



Practical Industrial Cyber Security Improvements.

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

Vibert Solutions

Vibert Solutions Ltd.



VIBERT SOLUTIONS



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, MIoD
- 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.



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



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



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



VIBERT SOLUTIONS

UK 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

Vibert Solutions in the industry ?



Award-winning Consultancy

Vibert Solutions Limited is a Winner!

“Best Cyber Security Advisory Firm 2017 – UK”

GDS Cybersecurity Awards 2017 by GDS-Review

Vibert Solutions Limited has been crowned:

Best Industrial Cyber Security Consultants 2019

Awards by Acquisition International



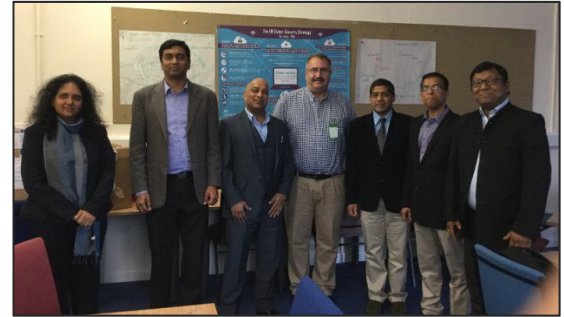
Cyber
Cevn



Analyst
Cevn



Community
Cevn





© Katelee Arrowsmith/SWNS.com/MailOnline

Nuclear

Cyber



Manufacturing

Security



ALES



VIBERT SOLUTIONS

Vibert Solutions

Vibert Solutions - recent successes



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.

THALES

Assistance was provided for industrial cyber security expertise.

Prominent UK Asset

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

Maritime Workshop

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

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.



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.



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 IISCP 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.

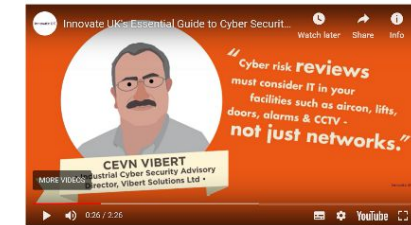
My session will highlight both alerts and advice for end-users of automation and control systems (ICS/OT), as well as selected advisory notes for practitioners of Industrial Cyber Physical Security. Strategic methodologies and programmes of activities for mitigation of impacts on IIOT, IOT and how holistic 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.

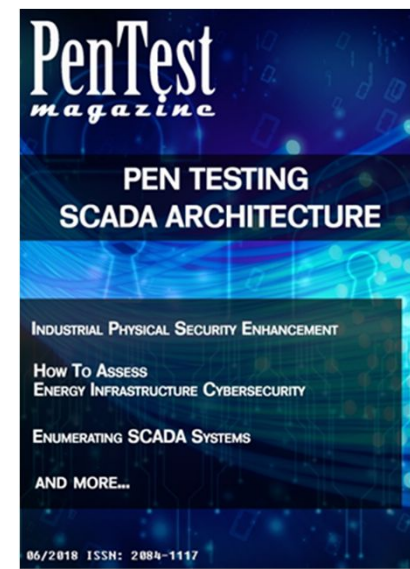


Identify All Possible Threats

"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/>



Hands Up !!

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

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



Information and Systems Cyber Security

Threats

"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



The IT World





16% of IT professionals admit to still running Windows XP and Windows Vista on some of their machines

43% of enterprises are still running Windows 7

15th Jan 2019 www.helpnetsecurity.com

Windows 7 is still popular, with 36% of all PCs in active use still running it, not far behind the 43.6% running Windows 10.

AV-Test.org registered 67.7 million new strains of Windows malware during 2018

1st Oct 2019 www.itpro.co.uk



Cyber Attacks are increasing because...???

LinkedIn breach affected around 117 million.

MySpace breach exposed 427 million users.

Tumblr data breach exposed 65 million accounts.

VK.com security breach exposed 93 million accounts.

DropBox security breach exposed 69 million accounts.

Verizon exposed 14 million records,

BellCanada breach 19 million records,

Edmodo breach 77 million accounts,

Equifax breach 143 million accounts

$$117M \times \$2.50 = \$300M$$
$$427M \times \$2.50 = \$1B$$

££££££££

Hacked sell price.

iTunes	\$8
Groupon.com	\$5
GoDaddy.com	\$4
Facebook	\$2.50
Twitter	\$2.50



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 Industrial IT World

Safety == Security



LIVE

Could it happen??

