



Advances in Process
Automation and Control 2019

18 – 20 November 2019, Manchester, UK

Inst
MC



VIBERT SOLUTIONS

Practical Industrial Cyber Security Enhancements

Tues 19th Nov. 2019 30mins 14:30pm - 15:0pm

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



- 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....



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

Content hub Building up the defence


ARTICLE

14 Mar 2019 5 min read

EMAIL SHARE TWEEET SHARE SHARE

Building up the defence

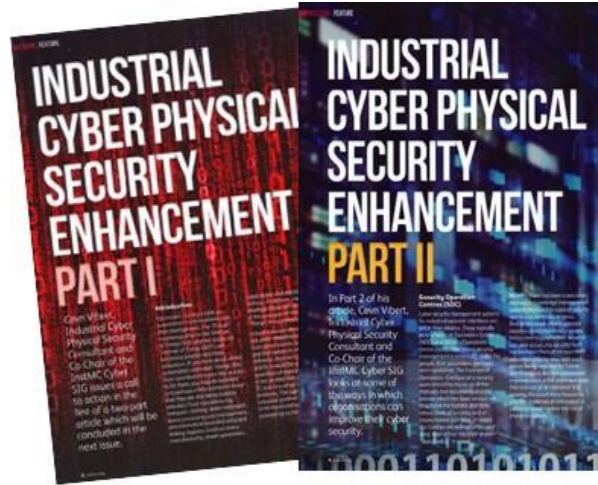
The cyber physical bad guys are now attacking internet of things (IOT) and the industrial internet of things (IIOT), says Cevn Vibert, Industrial Cyber Security Consultant and Educator. As the bad guys get better and better at attacking, so we must constantly get better at defending. There is evidence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



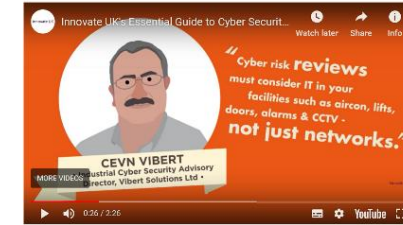
Our modern society is built on automation, control systems and their management. The things mentioned often in the internet of things (IOT) and the industrial internet of things (IIOT), are becoming smarter and more ubiquitous. If you think about all the automation-controlled things that have contributed 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

Recent Papers



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



BCS

(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 [IS/CP 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 IOT, IIOT 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.

ISC2

InstMC

Tripwire



PenTest Mag

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.



Chair of the **Institute of Measurement and Control's**
Industrial Cyber Special Interest Group

Join the SIG!



Department
for Culture
Media & Sport

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



CIPD

CompTIA



VIBERT SOLUTIONS



The UK Cyber Security Alliance to create the new UK Cyber Security Council



Vibert Solutions

OT ICS Cyber Security Activities



VIBERT SOLUTIONS

- 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**.....



VIBERT SOLUTIONS

Vibert Solutions



Hands Up !!

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

Who, in your organisation, is personally responsible for 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





TRW

**“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

117M x \$2.50 = \$300M

Account 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



Investments

The National Cyber Security Centre is part of GCHQ and aims to **make Britain the safest place to live and work online.**



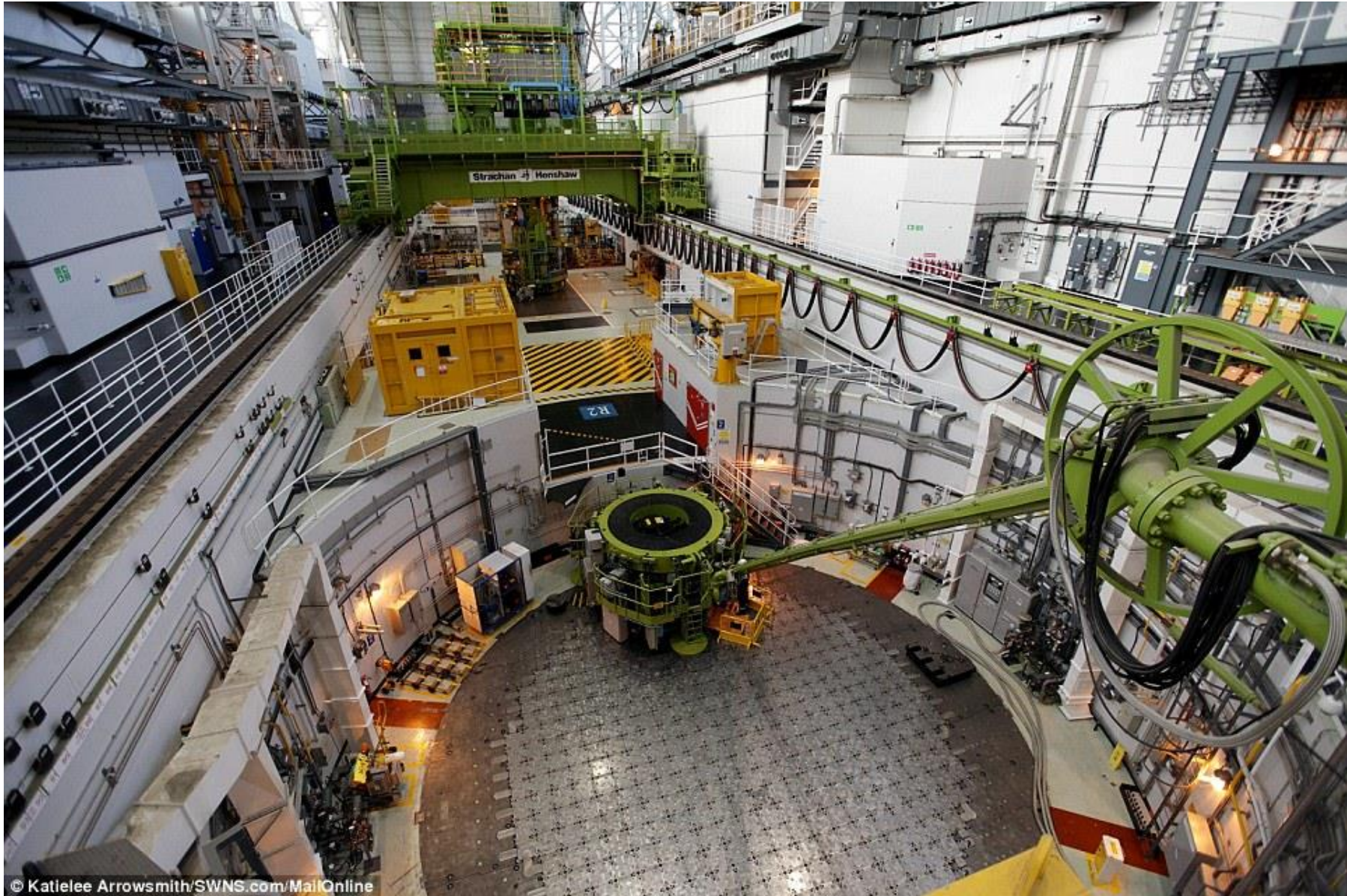
NCSC has defended the UK against more than 600 cyber attacks in the past year – bringing the **total number to almost 1,800** – significant number from Nation States.



