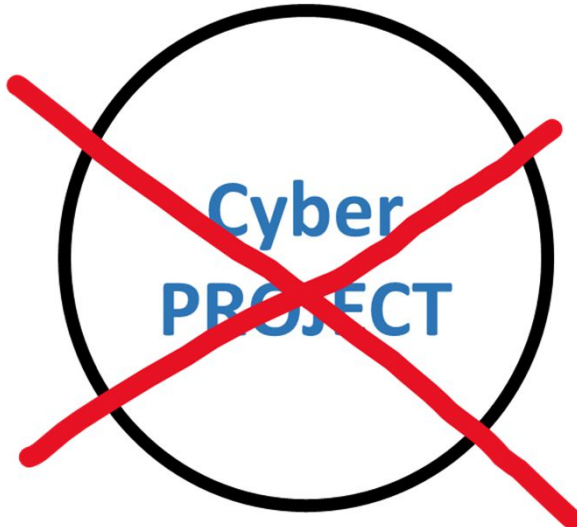
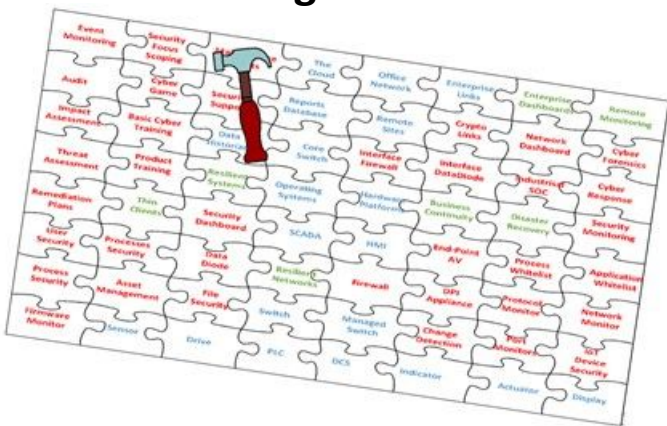
Security Methodologies

