Holistic Integrated Organisational Resilience, with a side of Cyber.

Accelerating Change in UK Security and Resilience.

Cevn Vibert

2023

linkedin.com/in/cevnvibert/

Cevn Vibert

- Chair of InstMC Cyber SIG.
- Formative Alliance to design the new UK Cyber Security Council.
- Ex-Principal Assurance at OFGEM Competent Authority.
- NIS Compliance Advisor and OT Cyber Consultant.
- Conference Chair/Speaker.
- Chartered IT Professional
- Chartered Engineer.
- Fellow of the BCS, IET, InstMC.
- Member of NCSC COI.

Find me on **LinkedIn**. Easy to Google!

CITP FBCS
CHARTERED FELLOW
bcs The Chartered Institute for IT
Chartered IT Professional citp

Engineering Council
Chartered Engineer

GLOBAL INDUSTRIAL CYBER SECURITY PROFESSIONAL
GICSP

VIBERT

Inst MC

I actually do real Engineering too !!

I encourage you to reflect on your story!

ICS - Control Rooms - Op Centres – Cyber – Physical - CNI

Talk a lot

CYBERUK

IET The Institution of Engineering and Technology

Holistic Integrated Organisational Resilience, with a side of Cyber.

Accelerating Change in UK Security and Resilience

The Resilience Buffet

Cyber Security and Resilience applies to **all** industries.

Stuxnet

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

We were missing **The Stories** of relevance in the UK…. But now..

DroppingElephant

DragonFly

Equation

Shamoon

wiper

StoneDrill

Carbanak

CrouchingYeti

Industroyer

DarkHotel

Andromeda

ShadowBrokers

WannaCry

Petya

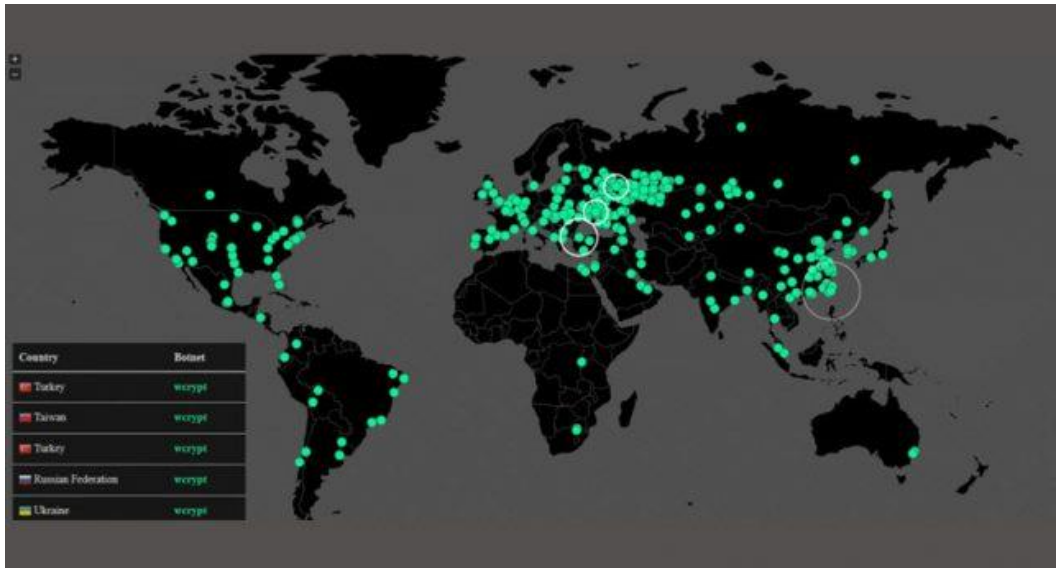
Turla

NotPetya

BlackEnergy

Ukraine1

Ukraine2



Mirai

Gaus

ZeuS

Dallas Emergency Sirens

German Steelmill

Kemuri Water

Flame

NightDragon

Maersk

RedOctober

Duqu

Aurora Test

EnergeticBear / CozyBear

PetulantPenguin

Slammer and Conficker Worm

Agora+ for Canvas and Metasploit

Brakes to the pace of change:

- Usual OT cyber excuses.
- No drive from above in the organisation.
- No news at home.
- No clear link of impacts to business drivers.
- No clarity on threats, likelihood, motivations, ...

What are biggest challenges you face in making improvements….

- **Cost?**
- **Resources?**
- **Technology?**
- **Knowledge?**
- **Compliance?**
- **Competitiveness?**
- **Skills and Experience?**
- **Understanding risks?**
- **Corporate will?**

The need for change is not new:

Many, many, years of different conference bleating and wailing from myself and my betters..