BREAKING NEWS

MASSIVE CYBER ATTACKS

12:49

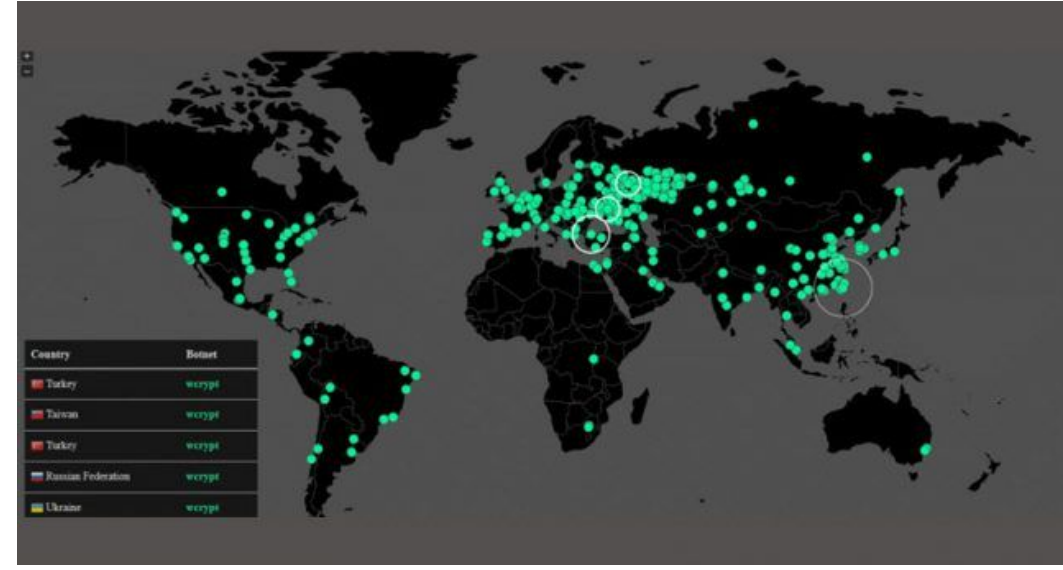
CRITICAL NATIONAL INFRASTRUCTURE DISABLED BY CYBER ATTACKS



In previous years we were missing **Stories** relevant to Industrial Cyber But now..

DroppingElephant Norsk Hydro LockerGoga
 Triton
 DragonFly Equation Shamoon StoneDrill CrouchingYeti Industroyer DarkHotel
 wiper Carbanak KillDisk Andromeda ShadowBrokers
 WannaCry

Petya
 Turla
 NotPetya
 BlackEnergy
 Ukraine1
 Ukraine2
 BlackEnergy2



Havex
 Mirai
 Gaus
 Zeus

Dallas Emergency Sirens Kemuri Water EnergeticBear / CozyBear PetulantPenguin
 German Steelmill Flame
 NightDragon Slammer and Conficker Worm
 RedOctober Maersk Duqu Agora+ for Canvas and Metasploit
 Aurora Test Vibert Solutions



Industroyer is modular, allowing attackers to customise the malware to their needs. ESET's analysis of it revealed four separate payloads which, when deployed, map the networks and issue commands, communicating with specific protocols used by its target: (IEC 60870-5-101, IEC 60870-5-104, IEC 61850, and OLE for Process Control Data Access) - SC Magazine

WannaCry ransomware attack has affected more than 200,000 systems in 150 countries around the world

Petya/NotPetya/Nyetya/Goldeneye

A month or so after WannaCry, another wave of ransomware infections that partially leveraged Shadow Brokers Windows exploits hit targets worldwide. This malware, called Petya, NotPetya and a few other names, was more advanced than WannaCry in many ways, but still had some flaws, like an ineffective and inefficient payment system.

Though it infected networks in multiple countries—like the US pharmaceutical company **Merck**, Danish shipping company **Maersk**, and Russian oil giant **Rosnoft**—researchers suspect that the ransomware actually masked a targeted cyberattack against Ukraine. The ransomware hit Ukrainian infrastructure particularly hard, disrupting utilities like power companies, airports, public transit, and the central bank, just the latest in a series of cyber assaults against the country.

Wired Magazine

94% of security professionals expect IIoT to **increase risk and vulnerability** in their organizations – Tripwire

TRITON malware proven able to damage or shut down **safety instrumented system (SIS)** controls designed to prevent industrial equipment failure or catastrophic incidents such as explosions or fire. – SC Magazine



A recent Kaspersky survey has discovered that two-thirds (67%) of industrial organizations do not report cybersecurity incidents to regulators.