Lifestyle Change
Not
Programmes or Projects

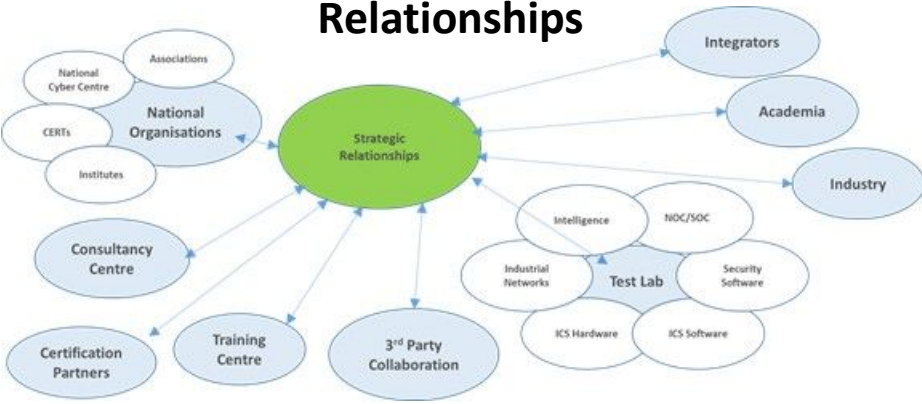
Audits



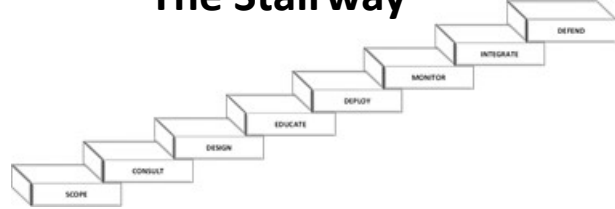
The Jigsaw



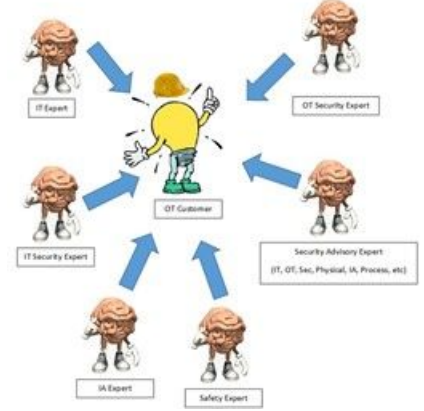
Relationships



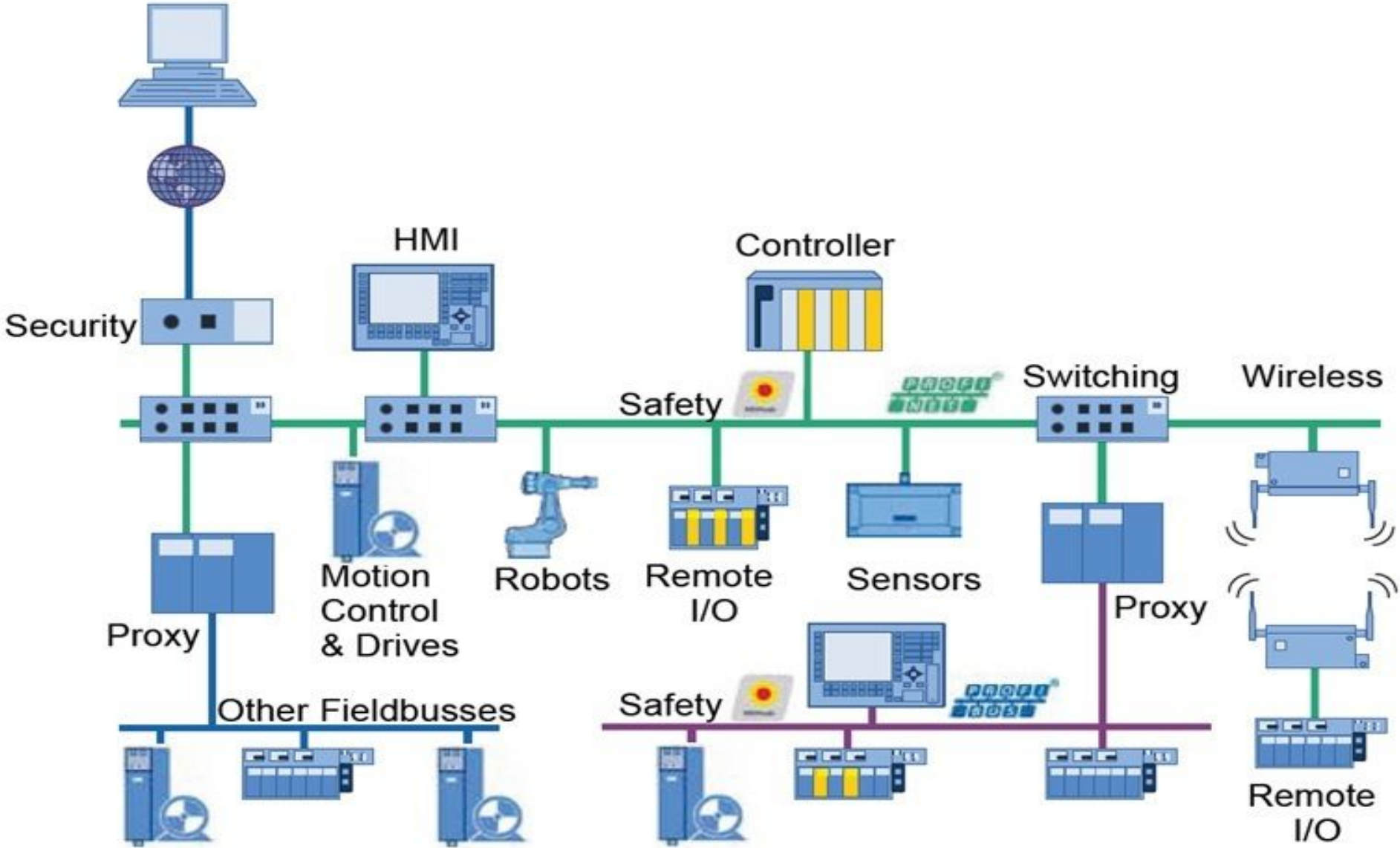
The Stairway



The A-Team



Example Industrial IT System Architecture



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

Wave the Flags. Socialise.
Enjoy. Promote.