30+yrs writing papers, speaking, and chairing industry conferences -

Change really does take time! ☺









The times they are a’changing…….

Activity in security and resilience is improving, and at an improving pace.

Threats are increasing. Nation States are back on the list.

The battlefield is constantly expanding.

IOT. Connectivity. Complexity. AI. Organised Crime.

Legislation.

…and more Legislation…

Competent Authorities (CA) carry out Cyber Regulation within the UK Operators of Essential Services (OES). This includes monitoring compliance with both license conditions, and the Network & Information Systems (NIS) Regulations.

CA's functions are to focus the companies on improving their cyber security, and resilience, in order to secure essential services to UK businesses and citizens.

CAs provide :-

.

Guidance and Advice

Inspections

Enforcement

Many Initiatives for improvement:

- **Legislation. e.g. NIS**
- **NCSC CAF**
- Crossover impacts from IT to OT are evidenced.
- World media news.
- Compliance Tools.
- **Inspection Programmes.**

What is the UK Government doing?

- Support through voluntary engagement with NCSC, BEIS and Industry forums
- Investment (RIIO)
- Regulation (NIS, SEC)

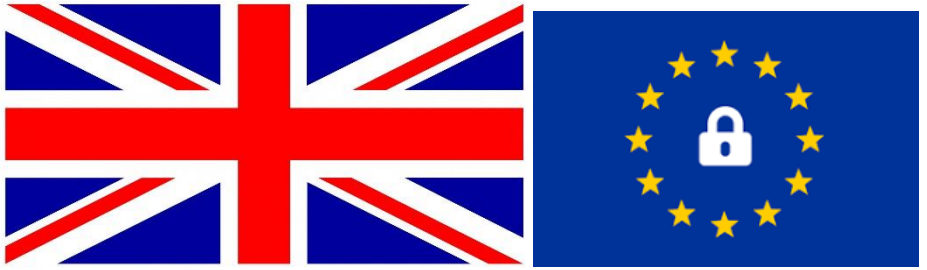
The UK has decided to use the **NCSC Cyber Assessment Framework (CAF)** to drive outcome improvements across all components of the Critical National Infrastructure (CNI), including energy

The **CAF focuses on security and resilience,** including:

- managing cyber risk
- protecting against attack
- detecting incidents
- minimising the impact of incidents

NIS Directive

Network & Information Security(NIS) Directive



NIS-Directive aims :

1. Improving national cyber security capabilities .
2. Increasing EU cooperation on cyber security .
3. Operators of Essential Service (OES) security measures & incident reporting obligations.

NIS-D adopted by EU Parliament Jul 2016, in force Aug 2016.

NIS-D introduced in UK in 2018.

NIS-D requires OES to adopt "appropriate and proportionate technical and organisational measures" to achieve compliance.

Fines of between £8million and £20million or 2–4% of annual global turnover have been proposed by the UK government in the recent NIS reform consultations (NIS2UK).

Fines only applied if organisations cannot demonstrate appropriate risk mitigation measures are in place.

Networks and Information Systems (NIS) Directive: NCSC CAF Security objectives and principles

A. **Appropriate** organisational structures, policies, and processes in place to understand, assess and systematically manage security risks to the network and information systems supporting essential services

- A.1 Governance
- A.2 Risk Management
- A.3 Asset Management
- A.4 Supply Chain

B. **Proportionate** security measures in place to protect essential services and systems from cyber attack

- B.1 Service Protection Policies and Processes
- B.2 Identity & Access Control
- B.3 Data Security
- B.4 System Security
- B.5 Resilient Networks & Systems
- B.6 Staff Awareness & Training

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

- C.1 Security Monitoring
- C.2 Anomaly Detection

D. Capabilities to minimise the impacts of a cyber security incident on the delivery of essential services including the restoration of those services where necessary

