DNV

WHEN TRUST MATTERS

Utility Cyber Security Implementation

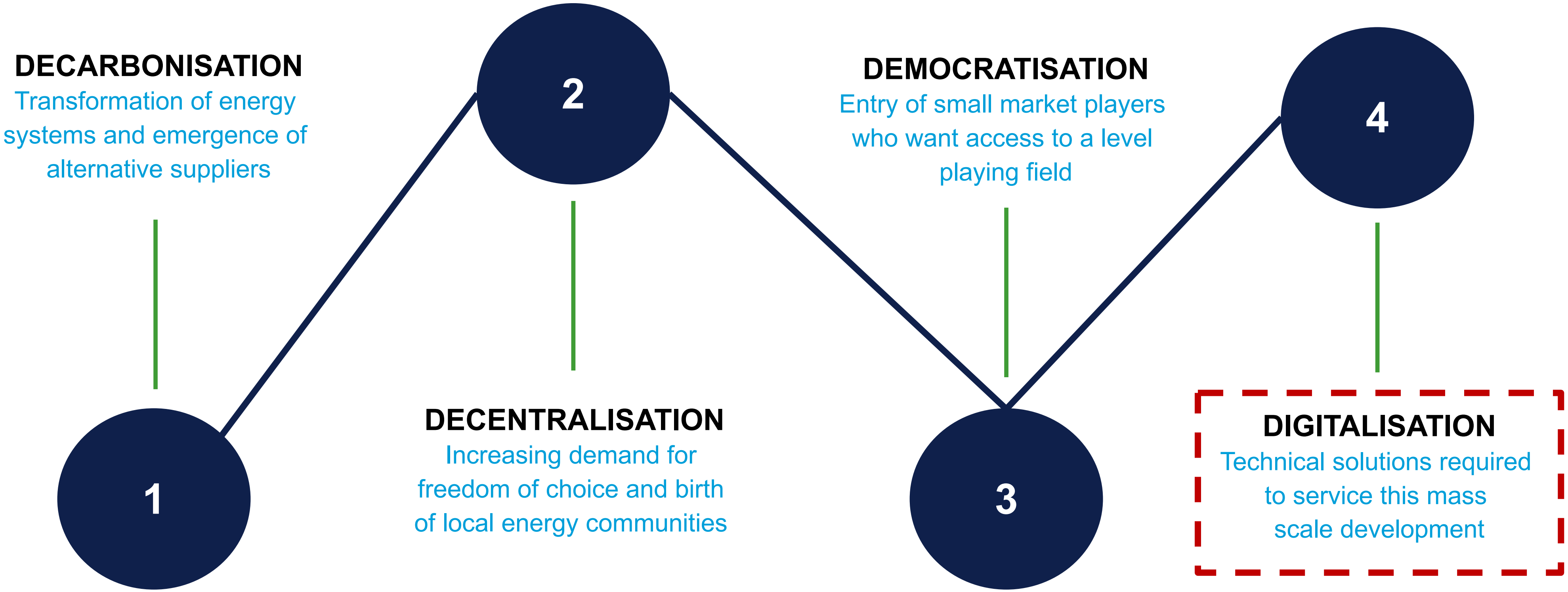
Jalal Bouhdada – Founder, Global Segment Director for Cyber Security

CIGRE Seminar 2022

10 November 2022

Situational awareness

The 4D revolution



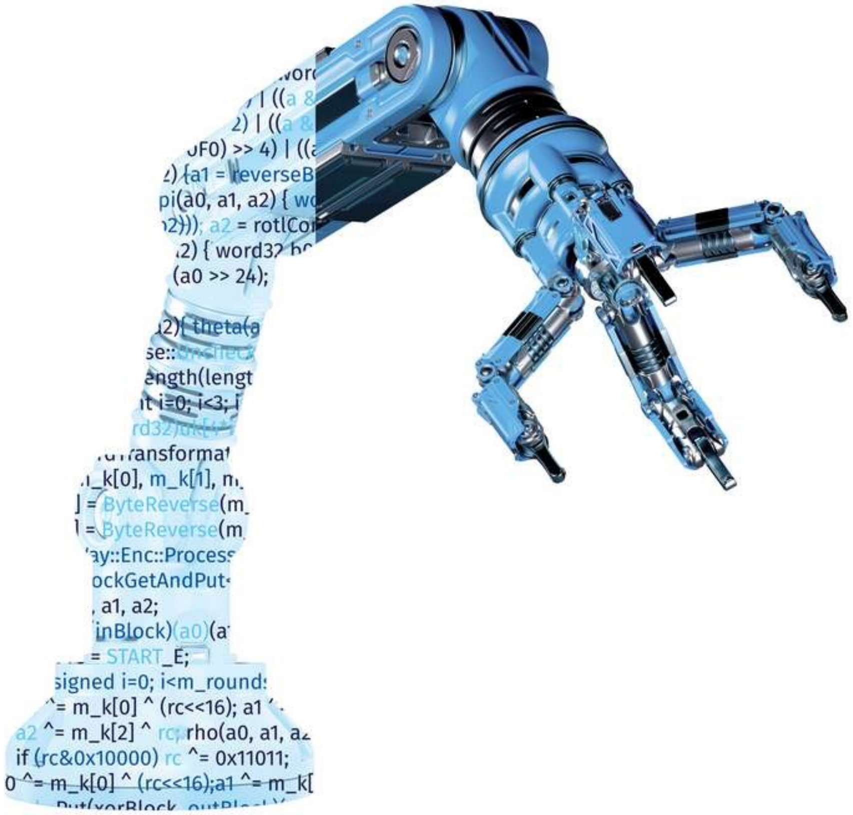
DECARBONISATION
Transformation of energy systems and emergence of alternative suppliers

DECENTRALISATION
Increasing demand for freedom of choice and birth of local energy communities

DEMOCRATISATION
Entry of small market players who want access to a level playing field

DIGITALISATION
Technical solutions required to service this mass scale development

Operational technology: an emerging vulnerability



Top 10 industries facing cyber-attacks in 2021*

1. Manufacturing
2. Finance and insurance
3. Professional and business services
4. Energy
5. Retail and wholesale
6. Healthcare
7. Transportation
8. Government
9. Education
10. Media