The Industrial IT World

Safety == Security





© Katielee Arrowsmith/SWNS.com/MailOnline



VIBERT SOLUTIONS

Vibert Solutions



© Katelee Arrowsmith/SWNS.com/MailOnline

Nuclear

Cyber



Manufacturing

Security



ALES



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

Triton

Norsk Hydro

LockerGoga

StoneDrill

Industroyer

DarkHotel

DragonFly

Equation

Shamoon

CrouchingYeti

Andromeda

WannaCry

wiper

Carbanak

KillDisk

ShadowBrokers

Petya

Turla

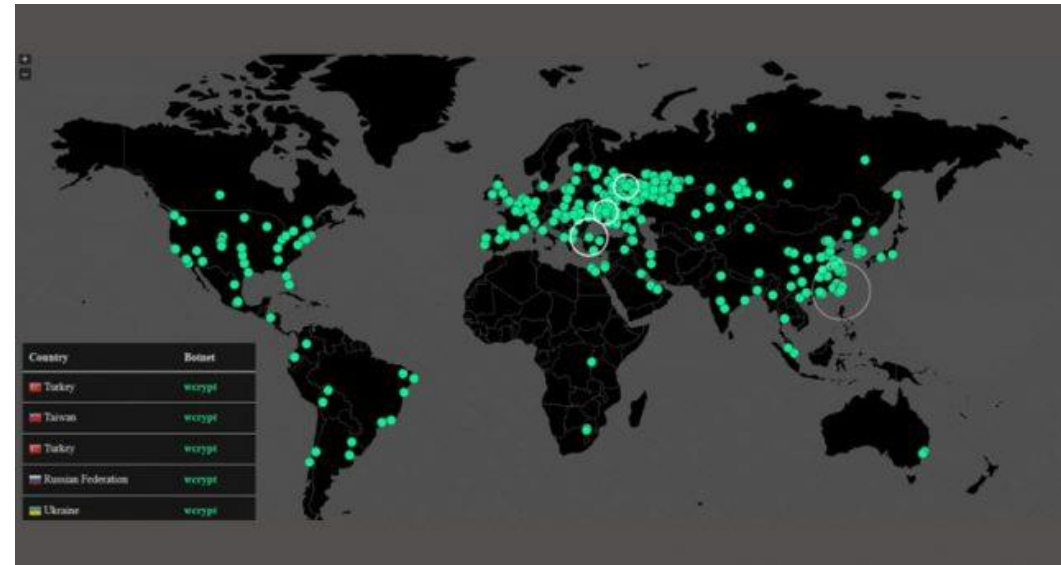
NotPetya

BlackEnergy

Ukraine1

Ukraine2

BlackEnergy2



Havex

Mirai

Gaus

Zeus

Dallas Emergency Sirens

Kemuri Water

EnergeticBear / CozyBear

PetulantPenguin

German Steelmill

Flame

Slammer and Conficker Worm

NightDragon

Maersk

Duqu

Agora+ for Canvas and Metasploit

RedOctober

Aurora Test



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

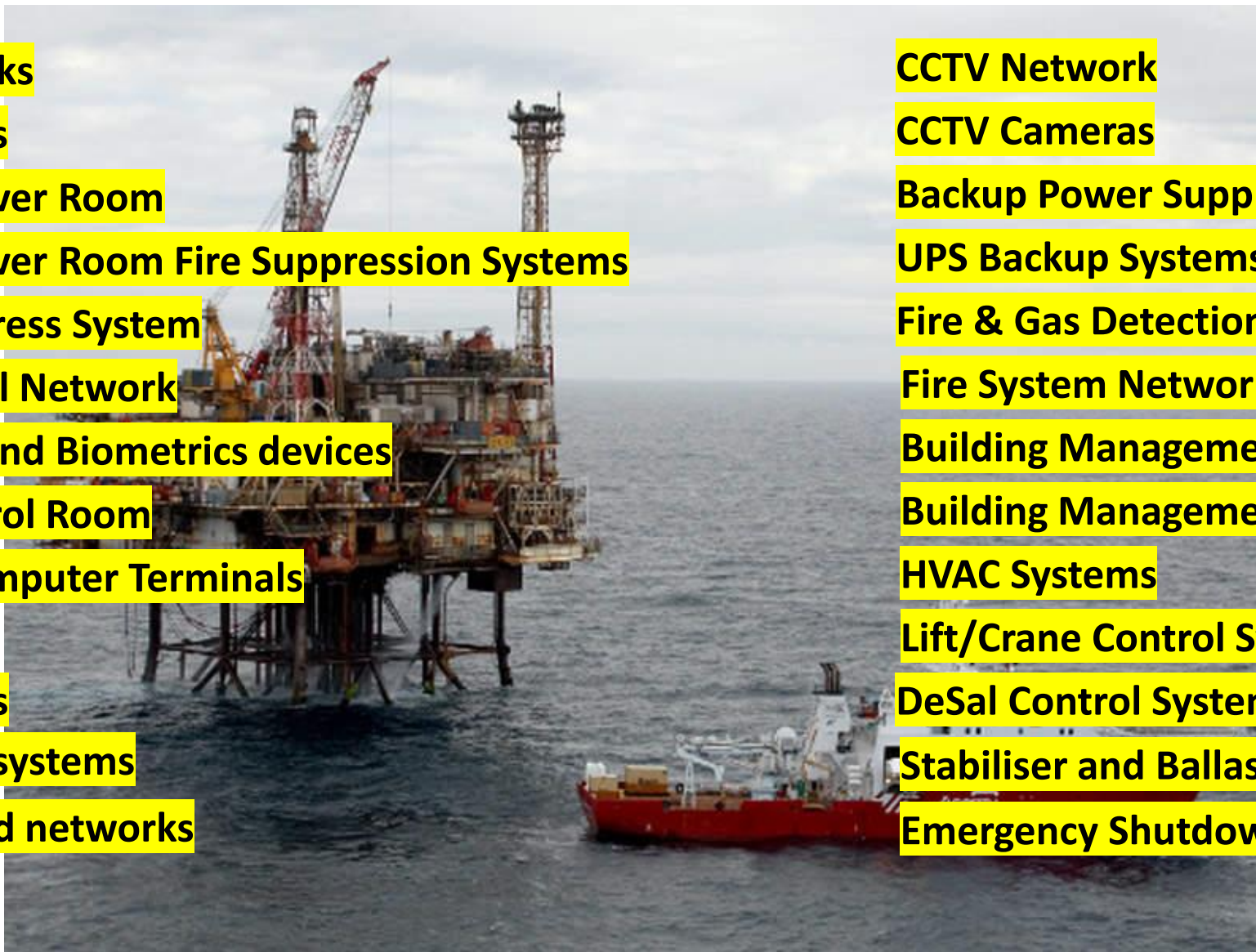
HVAC Systems

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

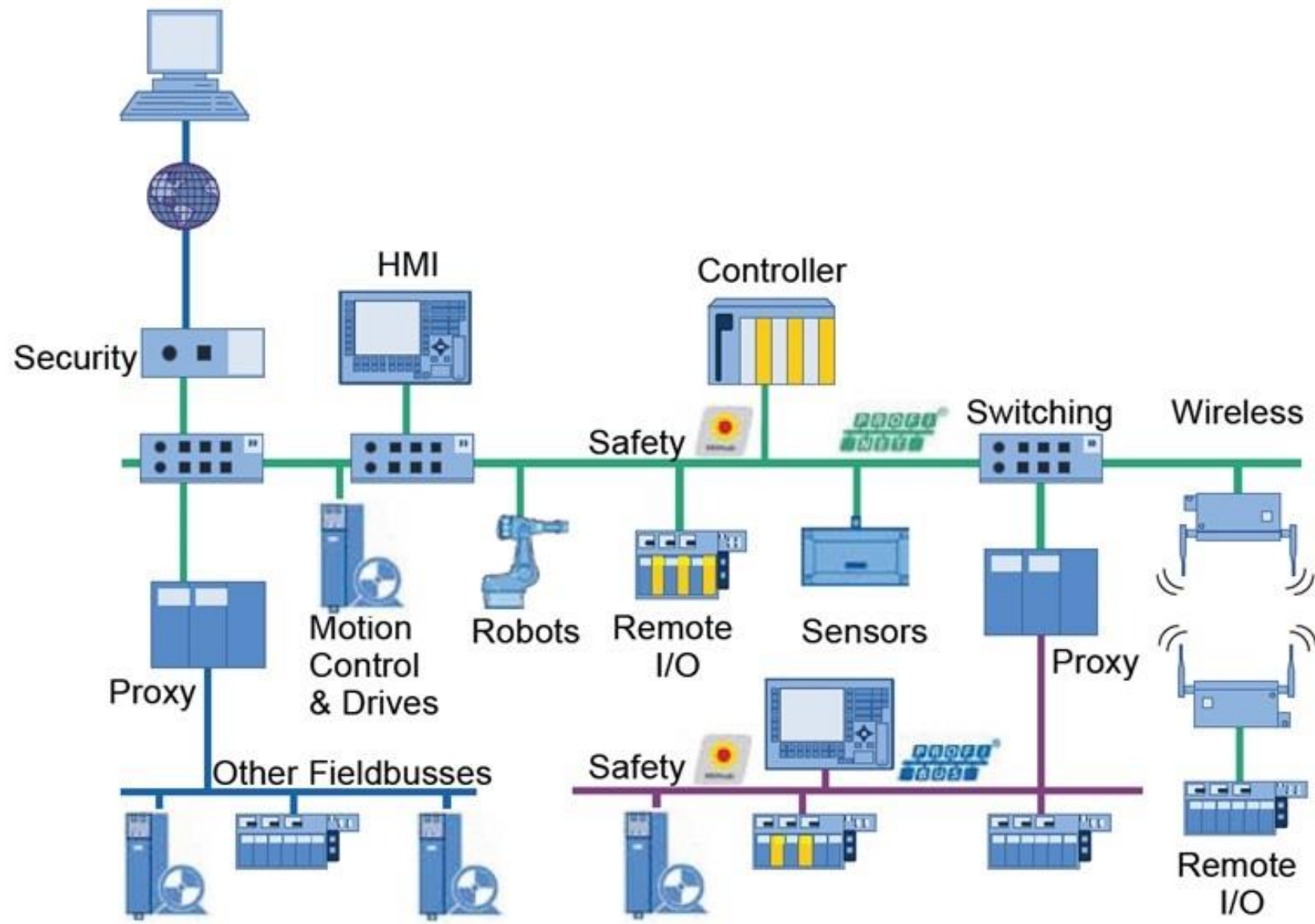
Vehicle Stopper Control Systems

Vending Machines and networks



Industrial IT System Architectures

Example industrial network



TI-E2E

The Industrial World..... vendor examples



Exploits – now easier to use



Is your site listed on **SHODAN**?.....

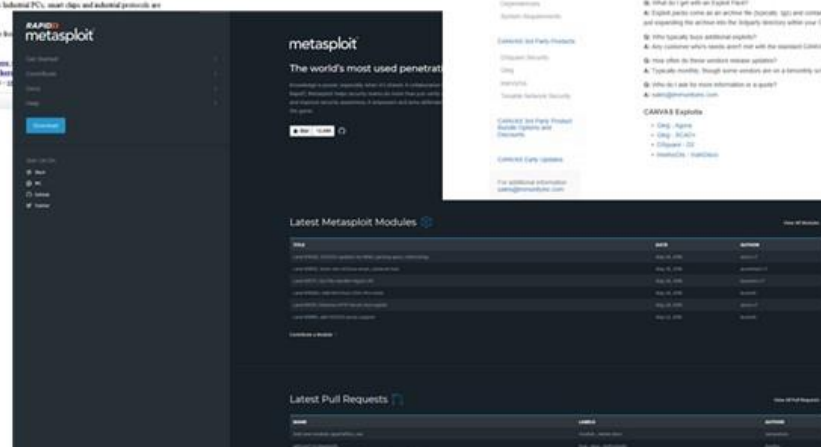
Are your trusted suppliers listed?.....



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