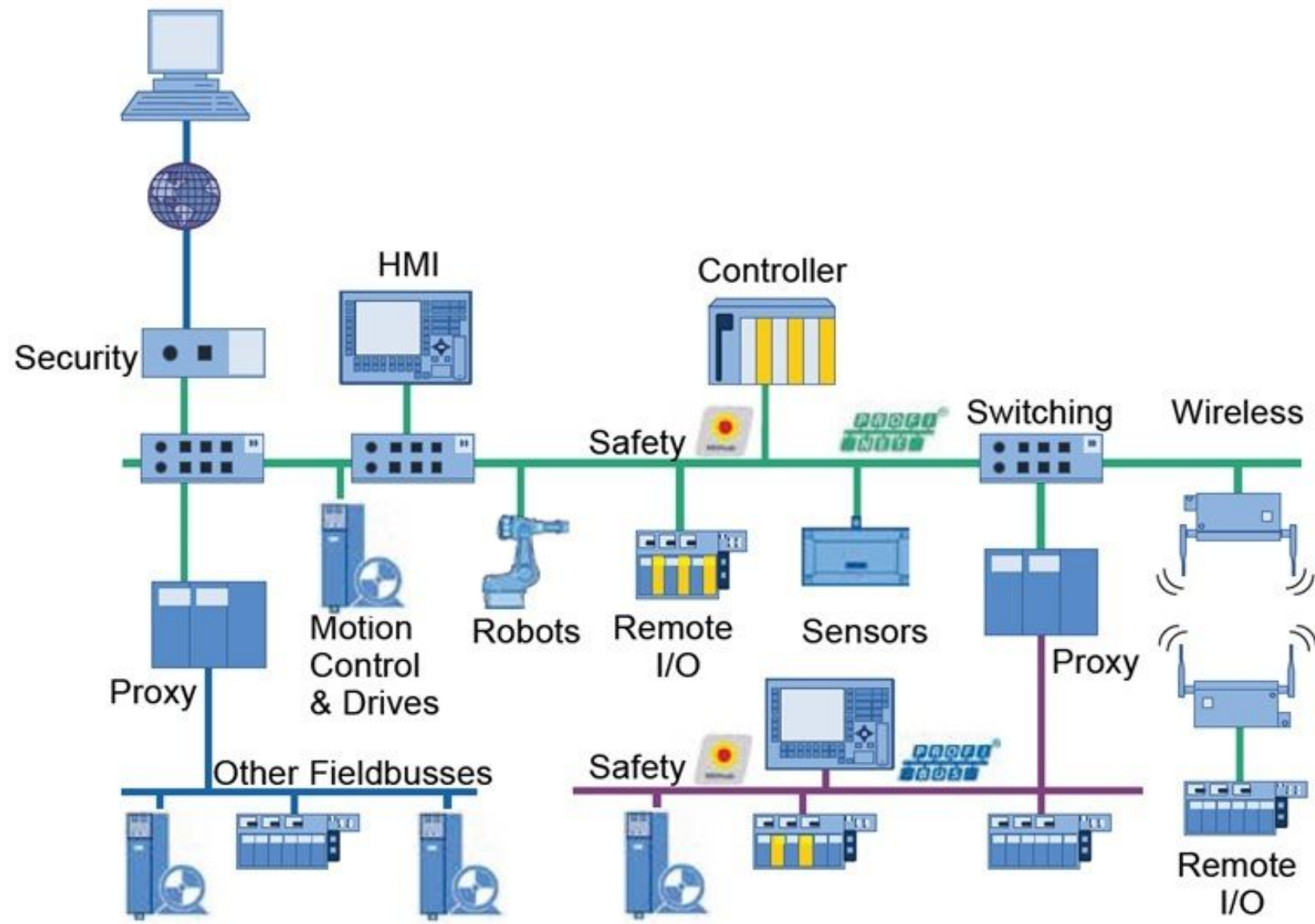
..only a fifth (21%) of industrial companies admitting that they do not currently comply with mandatory industry regulations

..more than half (52%) of incidents lead to a violation of regulatory requirements, while 63% of them consider loss of customer confidence in the event of a breach as a major business concern.