Source: IBM X-Force Threat Intelligence report

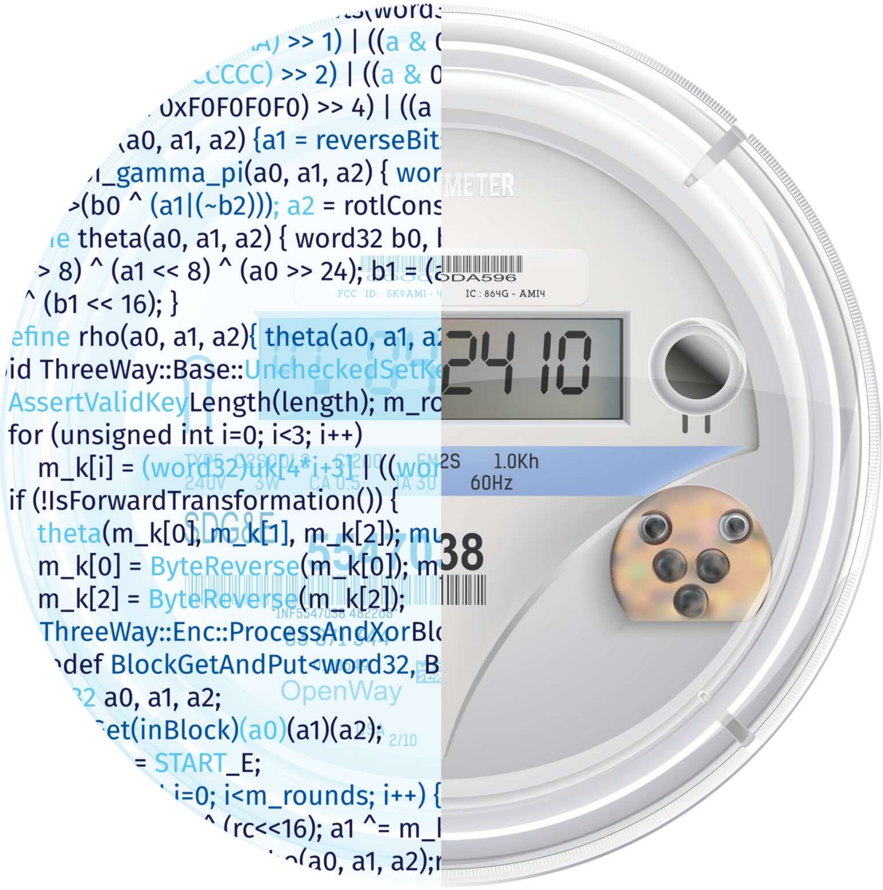
Developing risks

Changing geopolitical landscape and growing spotlight on critical infrastructure

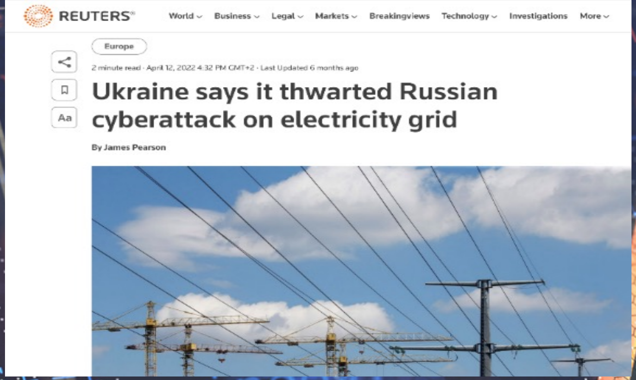
Supply chain: a deep and complex challenge for industries

IT/OT convergence: visibility, architecture and governance issues

Shortage of skills and qualified staff post COVID-19 pandemic



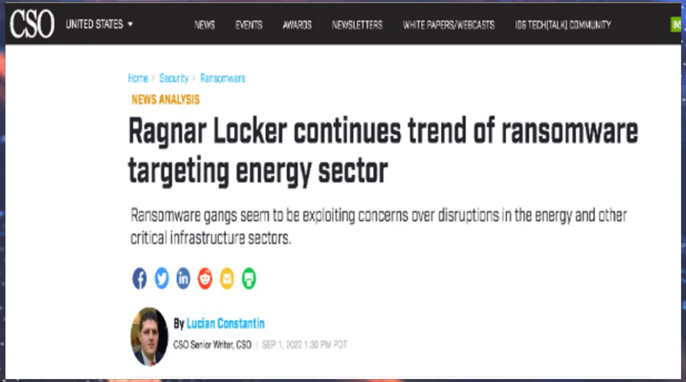
Recent attacks on critical infrastructure



2 minute read · April 12, 2022 4:32 PM GMT+2 · Last Updated 6 months ago

Ukraine says it thwarted Russian cyberattack on electricity grid

By James Pearson



Home > Security > Ransomware

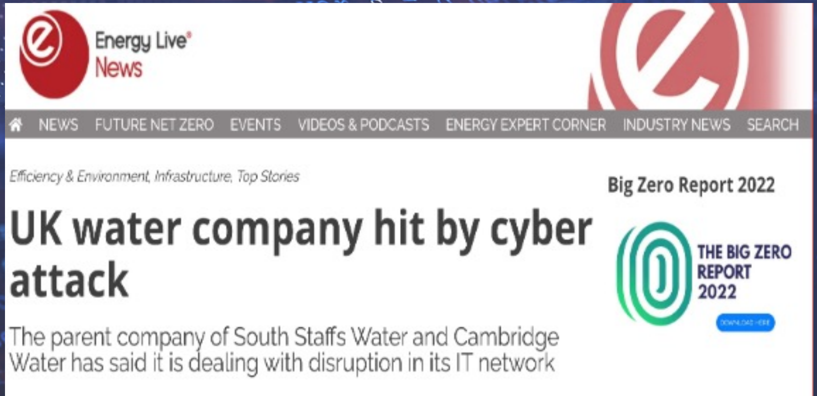
NEWS ANALYSIS

Ragnar Locker continues trend of ransomware targeting energy sector

Ransomware gangs seem to be exploiting concerns over disruptions in the energy and other critical infrastructure sectors.

By Lucian Constantin

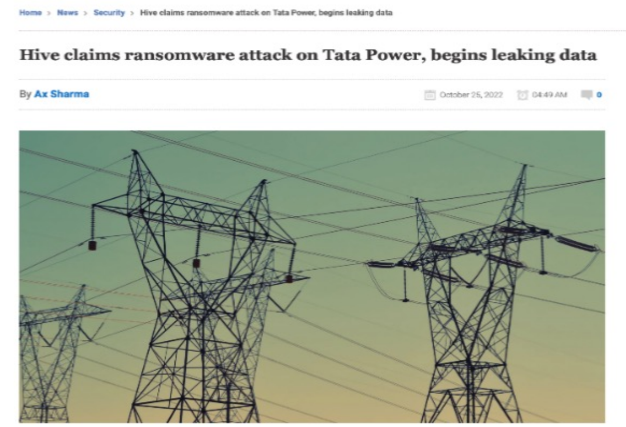
CSO Senior Writer, CSO | SEP 1, 2022 1:30 PM PDT



Efficiency & Environment, Infrastructure, Top Stories

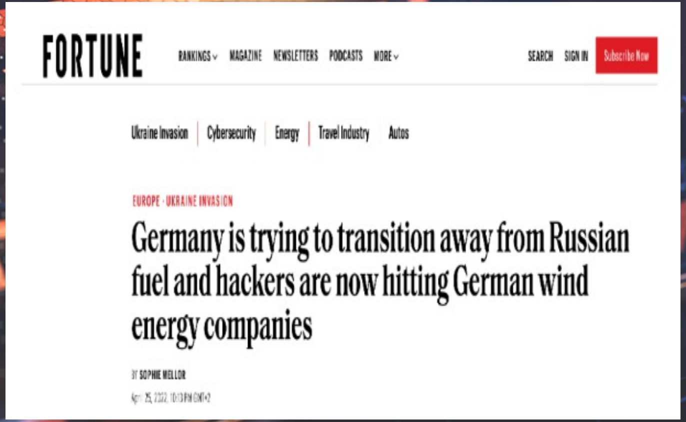
UK water company hit by cyber attack

The parent company of South Staffs Water and Cambridge Water has said it is dealing with disruption in its IT network


Home > News > Security > Hive claims ransomware attack on Tata Power, begins leaking data

Hive claims ransomware attack on Tata Power, begins leaking data

By Ax Sharma — October 25, 2022 — 04:49 AM — 0

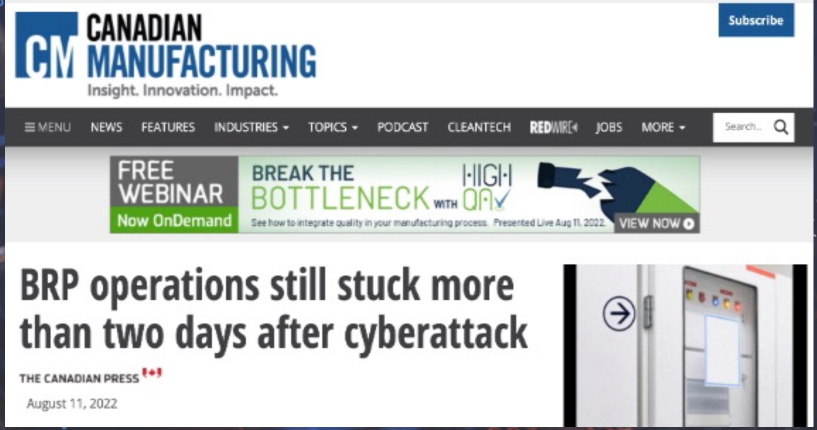


EUROPE · UKRAINE INVASION

Germany is trying to transition away from Russian fuel and hackers are now hitting German wind energy companies