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)

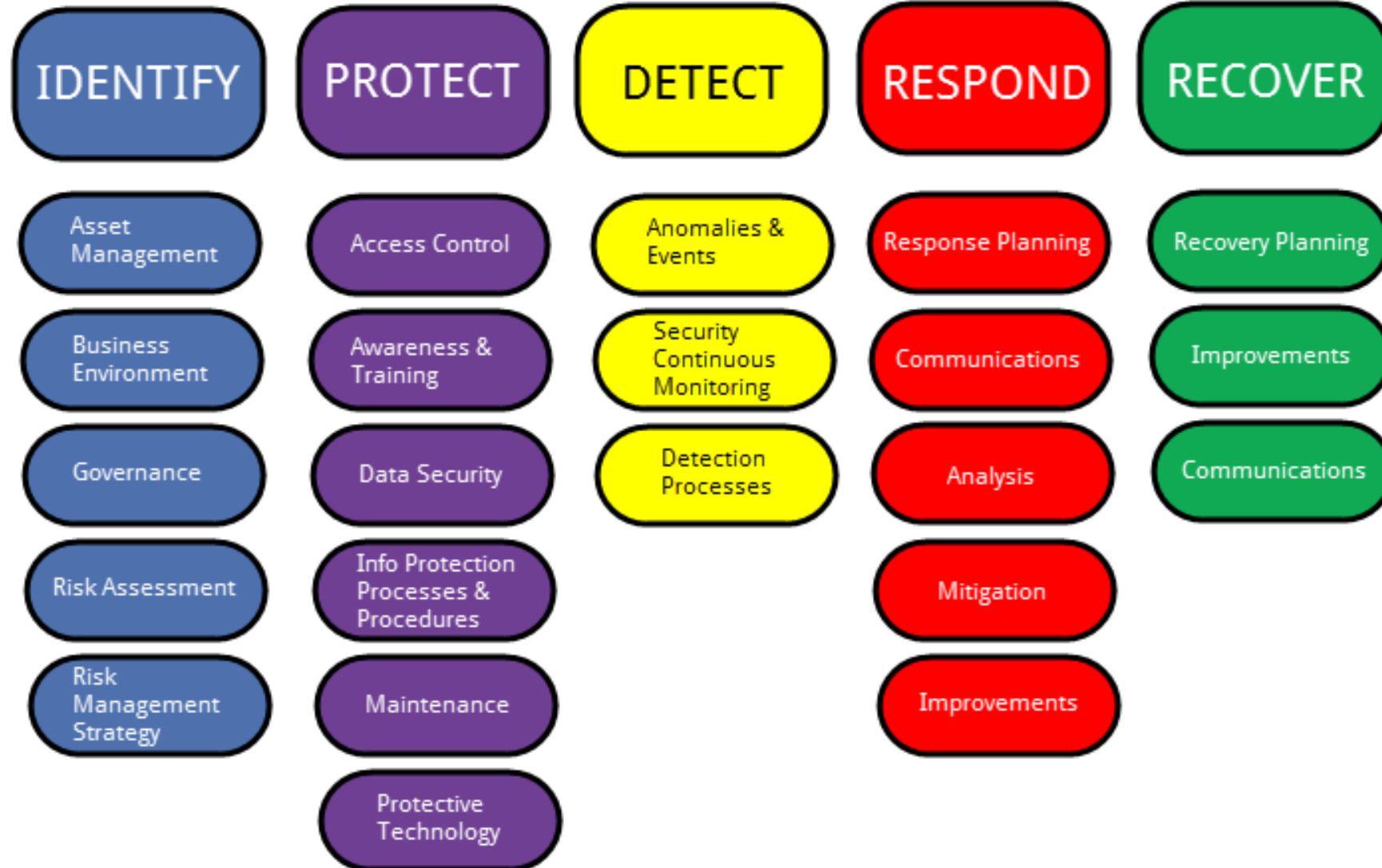
BSI Cyber Security for Information Systems (Germany)

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

....and.. Corporates/Enterprise's own home-brewed standards.....



NIST CyberSecurity Framework



NCSC CAF 3

Cyber Assessment Framework

Objective A: Managing security risk

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

A.1 Governance

Putting in place the policies and processes and approach to the security of network and information systems supporting essential functions.

A.2 Risk management

Identification, assessment and understanding of risk to the network and information systems supporting essential functions, and establishment of an overall organisational risk management approach.

A.3 Asset management

Determining the value of assets and supporting their protection.

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

Defining and communicating appropriate security policies for network and information systems supporting essential functions.

B.2 Identity and access management

Understanding and managing access to network and information systems supporting 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.

Security monitoring

Identifying and tracking potential security problems and track the effectiveness of existing security defences.