Industrial IT System Architectures

Example industrial network



TI-E2E

The Industrial World..... vendor examples



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

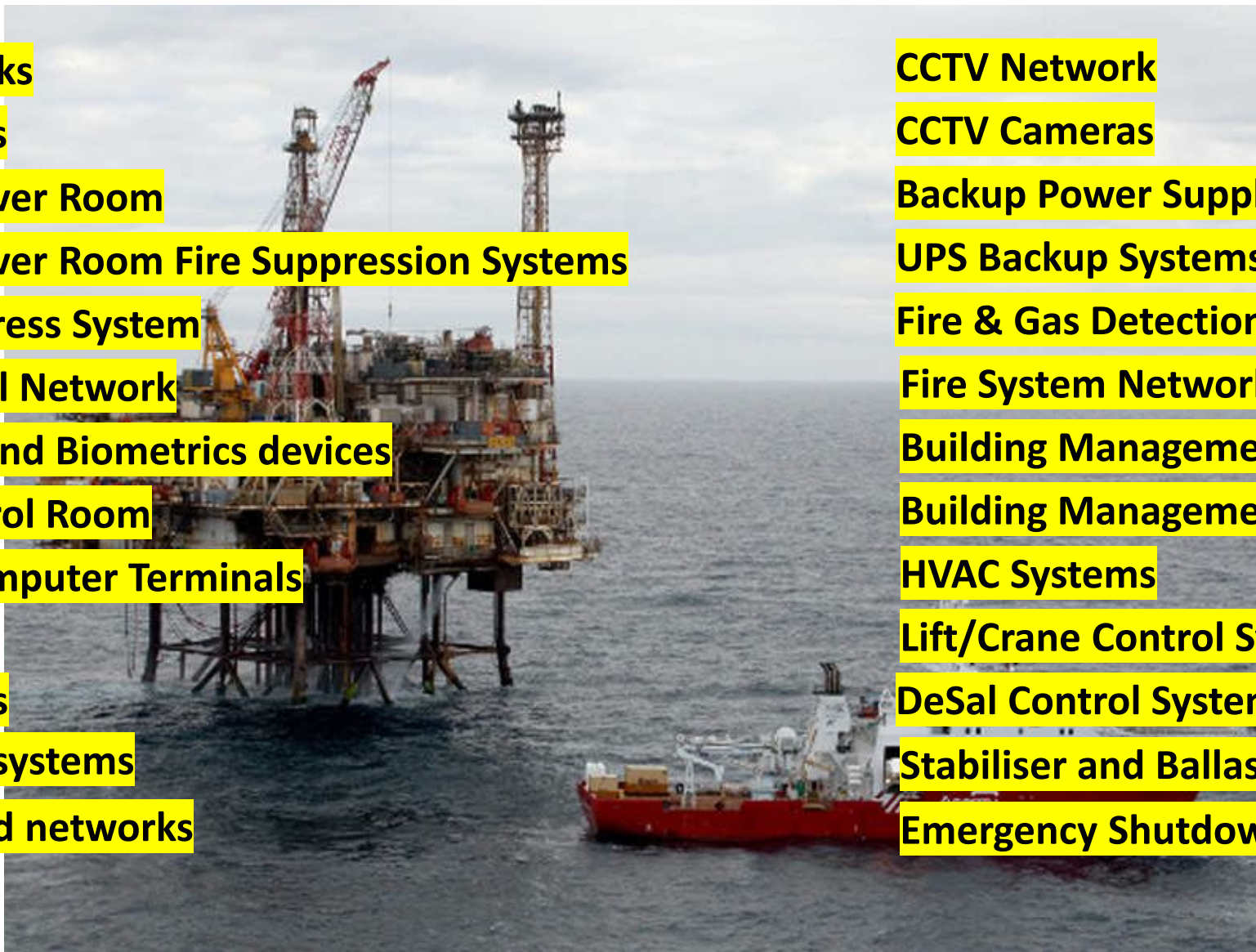
HVAC Systems

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



Exploits – now easier to use

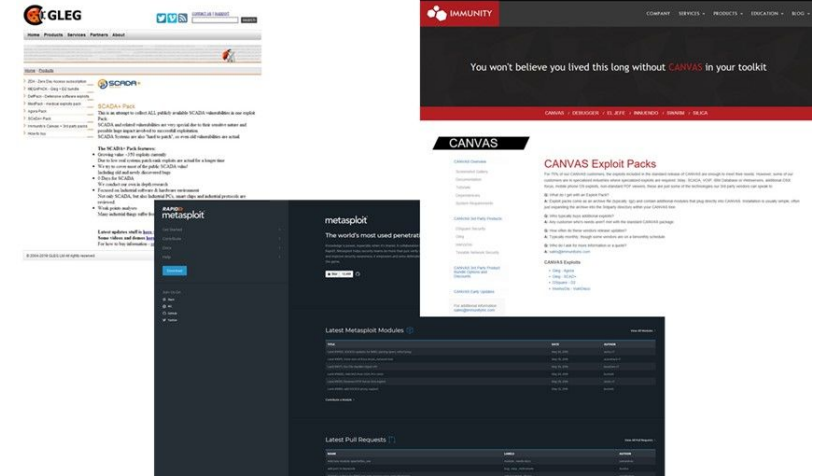


Is your site listed on **SHODAN**?.....
Are your trusted suppliers listed?.....



“Compromise Wizard App”
The New Super-Simple Targeting App..... ?
Ad-Free!

..... *Is this the future?*



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.**

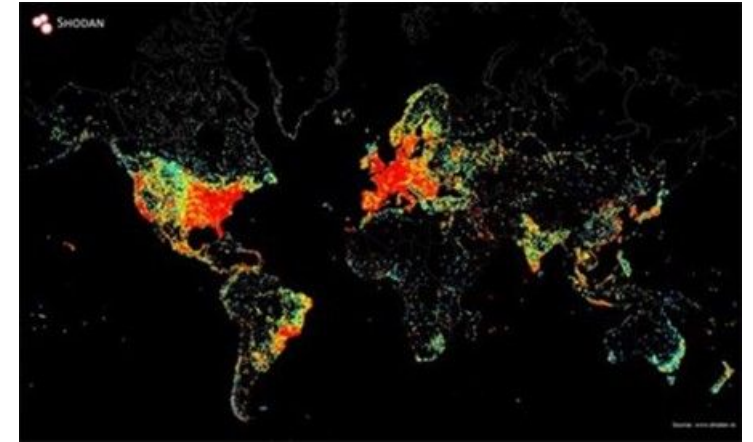
Fact: Increase of hackers specifically attacking you due to kudos of accomplishment.