Management of
Change. Build Resilience



1 Hour total!

Your workshop – your company – for your benefit

1. Define your problem! (“Concerned about APT Attacks on Safety Systems”)
2. Define your objectives and timescales
3. Understand Project Risks and Mitigations
4. Objective Budget Request Reasoning – “Business Benefits \$\$\$\$ ”
5. Strategy for small step proposals (a staircase.)
6. Build your A-Team
7. Choose Products and Services
8. Identify preferred Relationships and Sources of Learning
9. Measurements of Success
10. Inspiration for Future Steps

Quickly note them on the sheets. (2 mins per page – 20mins total)

Present them to the room. **(in brief 5 mins per team)**

Room discusses why it was difficult/easy in the time available. (excluding the obvious) **(10mins)**

KISS principle. Quickfire. Work Fast. Learn more. Share. Be Positive. Make it fun! It’s a race!



Your Company Name:

1. Define your Security/Safety Problem: APT Attacks on Safety Systems



High level of what you think the current security/safety problem is... (You are speaking to Senior Management/Directors/Board)

Your Company Name:

2. Define your Security/Safety Objective and Timescales:

Goal:.....

Timescales:.....

High level of what do you need to achieve and when (Big chunks but convincing)

Area	Project Management	Program Management
Focus	Single objective	Business strategy
Scope	Narrow	Wide-ranging, cross-functional
Benefits	Determined in advance Accrue after completion	Used to make decisions Accrue during the programme
Deliverables	Few, clearly defined	Many, many initially undefined
Timescale	Clearly defined	Loosely defined
Change	To be avoided	Regarded as inevitable
Success Factors	Time, budget, specification	Mission, cash-flow, ROI
Plan	Specific, detailed, bounded	High-level and evolving

Your Company Name:

3. Your Project Risks and Mitigations:

Risks:.....

Mitigations:.....

Accepted Risks:.....

High level of Major Risks and how you will deal with them (Big chunks but convincing)

Area	Project Management	Program Management
Focus	Single objective	Business strategy
Scope	Narrow	Wide-ranging, cross-functional
Benefits	Determined in advance Accrue after completion	Used to make decisions Accrue during the programme
Deliverables	Few, clearly defined	Many , many initially undefined
Timescale	Clearly defined	Loosely defined
Change	To be avoided	Regarded as inevitable
Success Factors	Time, budget, specification	Mission, cash-flow, ROI
Plan	Specific, detailed, bounded	High-level and evolving

Your Company Name:



4. Your Objective Budget Request Reasoning (Why):

e.g. Why this Project/Program?.....

Why this Budget?.....

What are the Benefits to the company?.....

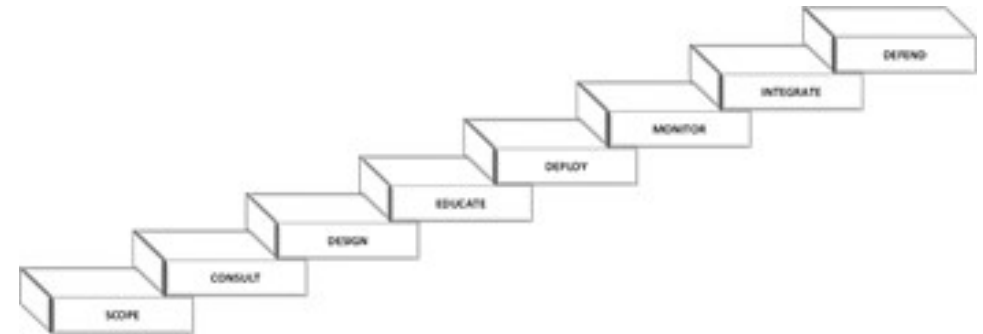
High level of why you need to achieve the goal, why does it cost so much and what are the benefits to the Board?