BY SOPHIE MELLOR

April 25, 2022, 10:13 PM GMT+2


CANADIAN MANUFACTURING
Insight. Innovation. Impact.
Subscribe
MENU
NEWS
FEATURES
INDUSTRIES
TOPICS
PODCAST
CLEANTECH
REDWIRE
JOBS
MORE
Search..
FREE WEBINAR
Now OnDemand
BREAK THE BOTTLENECK WITH HIGH QA
See how to integrate quality in your manufacturing process. Presented Live Aug 11, 2022.
VIEW NOW

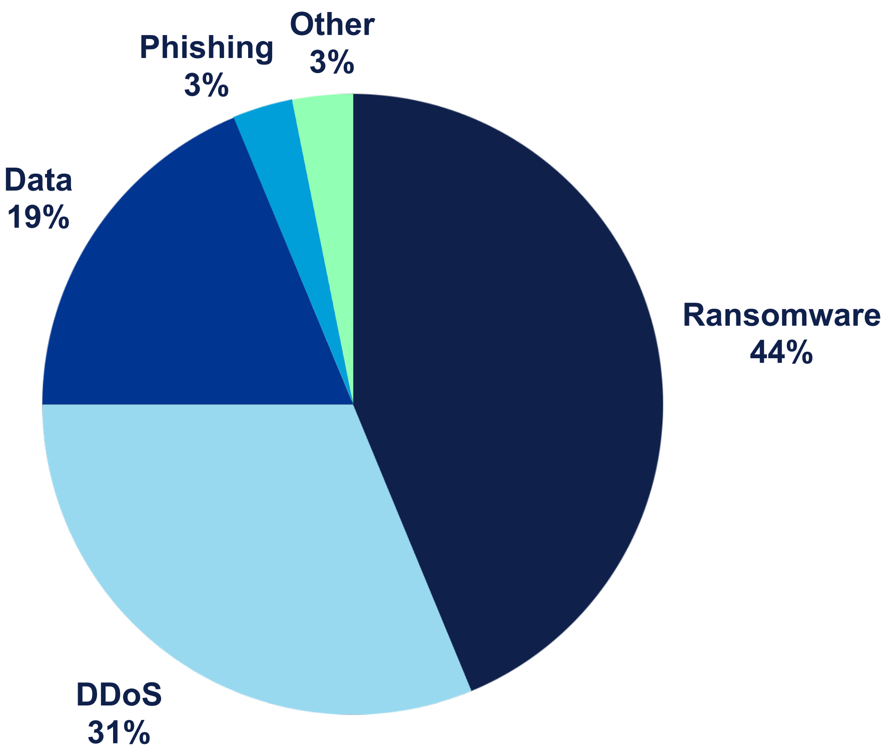
BRP operations still stuck more than two days after cyberattack