Incident discovery

Identifying and tracking potential security problems and track the effectiveness of existing security defences.

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.

Outcomes!



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

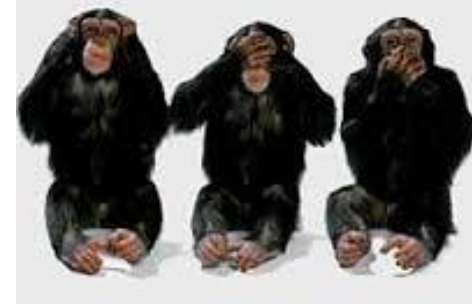
Frameworks, Jigsaw,
Compliance, Best
Practice, Governance

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**

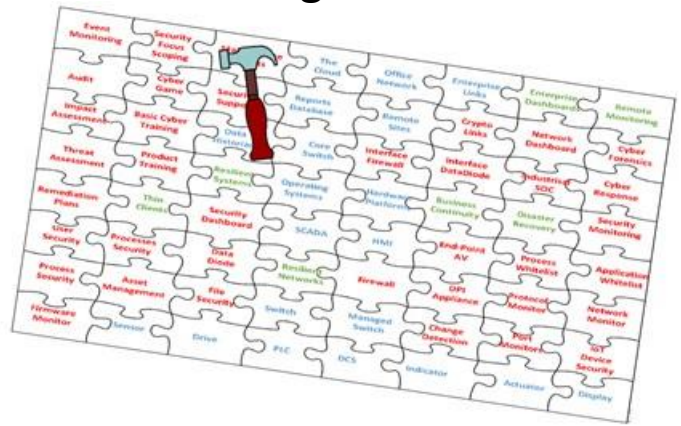


Security Methodologies Summary

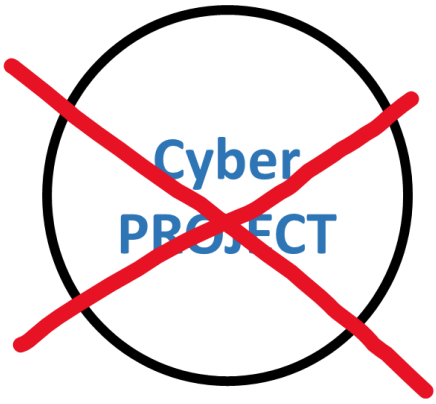
Audits



The Jigsaw

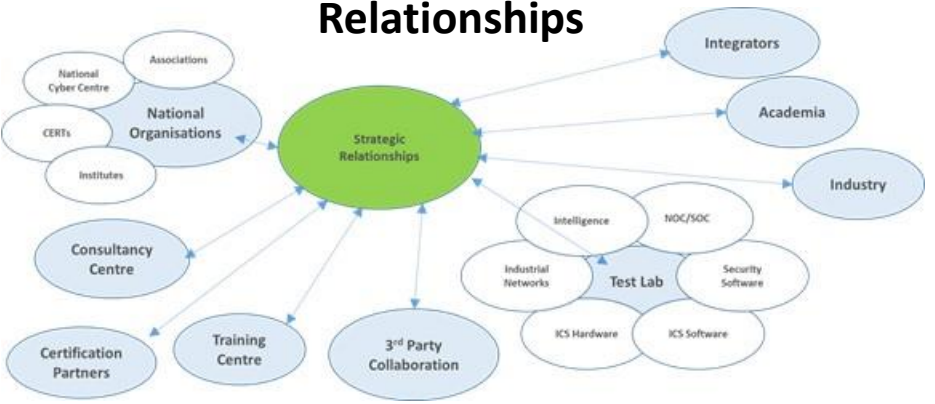


Lifestyle not Programmes & Projects

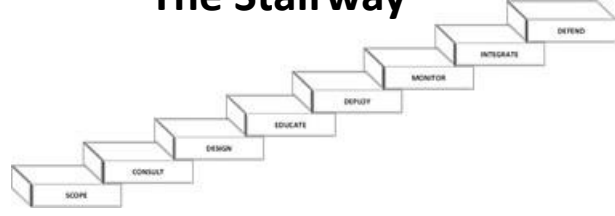


Lifestyle

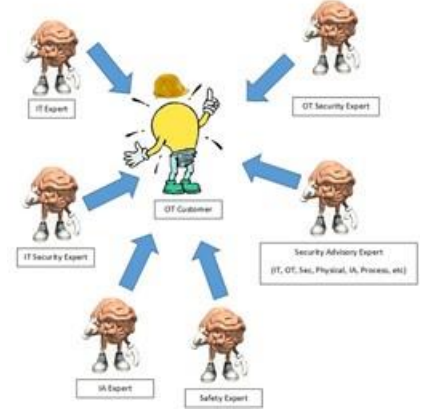
Relationships



The Stairway



The A-Team



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. 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

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 UK Cyber Capability Iceberg

- 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

20

6000



- 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?

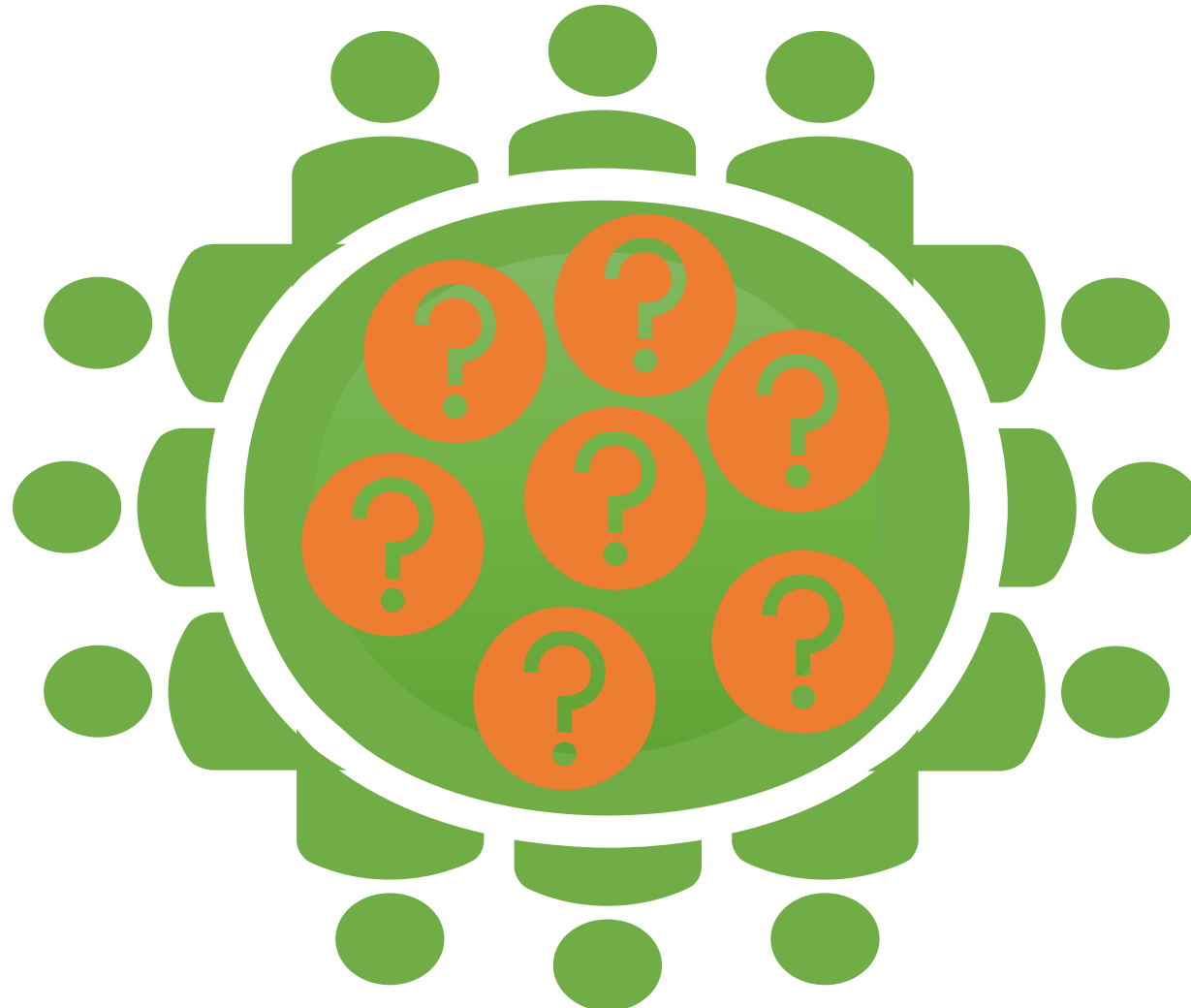
Does the institution have a security strategy?