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

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

IEC 62443 ANSI/ISA IEC Cyber Security Standard for Industrial Automation and Control Systems (formerly ISA99)

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.....



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

Wave the Flags. Socialise.
Enjoy. Promote.

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**



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

HSE OG86

ISO27001

IEC62443

ANSSI

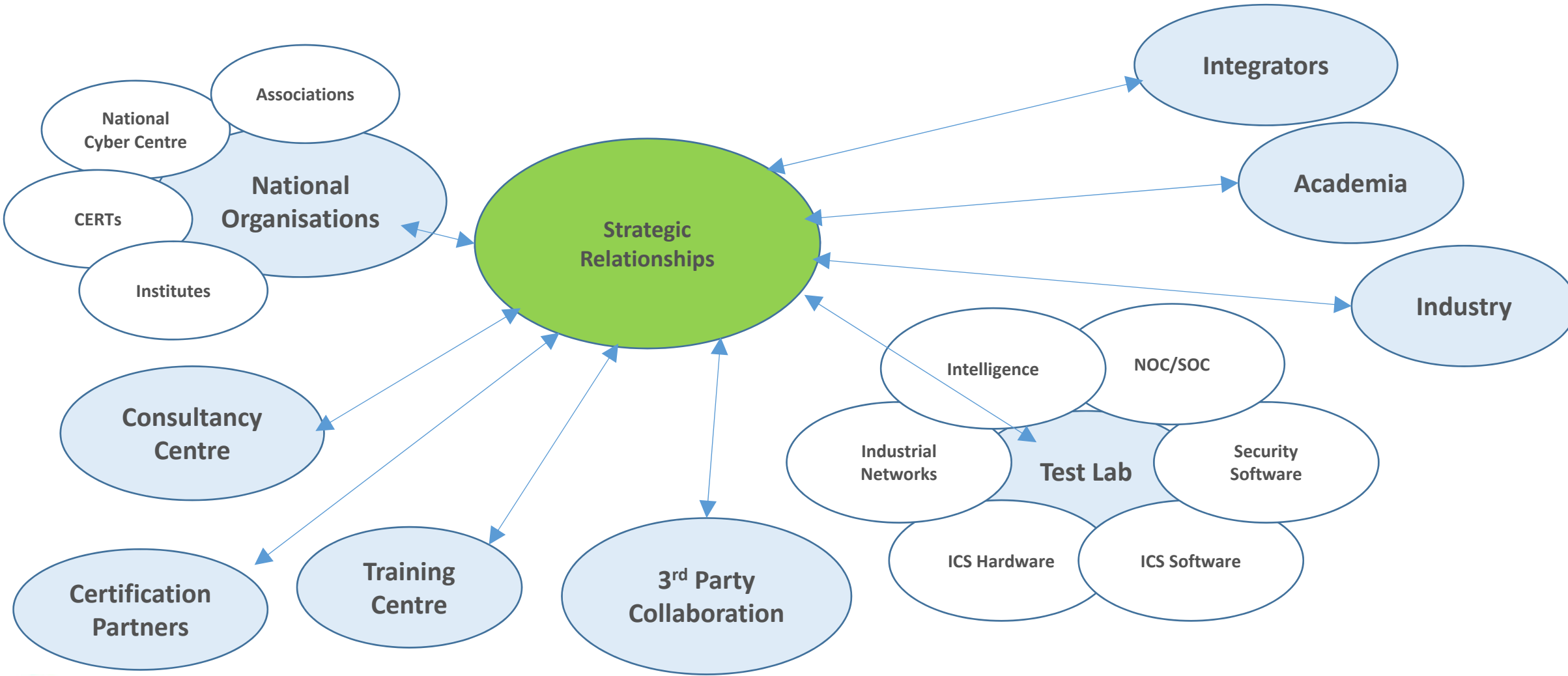
BS31111

Cyber Essentials

Cyber Essentials+

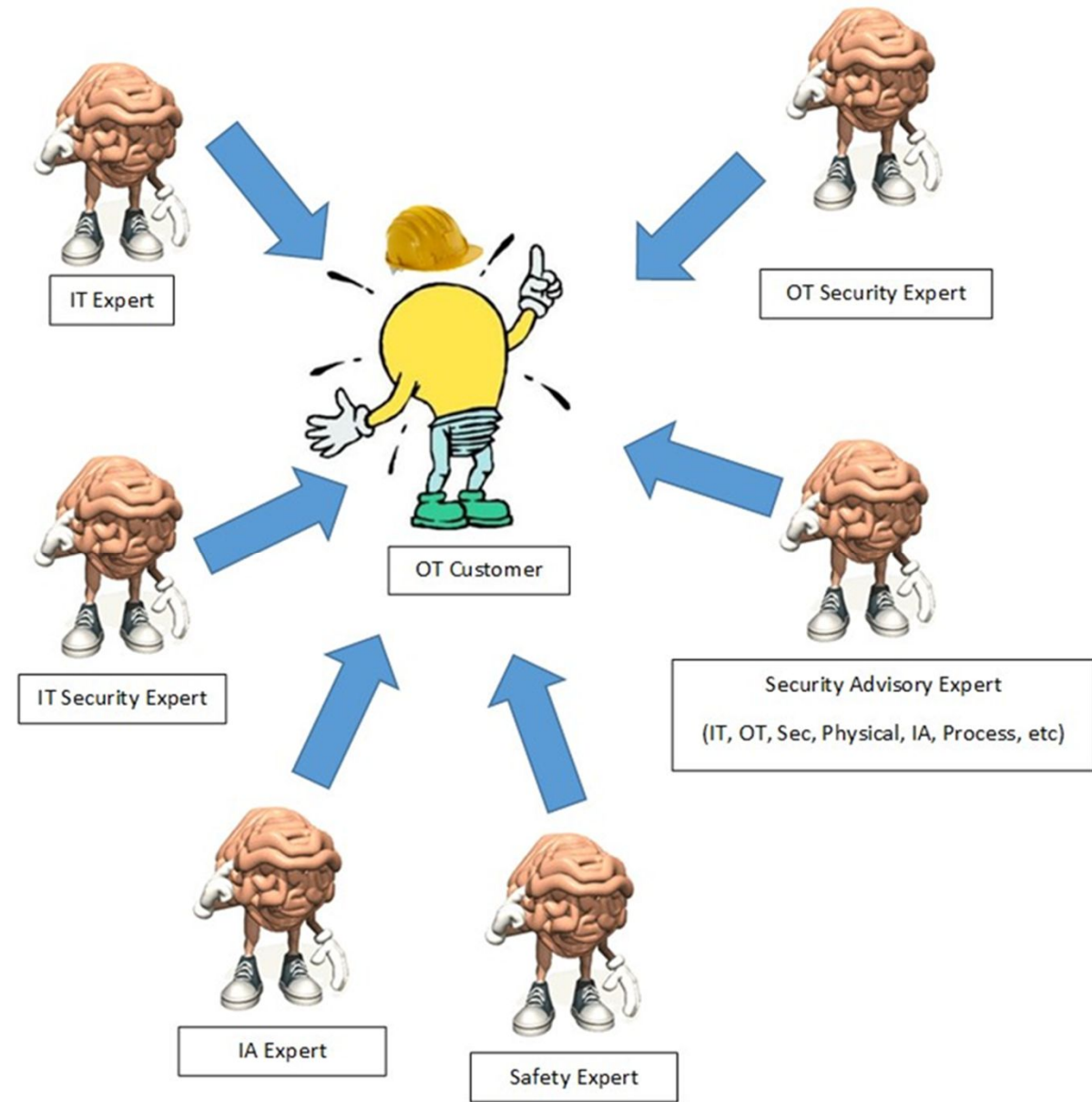


Strategic Relationships



The A-Team

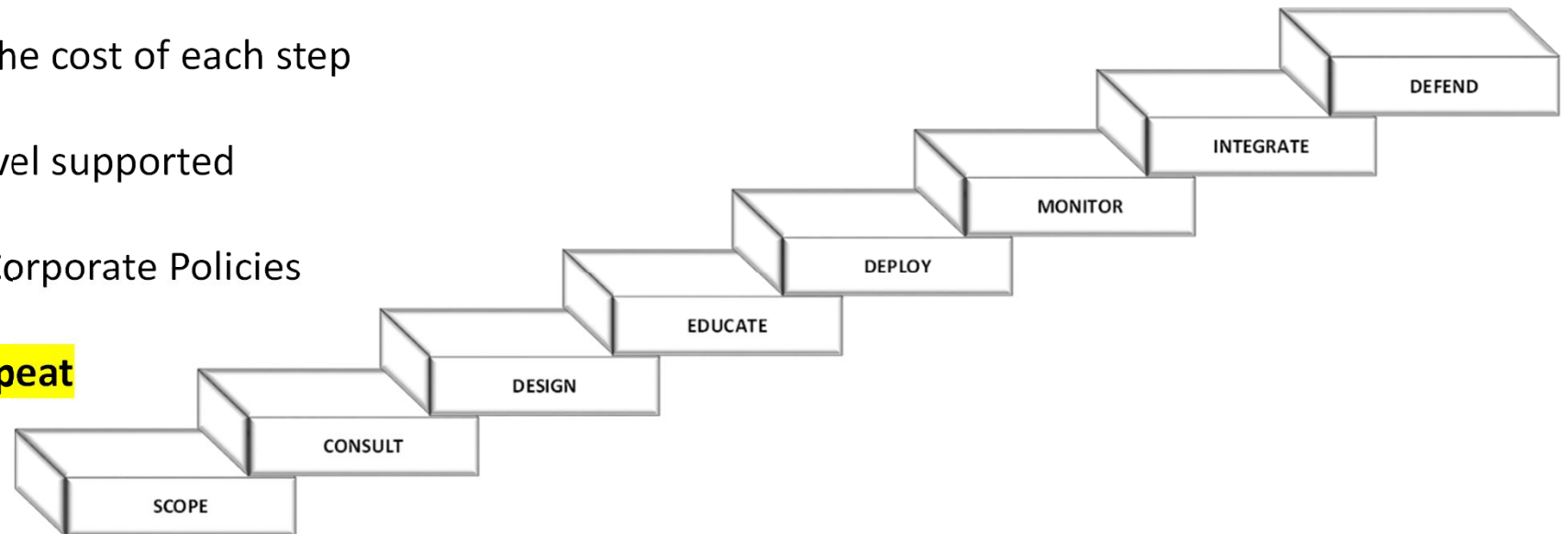
- The Team is the core
- Multi-role people
- Champions (social)
- Champions (technical)
- Financial budget holders
- Key decision makers
- Internal and External members
- Success is not simple