THE CANADIAN PRESS

August 11, 2022

Reported energy systems incidents in the EU

Incidents by Type

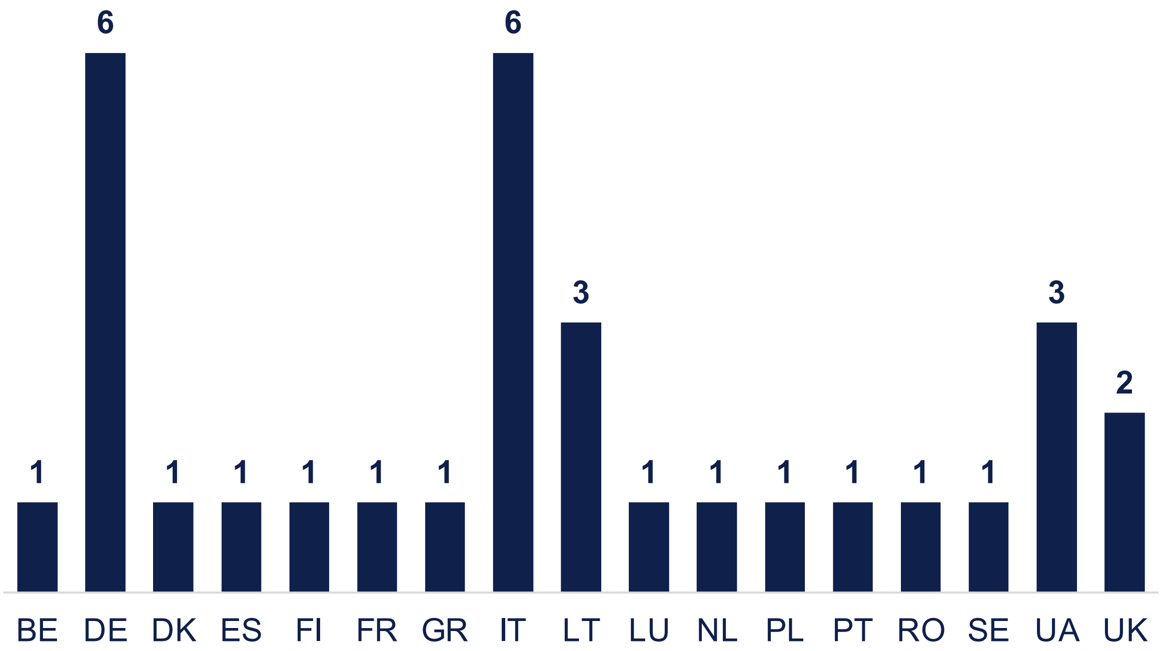


Source: ENISA EU Threat Landscape

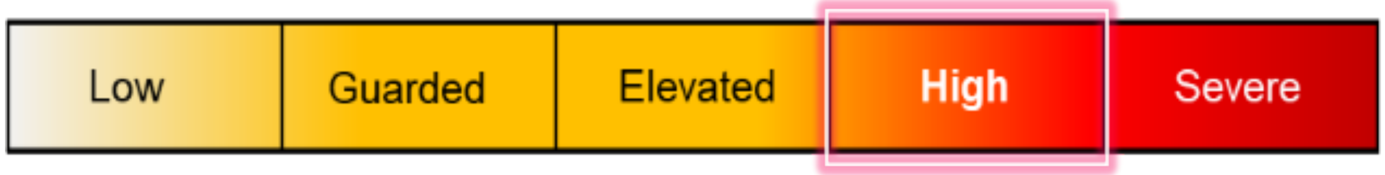
Incidents by Country

Total: 31 incidents

17 countries affected



Threat assessment

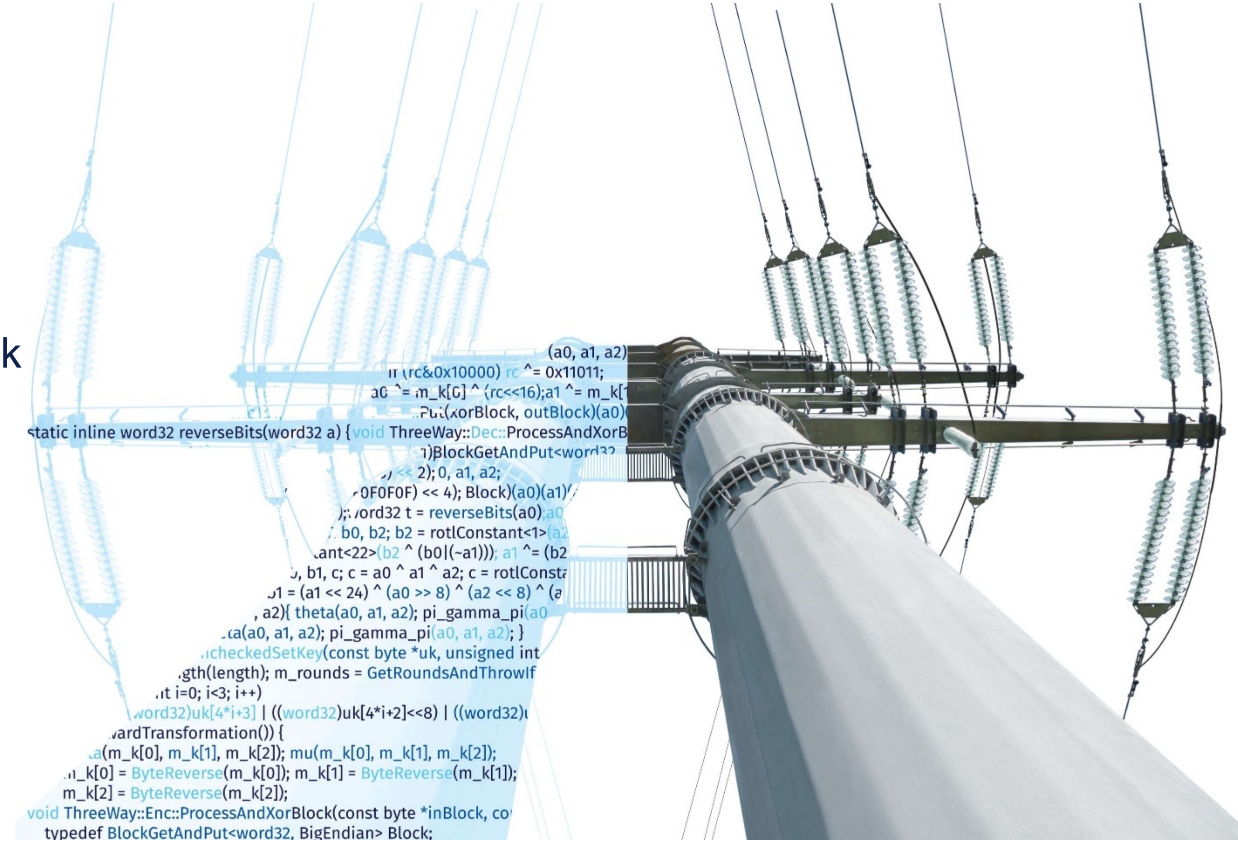


- The Ukraine conflict is still the primary source of concern
- Hacktivist and extortion/ransomware groups are taking sides
- Weaponization of the sector might attract ransomware actor interest
- Organizations are being targeted as a political statement
- Critical national infrastructure is being targeted to disrupt operations
- Continued possibility of intrusions directed at pre-positioning or information gathering.

Source: ENISA EU Threat Landscape

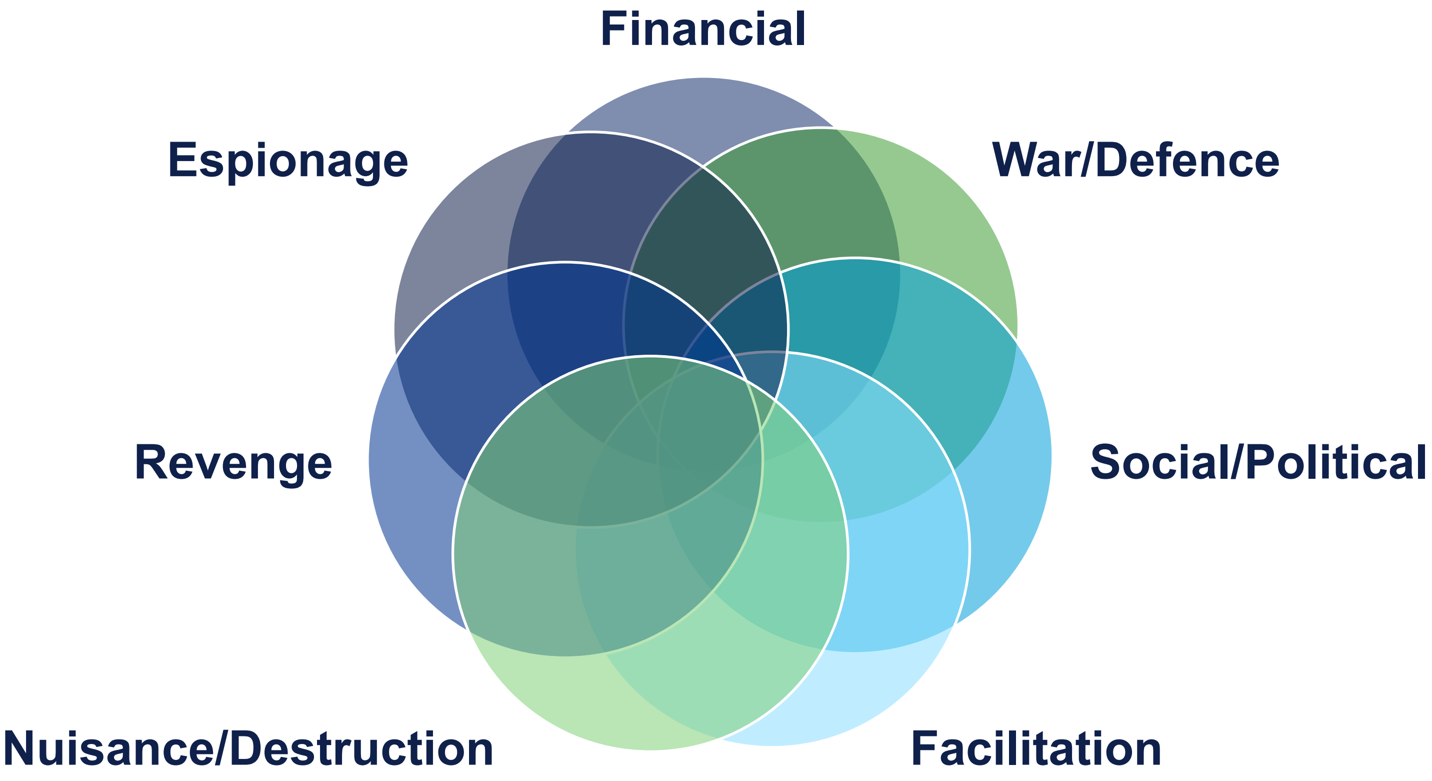
Energy crisis implications

- Six reported ransomware incidents in Europe: Italy, Greece, Germany, Luxembourg and Poland
- Increasing hacktivist attacks such as defacements, DDoS and data breaches against companies
- The wiper attack is the most reported destructive attack on Ukrainian assets. (WhisperGate, HermeticWiper, CaddyWiper, etc)
- No reports of a wiper, or other destructive attack detected on an IT system in EU member states.



```
                                          (a0, a1, a2)
                      if (rc&0x10000) rc ^= 0x11011;
                      a0 ^= m_k[0] ^ (rc<<16);a1 ^= m_k[1
                         Put(xorBlock, outBlock)(a0)(
static inline word32 reverseBits(word32 a) {void ThreeWay::Dec::ProcessAndXorB
                         1)BlockGetAndPut<word32
                      << 2);0, a1, a2;
                   F0F0F0F) << 4); Block)(a0)(a1)(
                 );word32 t = reverseBits(a0);a0
                 b0, b2; b2 = rotlConstant<1>(a2
               ant<22>(b2 ^ (b0|(~a1))); a1 ^= (b2
             b1, c; c = a0 ^ a1 ^ a2; c = rotlConsta
            b1 = (a1 << 24) ^ (a0 >> 8) ^ (a2 << 8) ^ (a
           , a2){ theta(a0, a1, a2); pi_gamma_pi(a0
          ta(a0, a1, a2); pi_gamma_pi(a0, a1, a2); }
         ncheckedSetKey(const byte *uk, unsigned int
       gth(length); m_rounds = GetRoundsAndThrowIf
     nt i=0; i<3; i++)
    word32)uk[4*i+3] | ((word32)uk[4*i+2]<<8) | ((word32)u
   ardTransformation()) {
  a(m_k[0], m_k[1], m_k[2]); mu(m_k[0], m_k[1], m_k[2]);
 m_k[0] = ByteReverse(m_k[0]); m_k[1] = ByteReverse(m_k[1]);
 m_k[2] = ByteReverse(m_k[2]);
void ThreeWay::Enc::ProcessAndXorBlock(const byte *inBlock, co
 typedef BlockGetAndPut<word32, BigEndian> Block;
```