Round-Table Questions..Questions..Questions...

Chatham House Rules – Non-Attribution!

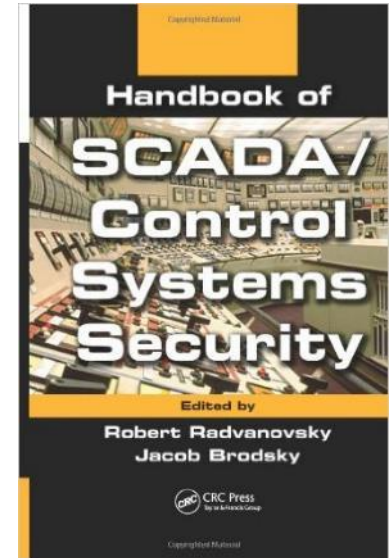
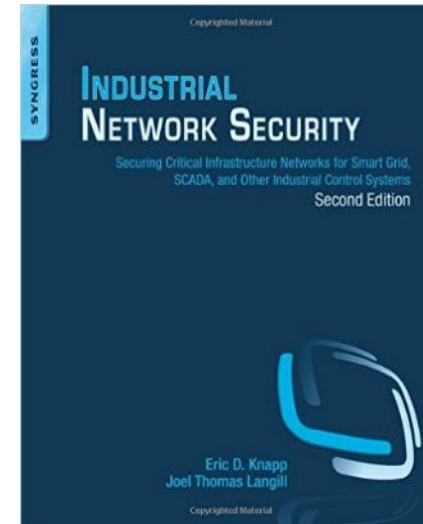
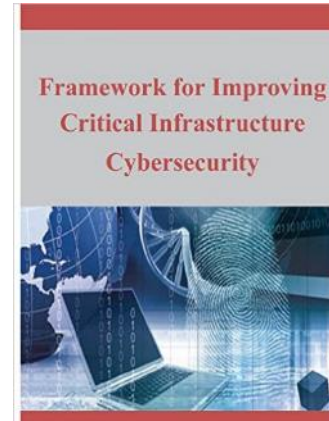
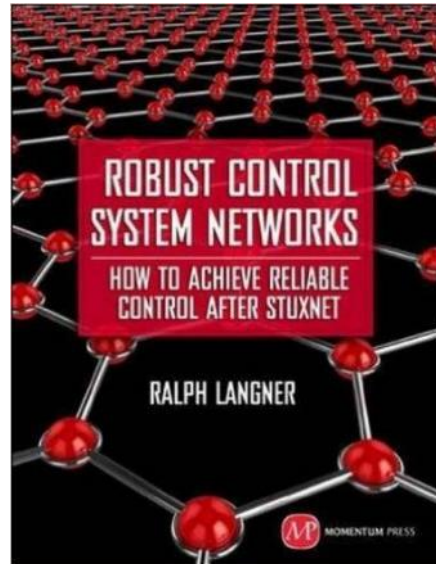
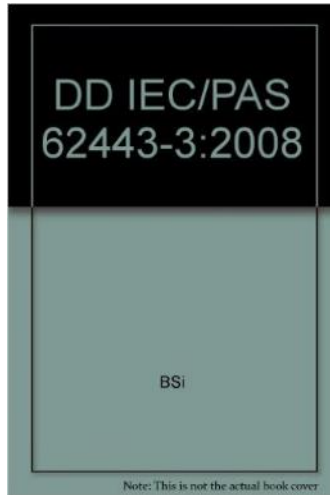
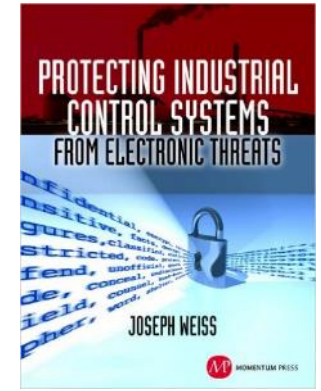
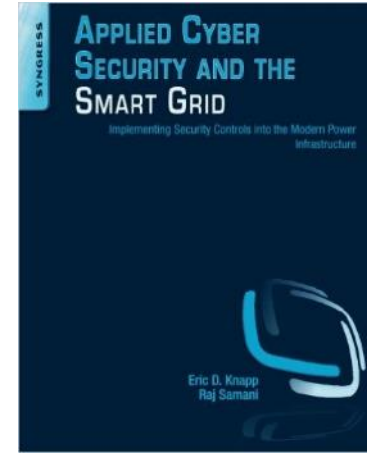
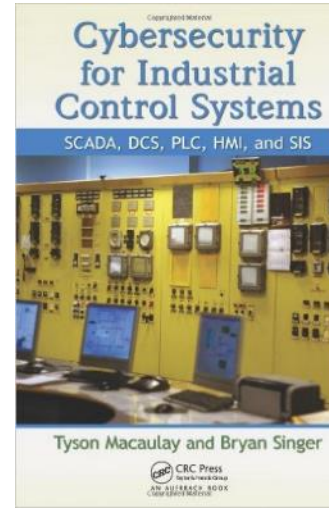
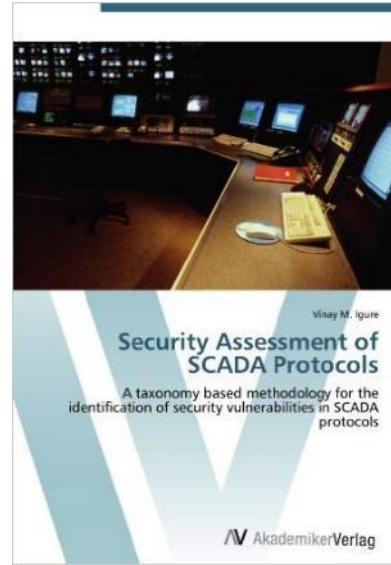
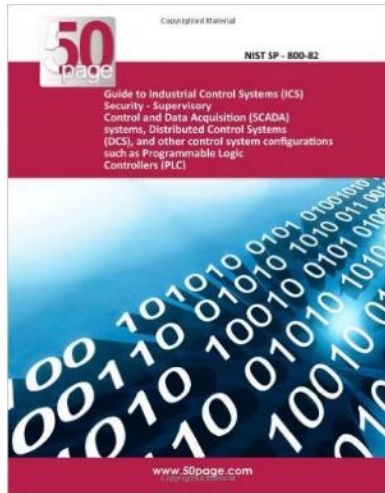
Compliance?
Audits?
Scans?
Surveys?
Briefings?
Workshops?
Training?
Board Advisory?
State of the Nation?
Essentials?
Threats?
Vulnerabilities?
Consequences?
Risks?
Governance?



Policies?
Procedures?
Assets?
Segregation?
UK/EU/US?
27001?
62443?
Tools?
Physical Security?
Wireless?
Gov?
GCHQ?
Certification?
Predictions?
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.