Your Company Name:

5. Your Program/Project Stages/”Staircase” (Small steps) and Why:

Stage 1: Why:.....

Stage 2: Why:.....



List key project/program stages and why they are in “a Stage”...

Your Company Name:

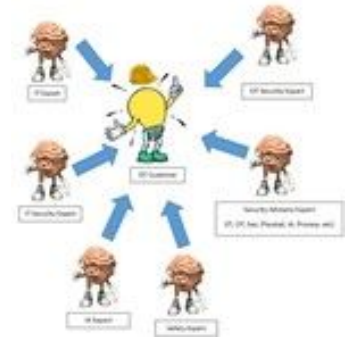
6. Your 'A-Team' and Why:

Role1: Why:.....

Role2: Why:.....

Role3: Why:.....

Role4: Why:.....



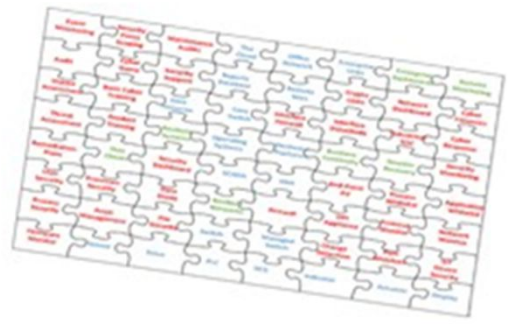
List key People/Roles and why they are chosen for this project/program...

Your Company Name:

7. Your 'Jigsaw' Products and Services and Why:

Product/Service1: Why:.....

Product/Service2: Why:.....



List major hardware/software Components (Services on separate page) you have chosen and why chosen...

Your Company Name:

8. Your proposed Relationships/Learning names/links:

Learning1: ...e.g. Talk to independent Consultants.....

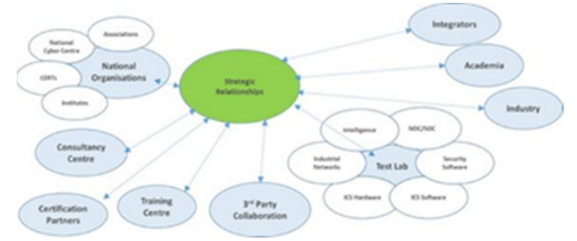
Why:...Impartial Advice.....

Learning2:

Why:.....

Learning3:

Why:.....



Chose some useful Learning Resources names/weblinks which will help this improvement plan (Vibert Solutions of course!! 😊)

Your Company Name:

9. Your Measurements of Success:

Success1: Why:.....

Success2: Why:.....



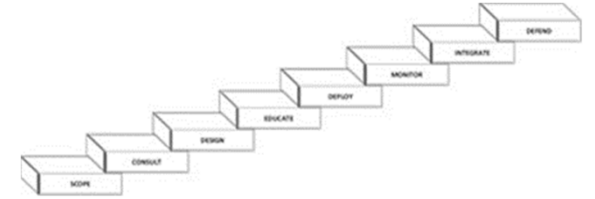
How will you measure your success, and what does GOOD look like for your audience?

Your Company Name:

10. Your proposed Future Steps on the next 'Staircase' of improvements:

Step1: Why:.....

Step2: Why:.....



What are you planning next, e.g. funding and resources to ask for ?

Cevn

Open Discussion

Ade

What are the biggest challenges?

What are the big successes?

How can we help others?

What more is needed?

What did you learn?

Biggest risks?

Why?



Thanks and What's Next....>>>>>>... ????

- What did you learn?
- How can **you** improve **your** security?
- What are you going to do next?
- Do you need help?
- **Vibert Solutions look forward to being on YOUR Security A-Team.**

Now you are...

The InstMC/SPE Guardians of The Galaxy !