The Staircase

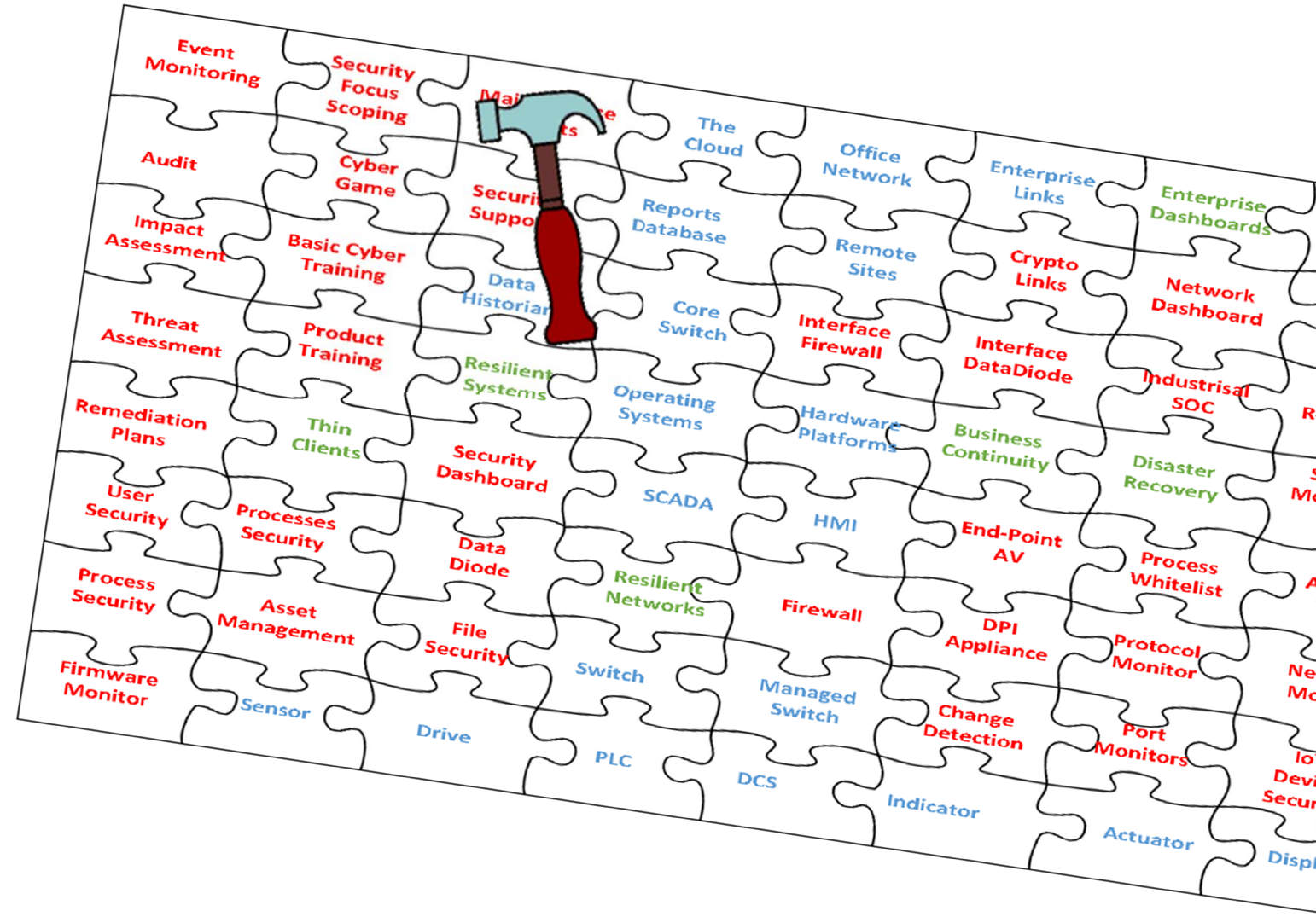
The Staircase

- 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.