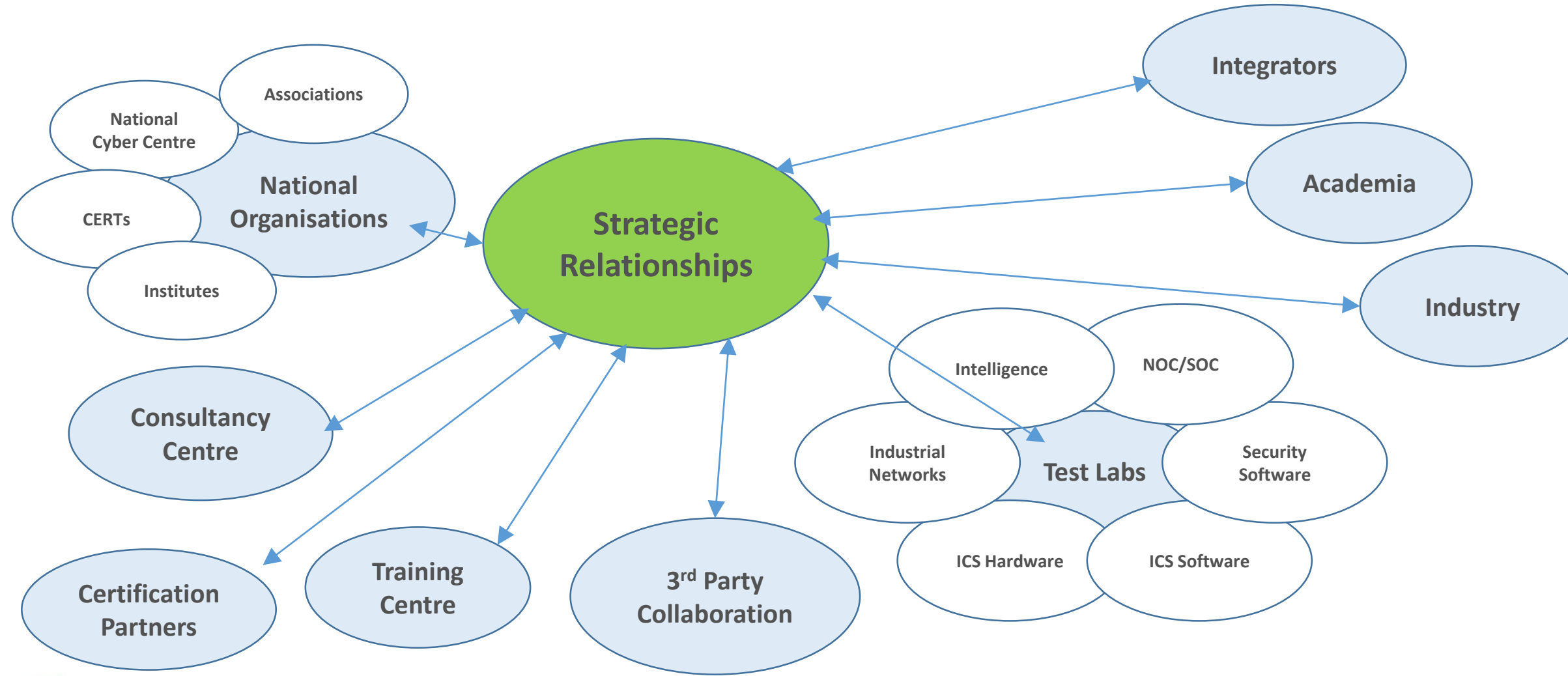
A level of assurance that critical decisions are not

based on faulty information

Accountability for safeguarding information.