- D.1 Response and Recovery Planning
- D.2 Improvements

Key highlights of Network and Information Systems (NIS) Regulations 2018

CAF

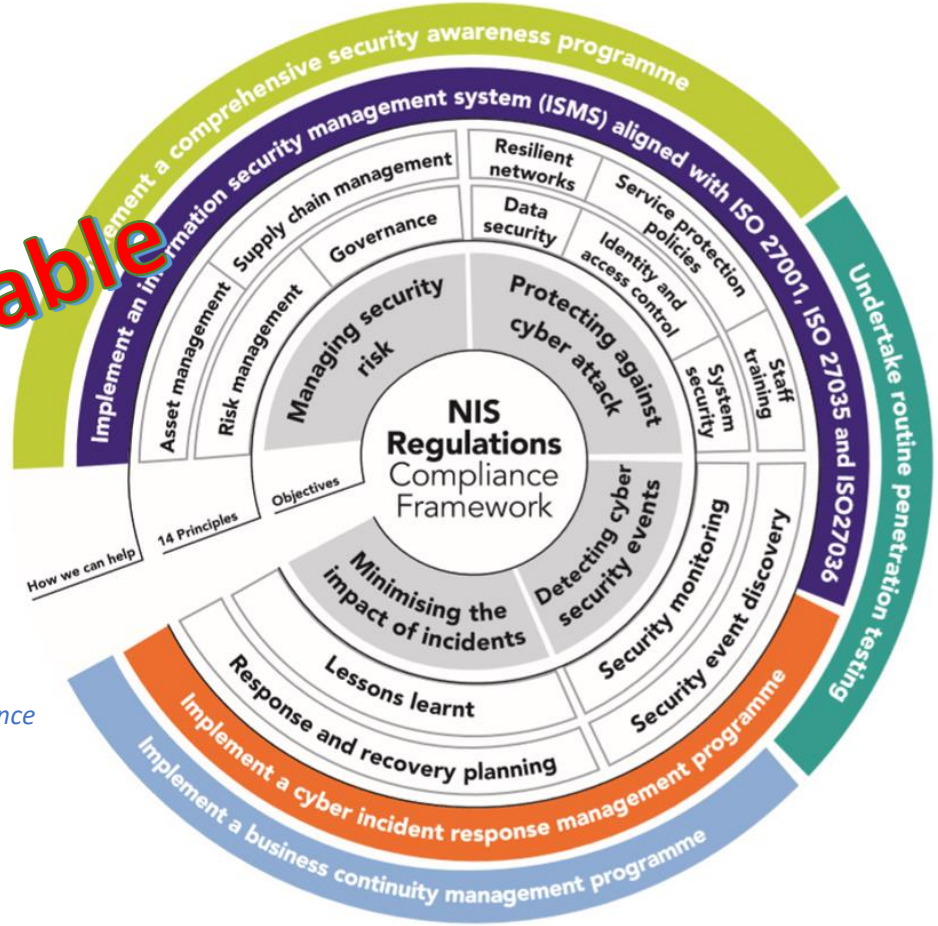
NIS Objectives							
A: Managing security risk		B: Protecting against cyber attack		C: Detecting cyber security incidents		D: Minimising the impact of cyber security incidents	
NIS Principles							
A1: Governance	A2: Risk management	B1: Service protection policies and processes	B2: Identity and access control	C1: Security monitoring	C2: Proactive security event discovery	D1: Response and recovery planning	D2: Lessons learned
A3: Asset management	A4: Supply chain	B3: Data security	B4: System security				
		B5: Resilient networks and systems	B6: Staff awareness and training				

NCSC (CAF)

NIS-D Guidance is available

Guidelines on
assessing DSP and OES compliance
to the NISD security requirements

ENISA



IT Governance

Objective	Principle	Contributing Outcome	R	A	G
A. Organisational Capabilities	A1. Governance	A1.a Board Direction			
		A1.b Roles & Responsibilities			
		A1.c Decision-making			
	A2. Risk Management	A2.a Risk Management Process			
		A2.b Assurance			
	A3. Asset Management	A3.a Asset Management			
	A4. Supply Chain	A4.a Supply Chain			
B. Protective Security Measures	B1. Service Protection Policies & Processes	B1.a Policy & Process Development			
		B1.b Policy & Process Implementation			
	B2. Identity & Access Control	B2.a Identity Verification, Authentication & Authorisation			
		B2.b Device Management			
		B2.c Privileged User Management			
		B2.d Identity & Access Management			
	B3. Data Security	B3.a Understanding Data			
		B3.b Data in Transit			
		B3.c Stored Data			
		B3.d Mobile Data			
		B3.e Media/Equipment Sanitisation			
	B4. System Security	B4.a Secure By Design			
		B4.b Secure Configuration			
		B4.c Secure Management			
		B4.d Vulnerability Management			
	B5. Resilient Networks & Systems	B5.a Resilience Preparation			
		B5.b Design for Resilience			
		B5.c Backups			
	B6. Staff Awareness & Training	B6.a Cyber Security Culture			
		B6.b Cyber Security Training			
C. Detecting Cyber Security Events	C1. Security Monitoring	C1.a Monitoring Coverage			
		C1.b Securing Logs			
		C1.c Generating Alerts			
		C1.d Identifying Security Incidents			
		C1.e Monitoring Tools & Skills			
	C2. Proactive Security Event Discovery	C2.a System Abnormalities for Attack Detection			
		C2.b Proactive Attack Discovery			
D. Minimising the Impact of Cyber Security Incidents	D1. Response & Recovery Planning	D1.a Response Plan			
		D1.b Response & Recovery Capability			
		D1.c Testing & Exercising			
	D2. Lessons Learned	D2.a Incident Root Cause Analysis			
		D2.b Using Incidents to Drive Improvements			