Rational actor & motivations



- Nations states, three-letter agencies
- Cyber criminals, gangs
- Hacktivists
- Competition
- Script kiddies
- Cyber mercenaries
- Insiders

The 4D tactics of choice

Disinformation

Deception

Denial
of Service

Distortion

Malicious actors’ game plan for control system intrusions

1. Establish intended effect and select a target
2. Collect intelligence about the target system
3. Develop techniques and tools to navigate and manipulate the system
4. Gain initial access to the system
5. Execute techniques and tools to create the intended effect

Utility Cyber Security

Utility Business → Continuing Energy Supply

Office

Wireless

Cloud

C = Confidentiality
I = Integrity
A = Availability

IT

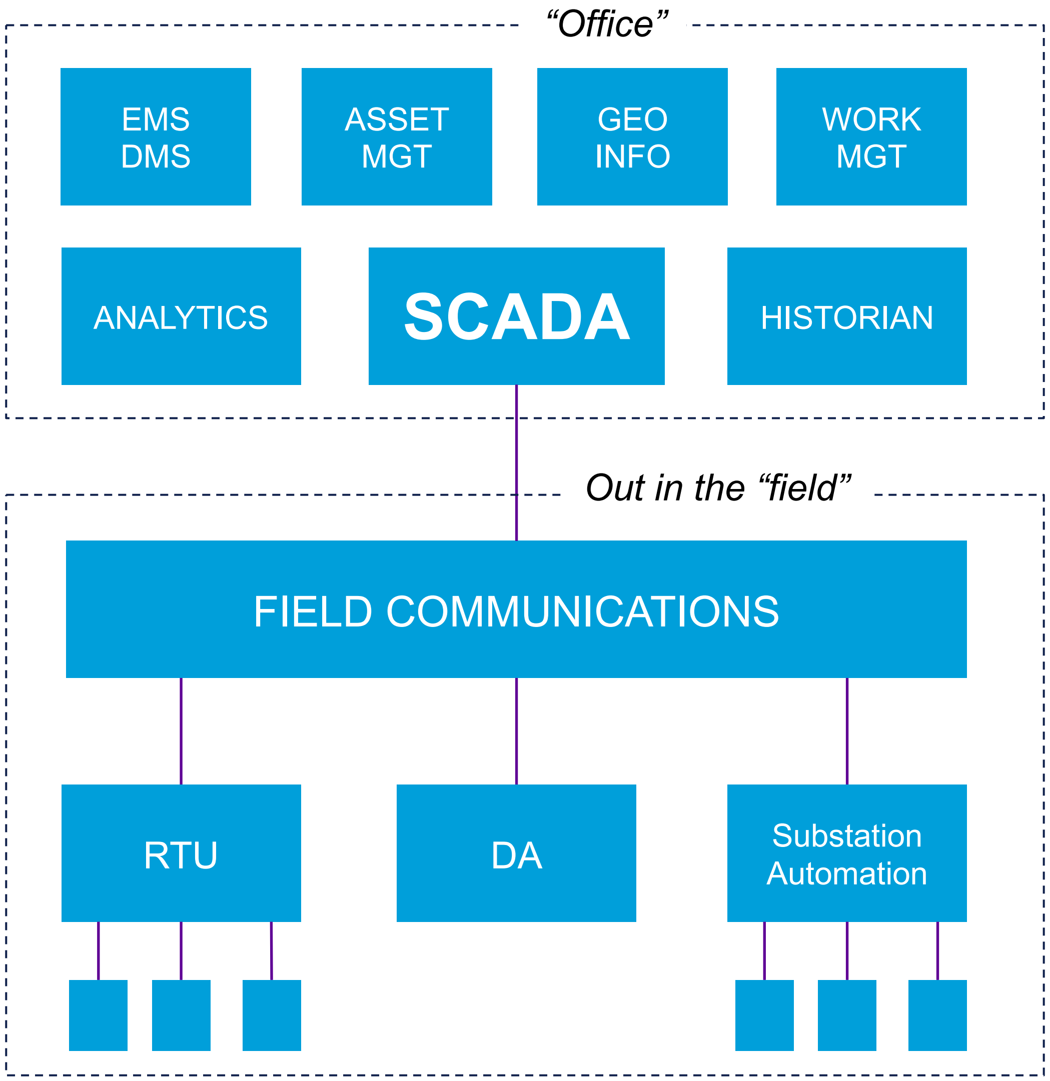
S = Safety
A = Availability
I = Integrity
C = Confidentiality

IT for **OT**

Grid/Plant Operations

OT + “IoT”

Grid/Plant Processes



Utility Business → Continuing Energy Supply – *Many systems + Apps involved*

C = Confidentiality
I = Integrity
A = Availability

IT

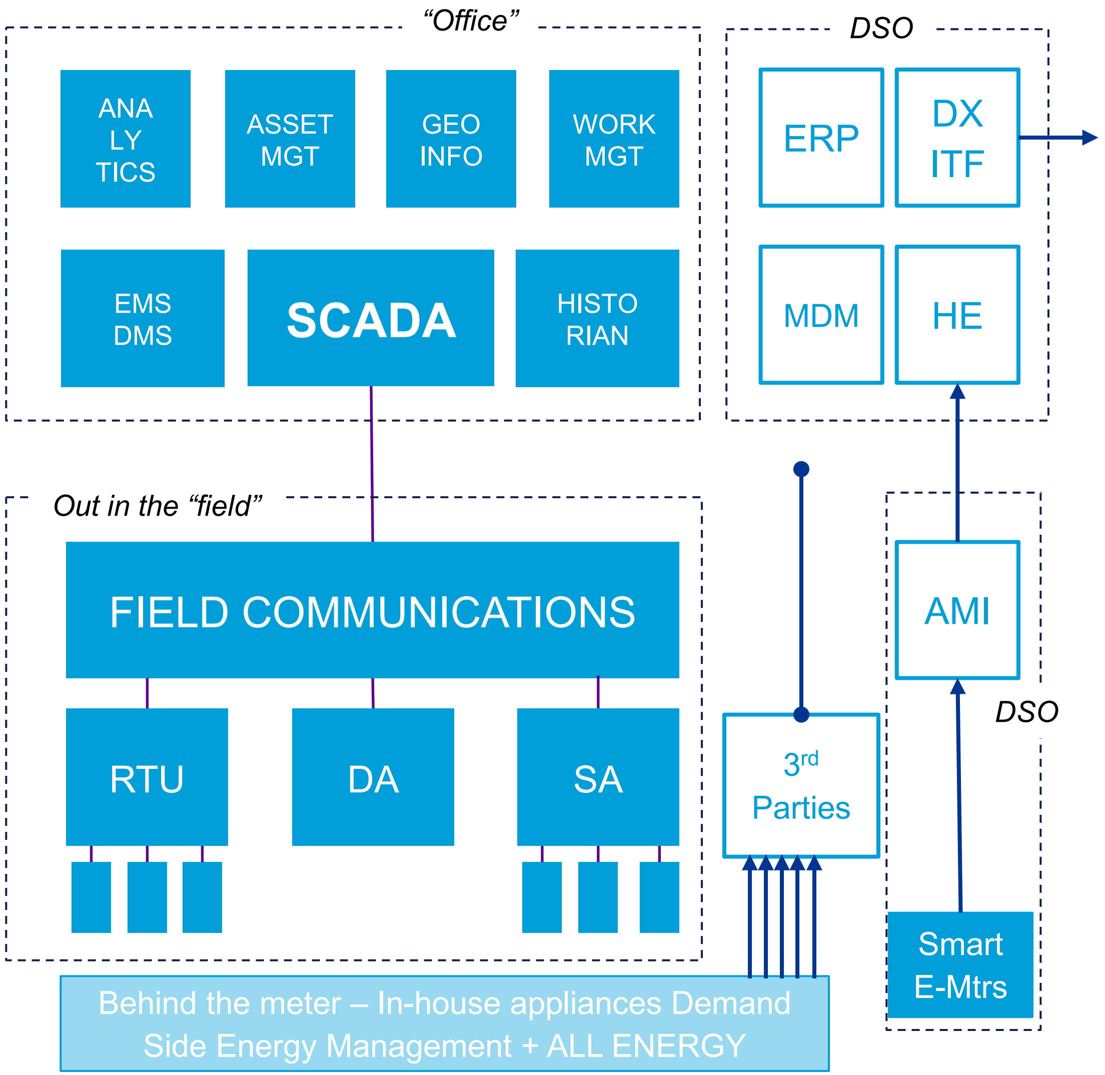
S = Safety
A = Availability
I = Integrity
C = Confidentiality