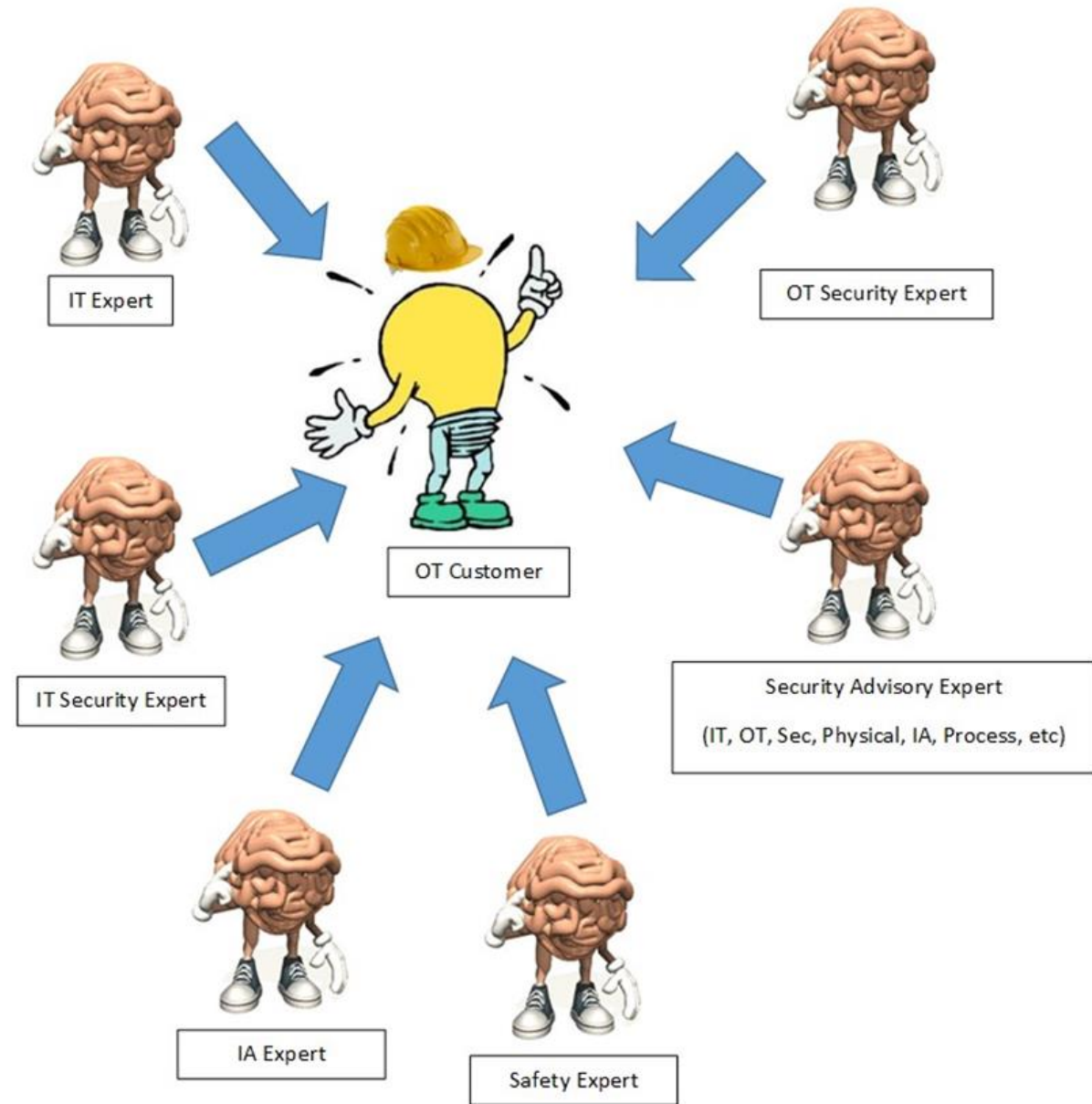


Security Enhancement Strategic Relationships



The Security A-Team

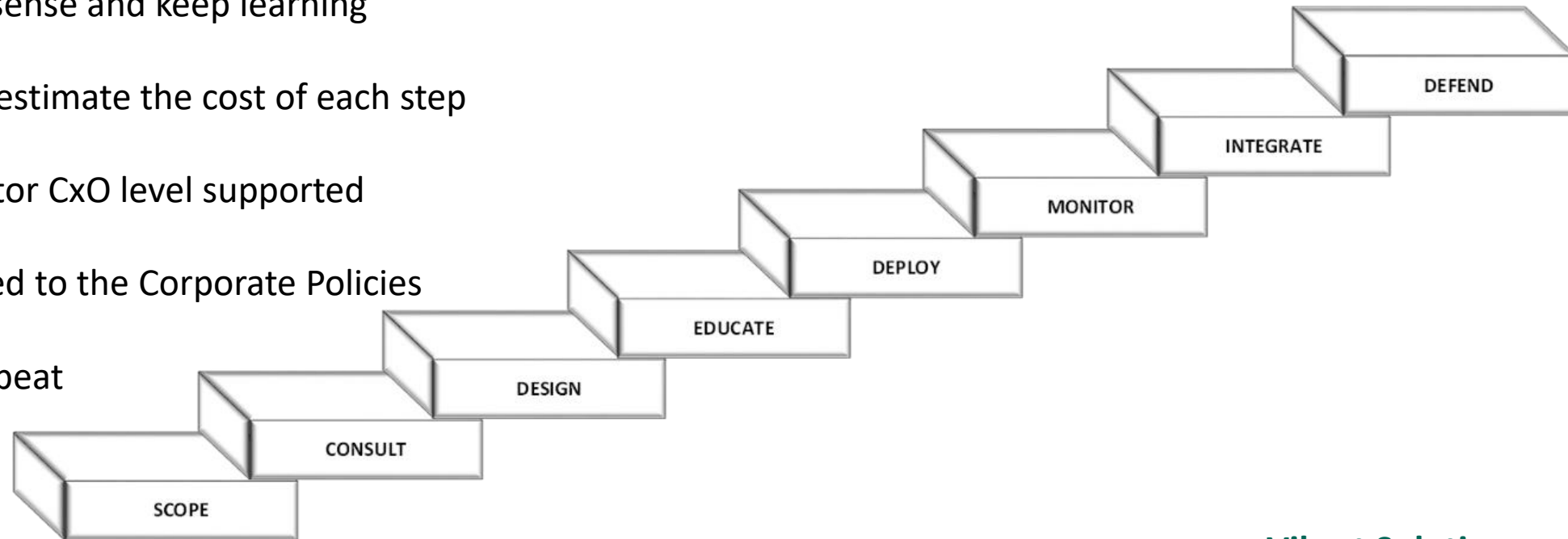
- The Team is the core
- Multi-role people
- Champions (social)
- Champions (technical)
- Financial budget holders
- Key decision makers
- Internal and External members
- Success is not simple



The Security Staircase

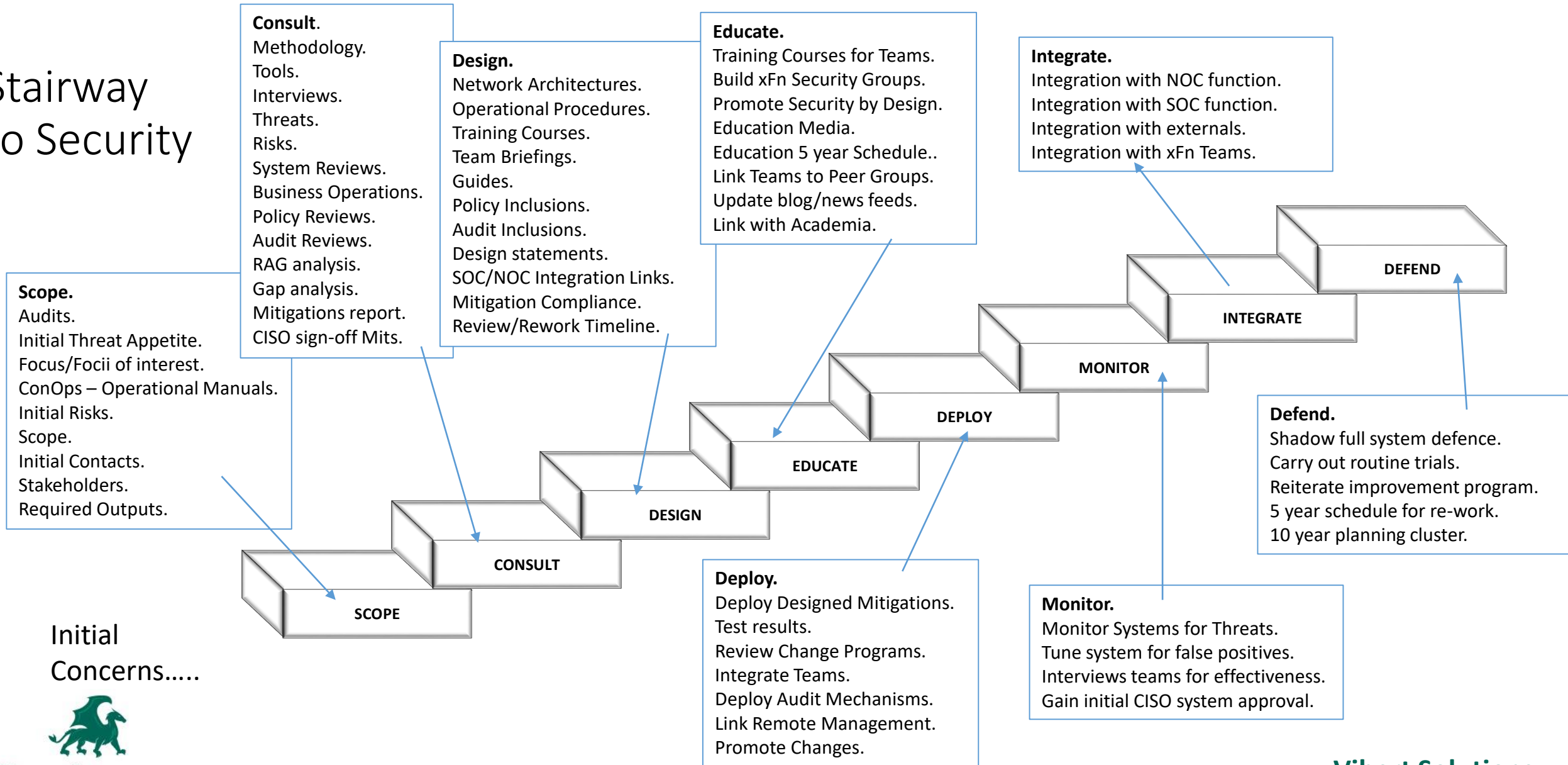
The Security Staircase

- 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



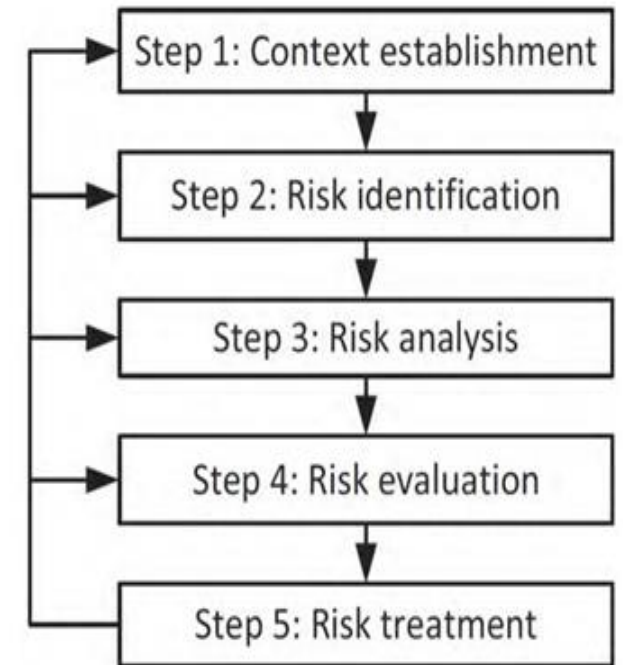
Initial Concerns.....