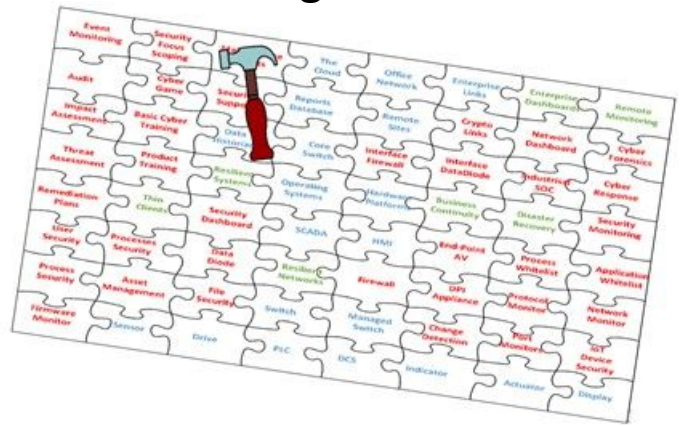


Security Methodologies Summary

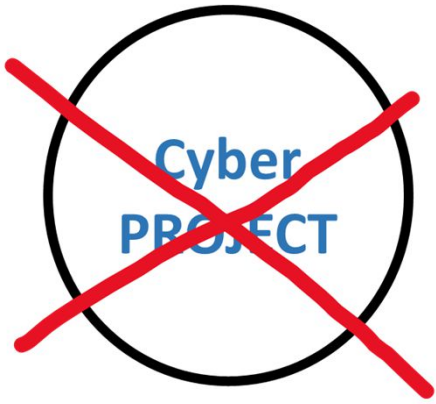
Audits



The Jigsaw

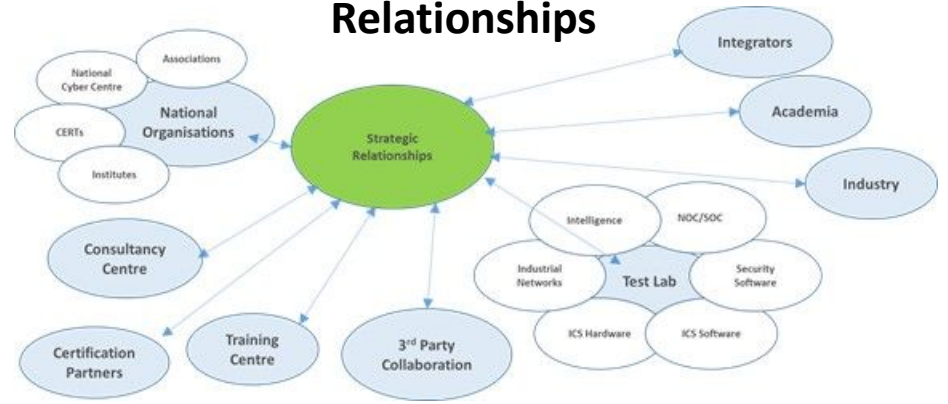


Lifestyle not Programmes & Projects

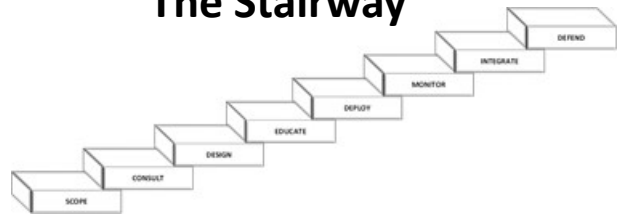


Lifestyle

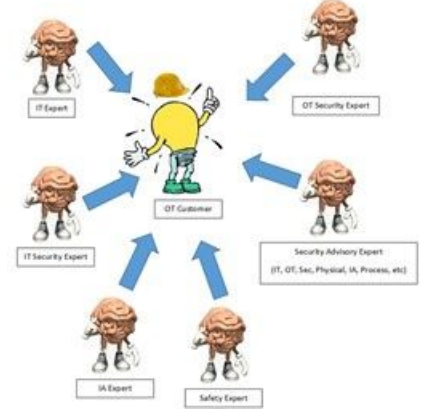
Relationships



The Stairway



The A-Team



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

SECURITY
101

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



Expert Books and Articles



Expert Websites



Raising Awareness Sharing Experience Cyber Games Basic Mitigations

Educational Games



'Threats
/Risks/
Impacts'

'Profitable
Business
Operations'

SECURITY 101



Predictions from 2017...2018..2019...

- Disclosing Attacks becomes mandatory. ✓
- Nation-State Alliances form. ✓
- Cyber and Safety no longer in silos. ✓
- Supply-Chain security mandatory. ✗
- ICS Cyber Insurance becomes “real”. ✗
- The Kaspersky 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. ✓



Industrial Cyber Security Capabilities



VIBERT SOLUTIONS

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



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

Vibert Solutions in the industry



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



Vibert Solutions

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?
- Vibert Solutions look forward to being on YOUR Security A-Team.

Join the SIG !

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)