IT for **OT**

Grid/Plant
Operations

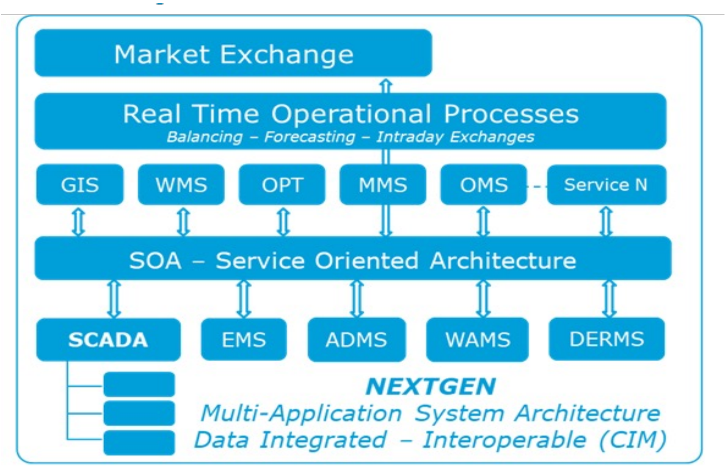
OT + "IoT"

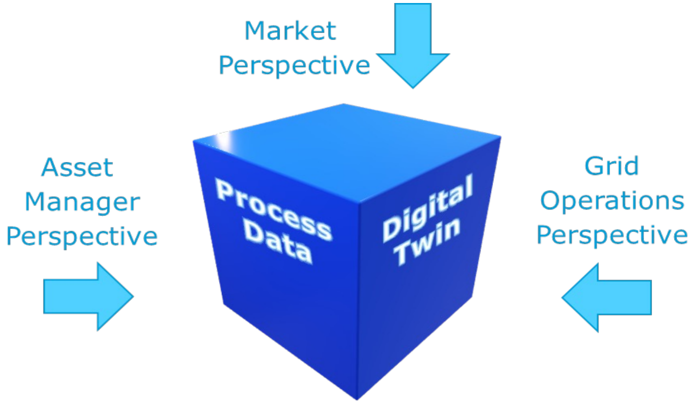
Grid/Plant
Processes



Digitalisation – Digital Transformation

Grid Ops Applications


Market Exchange
Real Time Operational Processes
Balancing – Forecasting – Intraday Exchanges
GIS
WMS
OPT
MMS
OMS
Service N
SOA – Service Oriented Architecture
SCADA
EMS
ADMS
WAMS
DERMS
NEXTGEN
Multi-Application System Architecture
Data Integrated – Interoperable (CIM)



Real-time Data Exchanges Grid Ops Applications

Real-time Exchanges

Automation & Communication

SA RTU	Distribution Automation	Smart Meters
Transformer Sensors	Smart Cable Guard	DERMS Aggre- gators
DLR	IoT Sensors	Home Energy Mgt System

Structured DATA of Assets

Single version of the **TRUTH**

Quality Data:
- Value
- Time
- Timely

Data Exchange via **Common Data Model** many different user groups / use cases:
- internal
- external

Structured & Standardised Data

Secure Architectures – Security by Design – Security Standard

Applying utility cyber security standards

IT Systems
ISO 27001(x)

OT Systems
IEC 62443

Process Controls
IEC 62443-2-1

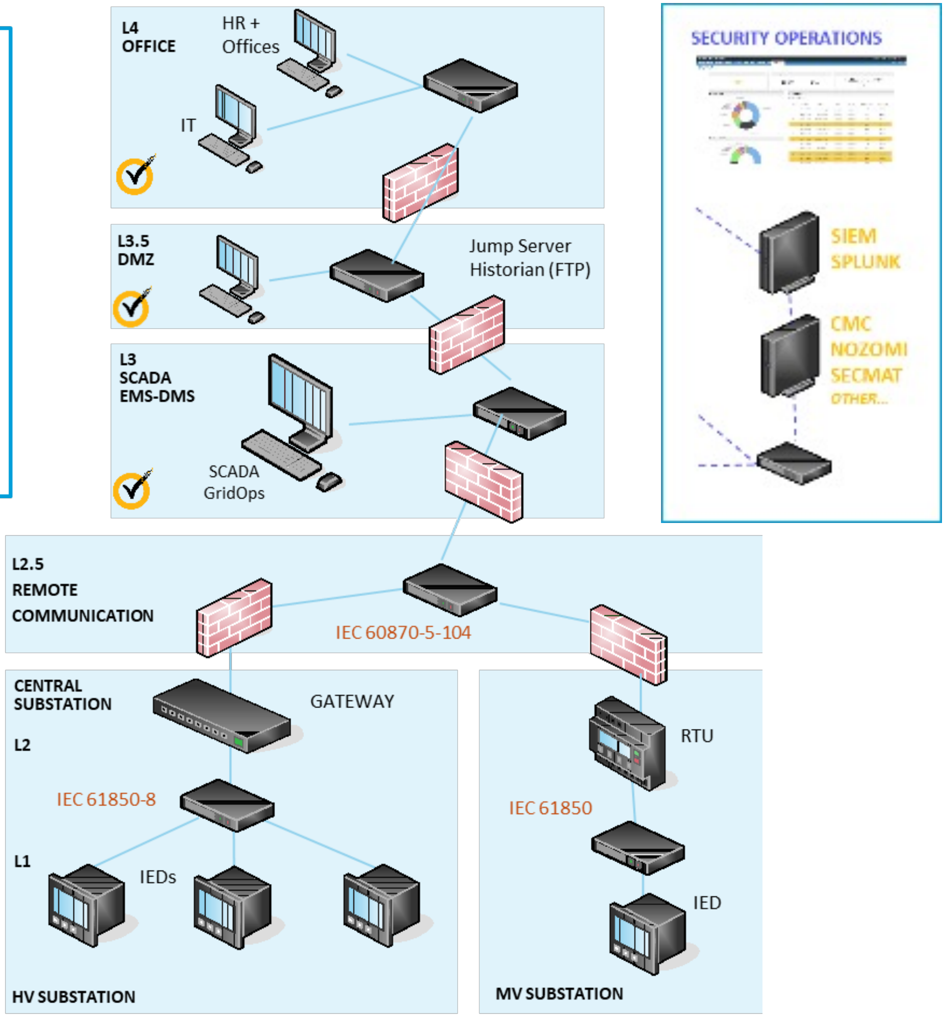
Tech. Security Levels
IEC 62443-3-3

Prot. + IED Security
IEC 62351

Grid Operations
Network/System Operators – Utilities
Portfolio Managers – Power Producers