Risks, Threats, Impact Assessments

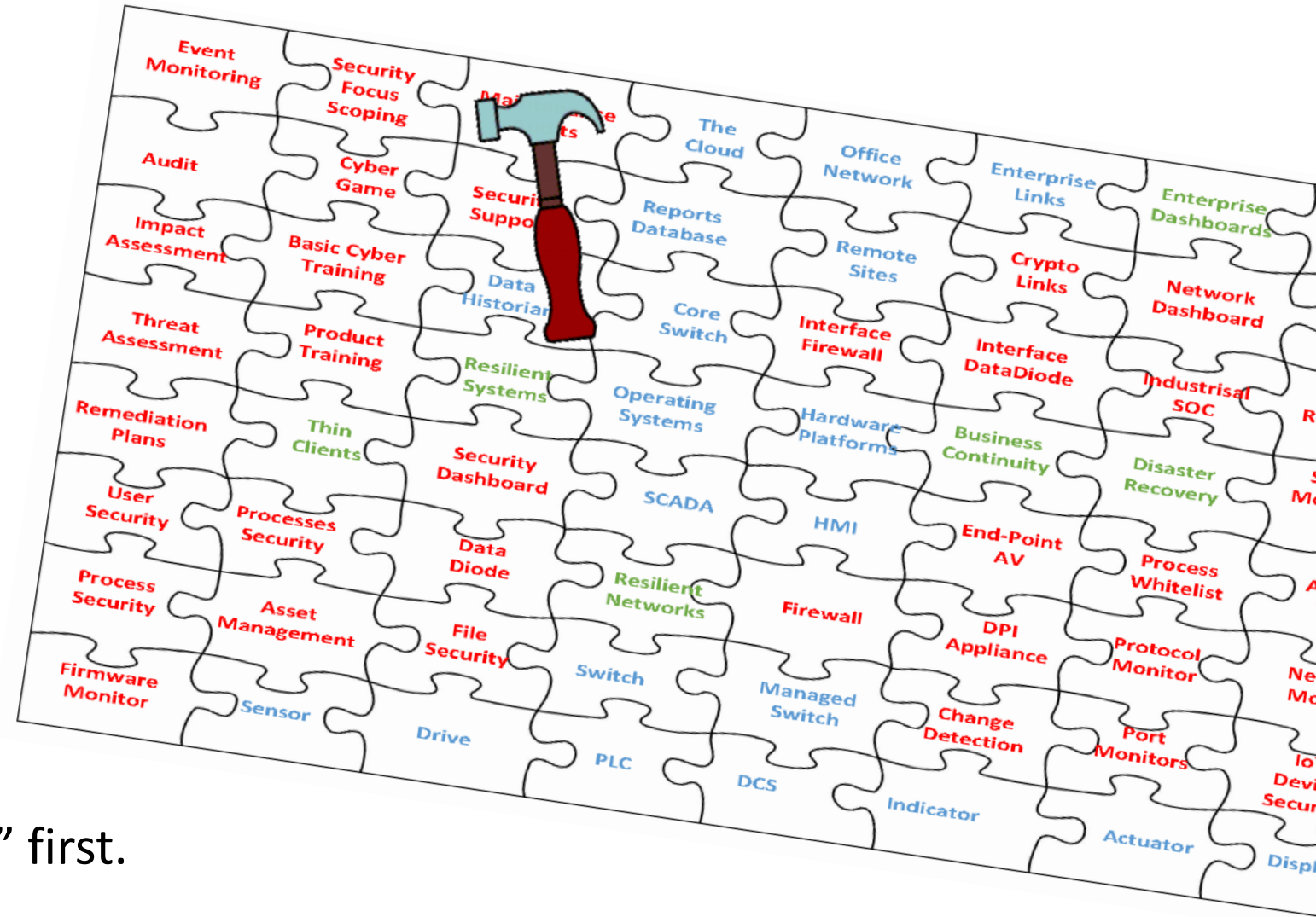
Security Assessments

- 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

SECURITY
101

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



This advice has been produced to help charities protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at www.ncsc.gov.uk/charity

Backing up your data

Take regular backups of your important data, and test they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

- Identify what needs to be backed up. Normally this will comprise documents, emails, contacts, legal information, calendars, financial records and supporter or beneficiary databases.
- Ensure the device containing your backup is not permanently connected to the device holding the original copy, neither physically nor over a local network.
- Consider backing up to the cloud. This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

- Switch on PIN/password protection/fingerprint recognition for mobile devices.
- Configure devices so that when lost or stolen they can be tracked, remotely wiped or remotely locked.
- Keep your devices (and all installed apps) up to date, using the 'automatically update' option if available.
- When sending sensitive data, don't connect to public Wi-Fi hotspots - use 3G or 4G connections (including tethering and wireless dongles) or use VPNs.
- Replace devices that are no longer supported by manufacturers with up-to-date alternatives.

Preventing malware damage

You can protect your charity from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

- Use antivirus software on all computers and laptops. Only install approved software on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.
- Patch all software and firmware by promptly applying the latest software updates provided by manufacturers and vendors. Use the 'automatically update' option where available.
- Control access to removable media such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.
- Switch on your firewall (included with most operating systems) to create a buffer zone between your network and the Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

- Ensure staff don't browse the web or check emails from an account with Administrator privileges. This will reduce the impact of successful phishing attacks.
- Scan for malware and change passwords as soon as possible if you suspect a successful attack has occurred. Don't punish staff if they get caught out (it discourages people from reporting in the future).
- Check for obvious signs of phishing, like poor spelling and grammar, or low quality versions of recognizable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

- Make sure all laptops, MACs and PCs use encryption products that require a password to boot. Switch on password/PIN protection or fingerprint recognition for mobile devices.
- Use two factor authentication (2FA) for important websites like banking and email, if you're given the option.
- Avoid using predictable passwords (such as family and pet names). Avoid the most common passwords that criminals can guess (like password).
- Do not enforce regular password changes; they only need to be changed when you suspect a compromise.
- Change the manufacturers' default passwords that devices are issued with, before they are distributed to staff.
- Provide secure storage so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.
- Consider using a password manager. If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.

Delivery



Network Perimeter Defences

Can block insecure or unnecessary services, or only allow permitted websites to be accessed.



Malware Protection

Can block malicious emails and prevent malware being downloaded from websites.



Password Policy

Can prevent users from selecting easily guessed passwords and locks accounts after a low number of failed attempts.



Secure Configuration

Can prevent users from selecting easily guessed passwords and locks accounts after a low number of failed attempts.

Breach



Patch Management

Apply patches at the earliest point to limit exposure to known software vulnerabilities.



Monitoring

Monitor and analyse all network to identify any malicious or unusual activity.



Malware Protection

Malware protection within a gateway can detect malicious software.



Secure Configuration

Remove unnecessary software user accounts. Ensure default settings are changed, and that automatic updates that could activate malware are in an important item.



User Access

Well maintained user access controls restrict the applications, privileging that users can access.



User Training

User training is extremely valuable reducing the likelihood of successful social engineering attacks.



Device Controls

Devices within the internal gate can be used to prevent unauthorised access to critical services or inherently sensitive data that may still be required.

Affect



Controls For



NCSC Glossary

This glossary explains some common words and phrases relating to cyber security, originally published via the @NCSC Twitter channel throughout December. The NCSC is working to demystify the jargon used within the cyber industry. For an up-to-date list, please visit www.ncsc.gov.uk/glossary.

£600K-£1.15m
Average cost of security breach



10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime - together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.



Network Security

Protect your networks from attack. Define the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.



User education and awareness

Produce user security policies covering acceptable and secure use of your systems, include in staff training. Maintain awareness of cyber risks.



Malware prevention

Produce relevant policies and establish anti-malware defences across your organisation.



Removable media controls

Produce a policy to control all access to removable media. Limit media type and use. Scan all media for malware before importing onto the corporate system.



Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline tool for all devices.

Make cyber risk a priority for your Board

Produce supporting risk management policies

Set up your Risk Management Regime

Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

Determine your risk appetite

Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and rules to all devices. Protect data both in transit and at rest.



Content hub Building up the defence


ARTICLE

14 Mar 2019 5 min read

EMAIL SHARE TWEET SHARE SHARE

Building up the defence

The cyber physical bad guys are now attacking internet of things (IOT) 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 (IOT) 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

(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 ISC² 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 IOT, IIOT 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 - 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.



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 lets talk.



NCSC CAF 3

Cyber Assessment Framework

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.



NCSC CAF 3

Cyber Assessment Framework

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.



NCSC CAF 3

Cyber Assessment Framework

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.