The CAF

Cyber Assessment Framework
(NCSC)

Key failings experienced in industries:

a) Mapping to Governance throughout.
b) Technical Risk Assessments, and full-circle Risk Management linked to Governance.
c) Asset Management including criticalities.
d) Incident Management and exercising.
e) Secure Configuration/ Development.
f) Embedded Device Security.
g) Physical and Operational Security.
h) Supply Chain Security.

Big Steps for your Organisation

Review Governance A1: What functions are required to be resilient to make the business cores function according to the business, and what are the leeways.

Determine current state of assets, functions, processes, people and technology.

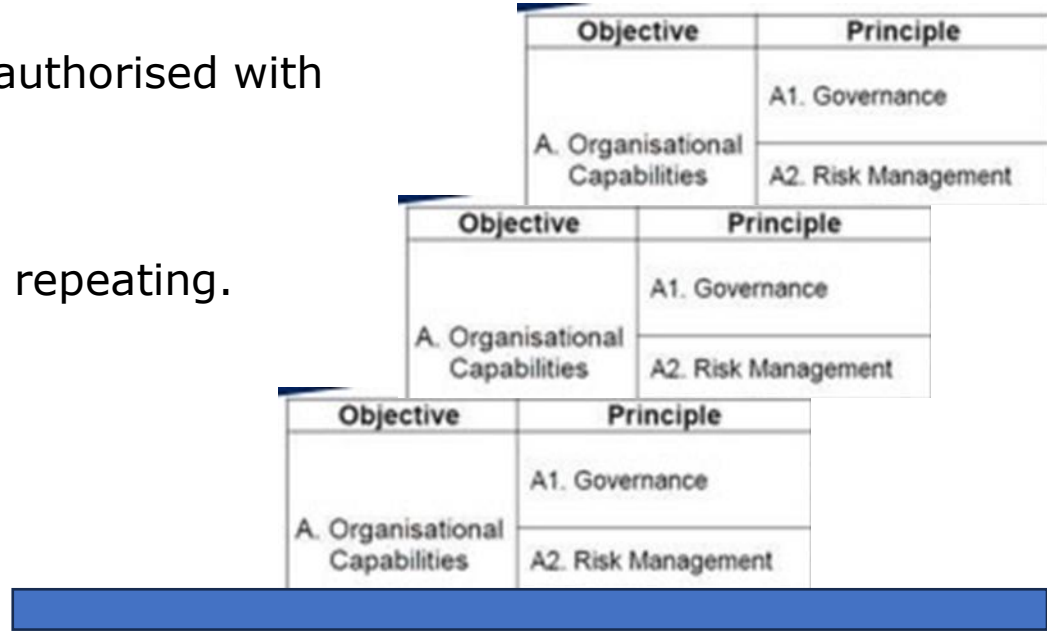
Risk Assess A2: Assess the above to ensure it all meets the Governance business aims and requirements.

Determine mitigations against gaps and ensure integrated and authorised with the business governance.

Document all reviews and decisions. Communicate.

Repeat and make the whole process easy and thorough to keep repeating.

Ensure two-eyes minimum on the whole process.



Communicate: Everyone's responsibility.

Build the industry: More apprentices, juniors, trainees, interns, recruits, etc. are needed to counter the SQEP drought.

And the Future? **?**

- NIS2 – UK Version? Supply chains, other OES/Important services, Director accountability, 2% global…
- Lights-on, heating-on, fresh water, communications OK, transport ok, food ok,…..
- Increased Process resilience, Corporate resilience and Intra-Corporate resilience.
- Increased preparedness and exercising.
- Organisations develop a **"culture of security and resilience"** as already exists in Health & Safety?

- Cyber-attack events will continue.

"Culture of Holistic Integrated Security and Resilience"

The future is brighter, but more pace of change is required.

More recruits and more experience to counter the SQEP drought are being sought.

More focus and understanding seen at all levels.

Winning more hearts-and-minds of senior execs.

Suitably
Qualified
Experienced
Person

Increased pace of change is still very much required.

What do you need?

How can you help others?

What have you learned?

Thank You.

Vibert Ltd – Advisory, Consulting and Training

InstMC Cyber SIG

Cevn Vibert

2023

linkedin.com/in/cevnvibert/

Simulation Games

Typical Scenarios

** New !! **

IT and ICS networks

Exciting!

Educational