SCADA + GridOps Systems
Secure System Architectures
Remote Control – Remote Access

SCADA Protocols
ICCP
IEC-101/104
IEC 61850
IED's



Add Power Generators:

- Large – DCS + SCADA connected to TSO
- Windmills (parks) – DER
- Solar (fields)

Add Smart Metering + Comms Infra

Add ICCP – TSO-TSO-RSC + DSO-TSO

Implementing your SECURITY STRATEGY – Risk Based

Security Framework *IT + OT + IT for OT + IoT*

Security Organization *RACI – Responsible/Accountable/Consult/Inform*

Security Operating Model *Security Controls – Maturity Levels – PDCA*

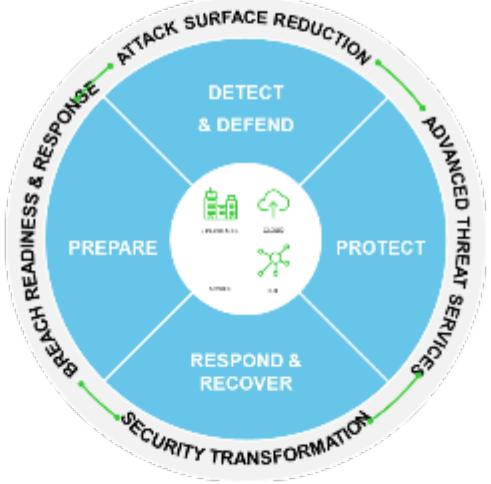
From Strategy → to → Transformation → to → Managed Security & Cyber Defense

Preprare
- Strategy & Business Alignment
- Assessment & Architecture
- Governance, Risk & Compliance
- People & Culture Change

Protect
- Application & Data Security
- Platform & Infrastructure Security
- Digital Identity

Detect & Defend
- Vulnerability Management & Threat Intelligence
- Advanced Adversary Simulations
- Security Monitoring
- Cyber Threat Analytics

Respond & Recover
- Incident Response
- Remediation

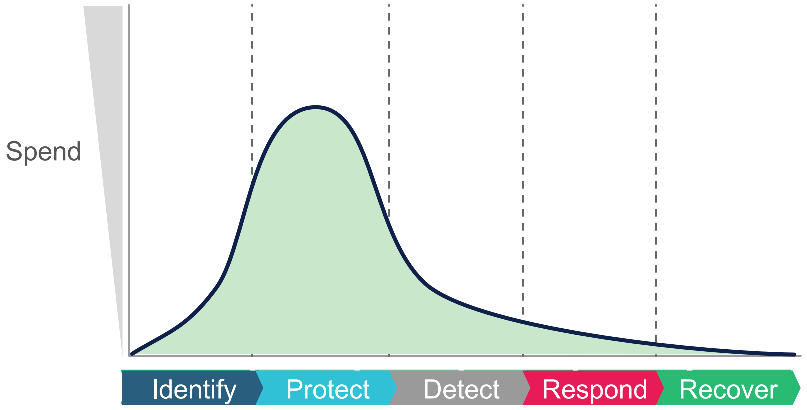


MANAGE YOUR SECURITY SERVICES

- Cyber asset management + detect unknown devices
- Vulnerability management
- Threat detection
- Incident management & reporting
- Response & recovery
- Governance
- Risk management process
- Supply chain
- System hardening
- Staff awareness & training

Company spend has been shifting from purely protection to building capabilities for reacting and recovering as fast as possible

Historical

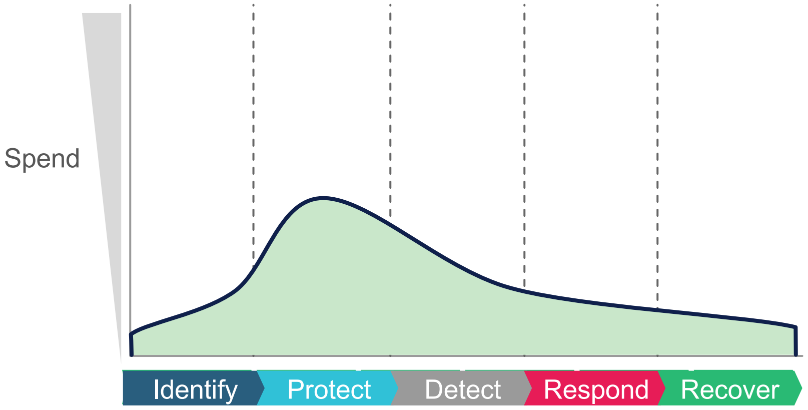


Highest possible protection

Primary focus was on protection and to avoid security breaches

Since it is practically impossible to guarantee 100% protection, the market has shifted to increasing capabilities for reacting and recovering as fast as possible