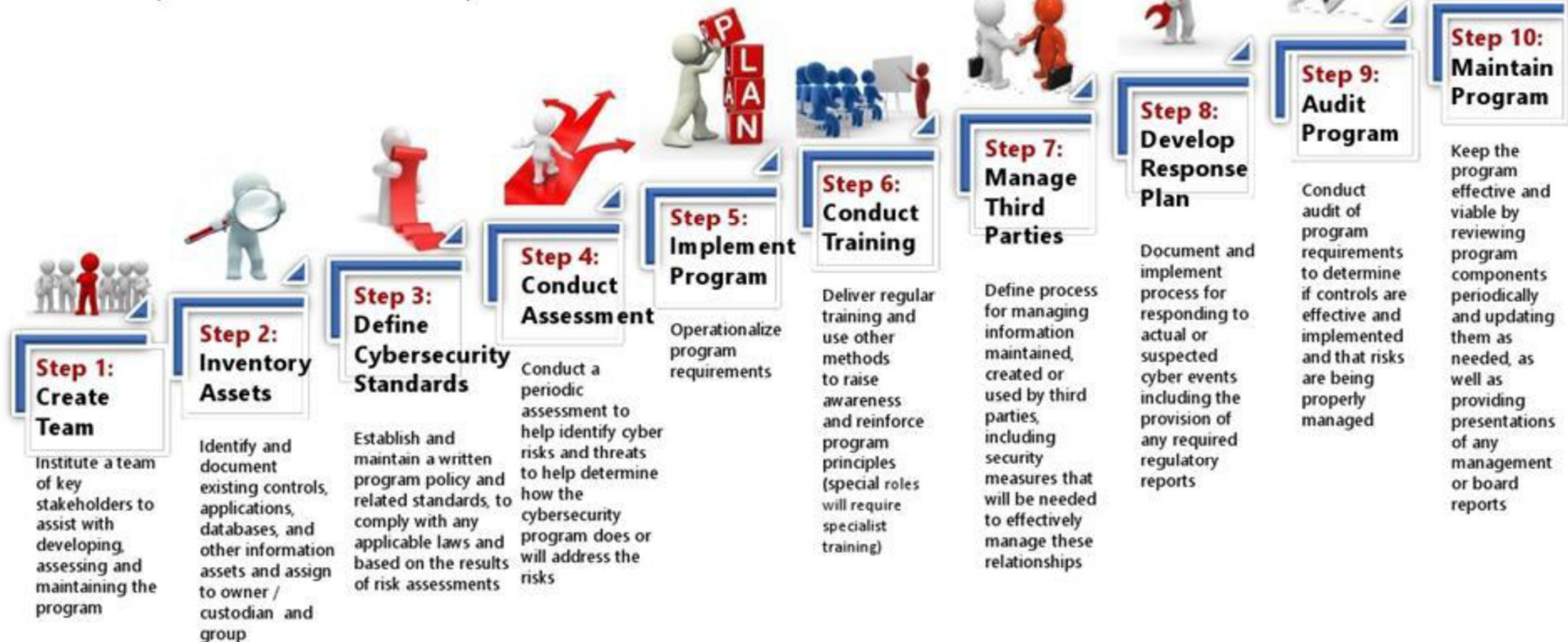




10 Steps to a Cybersecurity Program



Defining and maintaining your Cybersecurity Program is central to your company's overall cyber strategy. This program is contingent on the completion of the 10 steps described below.



© ed.2017 Policy Patty Toolkit. All rights reserved. More information on the toolkit is available at www.policypatty.com.





VIBERT SOLUTIONS

The Cyber Security Alliance to create the new UK Cyber Council



Associations, professional bodies and organisations that today support the majority of cybersecurity practitioners in the UK together to advance:

Progress professional support, and clear guidance for people interested in cybersecurity

Opportunity to raise standards, good practice and understanding of cybersecurity imperatives, and assure

Impact on the digital transformation of our economy

New UK Cyber Council is DCMS and NCSC Funded for a body towards Chartered Cyber Professionals



Vibert Solutions

What has Vibert Solutions Ltd. done?



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 Infineum GSOC solution.

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



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



Assistance was provided for industrial cyber security go-to-market strategies, website, marcoms and industrial cyber security market knowledge.



VIBERT SOLUTIONS



Assistance was provided for industrial cyber security expertise.



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.

A Company

The Business Challenge

Company 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 Company 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 company solution.

Vibert Solutions