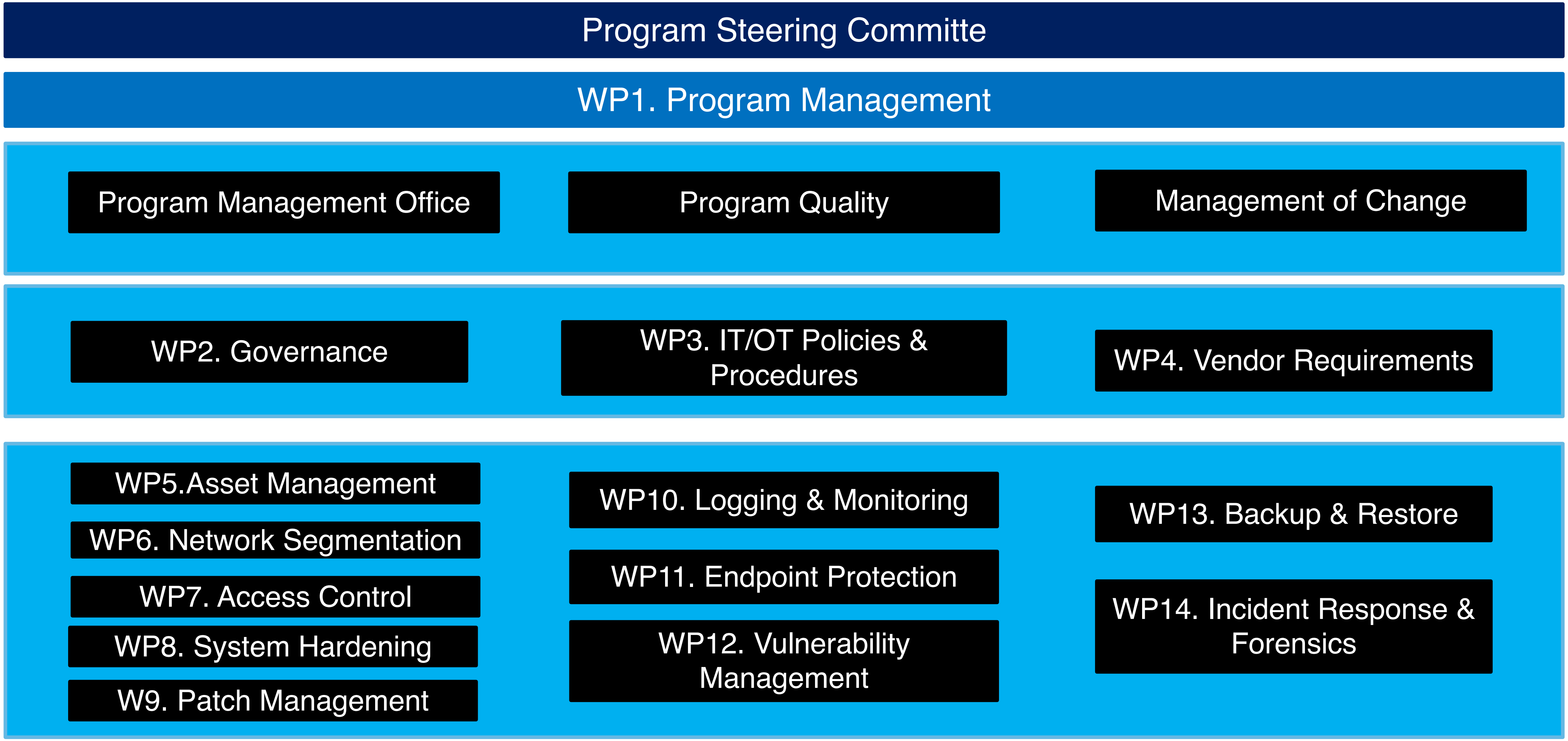
Today



Market best-practice

Incremental increase of detection, response and recovery capacities

Case Study - Program Governance



Program Steering Committe

WP1. Program Management

Program Management Office

Program Quality

Management of Change

WP2. Governance

WP3. IT/OT Policies & Procedures

WP4. Vendor Requirements

WP5.Asset Management

WP6. Network Segmentation

WP7. Access Control

WP8. System Hardening

W9. Patch Management

WP10. Logging & Monitoring

WP11. Endpoint Protection

WP12. Vulnerability Management

WP13. Backup & Restore

WP14. Incident Response & Forensics

Preventing security breaches must start at the top

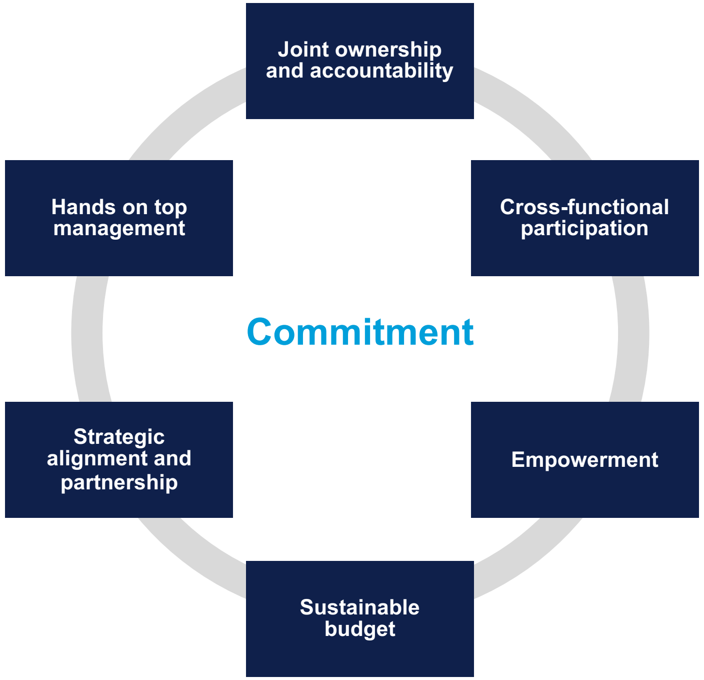
Technology alone will not stop successful threat actors attacking your company. C-level executives must lead the way in planning implementing and monitoring effective security initiatives.

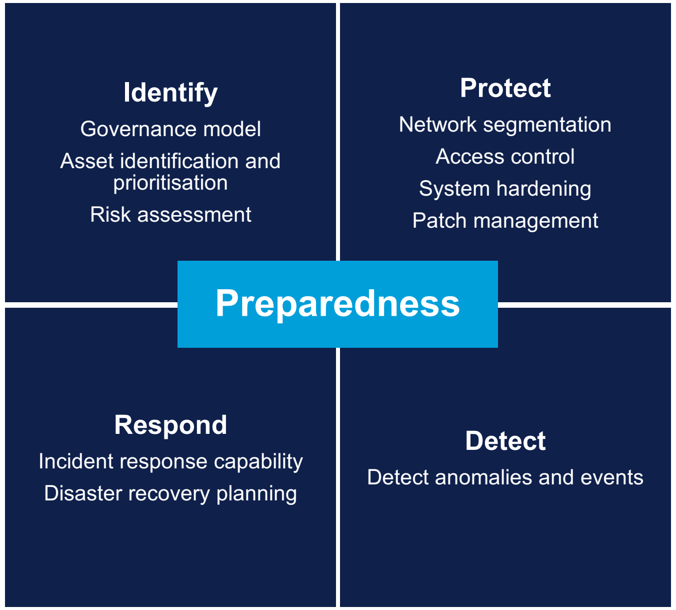
Commitment

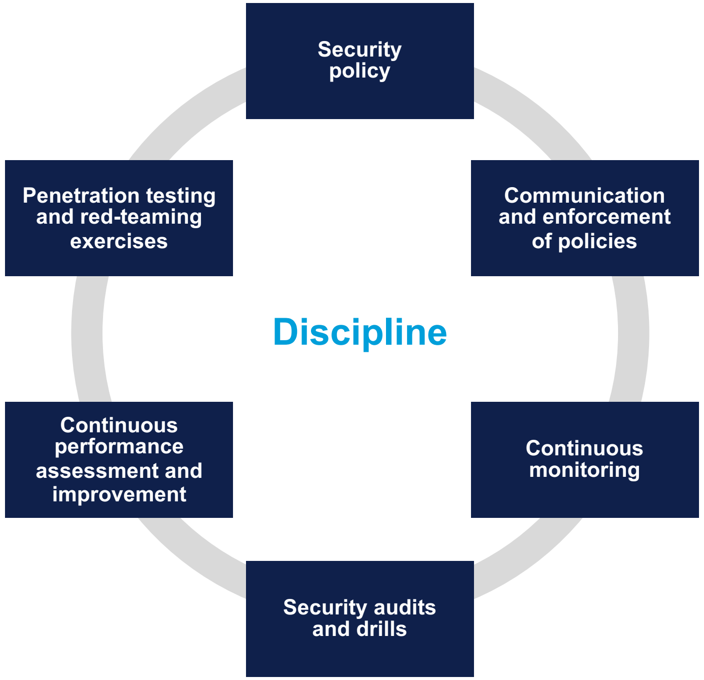
Preparedness

Discipline

Supreme ingredients


Joint ownership and accountability
Hands on top management
Cross-functional participation
Commitment
Strategic alignment and partnership
Empowerment
Sustainable budget




Security policy
Penetration testing and red-teaming exercises
Communication and enforcement of policies
Discipline
Continuous performance assessment and improvement
Continuous monitoring
Security audits and drills

RECOMMENDATIONS

Strategic & tactical recommendations

Regardless of the belief of state-sponsored cyber attacks, these recommendations are example steps for any organization looking to prevent cyber attacks to their environments.

- Address cybersecurity as continuous journey (People, Process and Technology) and business enabler
- Adopt relevant international standards such as IEC 62443/NIST series
- Collaborate with your vendors and service providers
- Stay sharp and vigilant.

> “The stakes are high, so don’t play Russian roulette with your OT security… ”

WHEN TRUST MATTERS

Thank you.

Jalal@applied-risk.com

www.dnv.com
www.applied-risk.com

DNV