Cyber Security – The Key Tests

02/04/2019 | Steve Ross

CATAPULT
Offshore Renewable Energy

Agenda

- Who are ORE Catapult?
- Cyber security – what's in store?
- Some trends – none of this bit is good!
- How you can start to change things

Offshore Renewable Energy Catapult

Our mission

To accelerate the creation and growth of UK companies in the ORE sector

Our vision

By 2023, ORE Catapult will be the world's leading offshore renewables technology centre

- **Centres of Excellence**
- **Academic Research Hubs** in partnership with leading universities
- **Expanding our assets in Blyth and Levenmouth** the world's foremost open-access facilities

Our Impact

Our impact in 2017/18 and since 2013

What we are doing in data analytics

- Already run the industries benchmarking programmes – SPARTA and WEBS
- Recently conducted an industry wide research programme looking at the next generation of data needs
- Have a dedicated team based in the UK to support the industry in AI, ML and big data analytics and data sharing platform.

SPARTA Portfolio Review

webs
WIND ENERGY BENCHMARKING SERVICES

WEBS

So why am I here discussing Cyber Security?

Cyber Security – In the Offshore Wind Industry???

- We deal with petabytes of data across the industry every day.
- The majority of the data is operationally sensitive, in terms of power generation, IP or costs.
- We deal with numerous suppliers, partners and associates that need access to data or are feeding data to our business'.
- The industry is fast moving towards data dependency and a groundswell of different skills and capabilities.
- We are using multiple devices and technology that give access to numerous people to our businesses.

What a data network looks like

Wind Farm

Storage

Transformers/
Switchgear

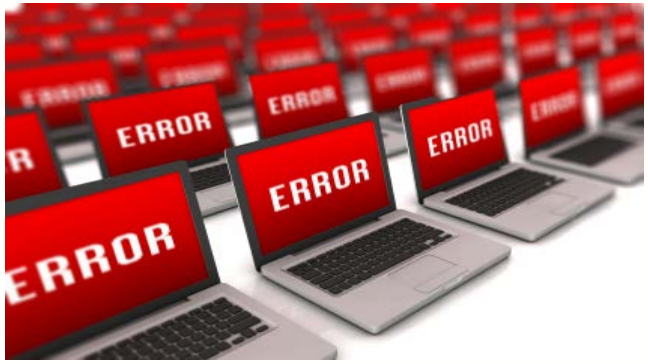
Sub-stations

Grid Connection

No option is not an option

What the next few years looks like

- Data theft and ransoms are turning to data manipulation, that could bring down businesses and reputations
- Already a global demand/ shortage of cyber security people and skills
- Hackers will get smarter and become more organised and professional
- Breaches will become more complex and harder to overcome
- Cyber Risk Insurance will become more prevalent



What are the trends predicted for the next 5 years

Who the industry is fighting

Organised Crime

- Hackavist
- Ransom
- Theft of company IP

Terrorist

- Hijack control
- Sabotage and destroy data/ shut down plants and operations.

Nation States (?)

- In the last few years there has been wide-spread disruption of the Ukrainian grid
- Hacks into US, CH and Turkish utilities, with the potential to gain access and control
- Iranian nuclear facility hack and collapse

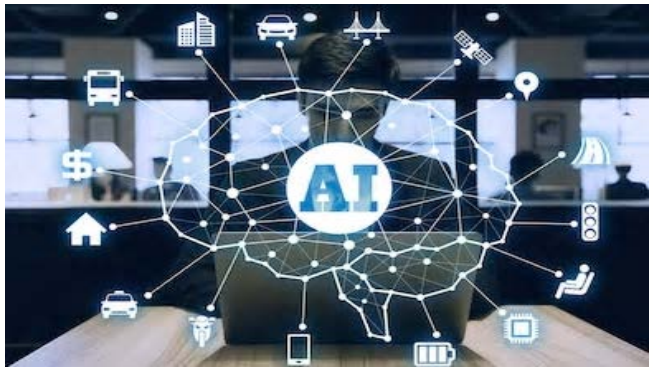
Who we are fighting

Some 2018 stats

Thanks to www.capterra.com

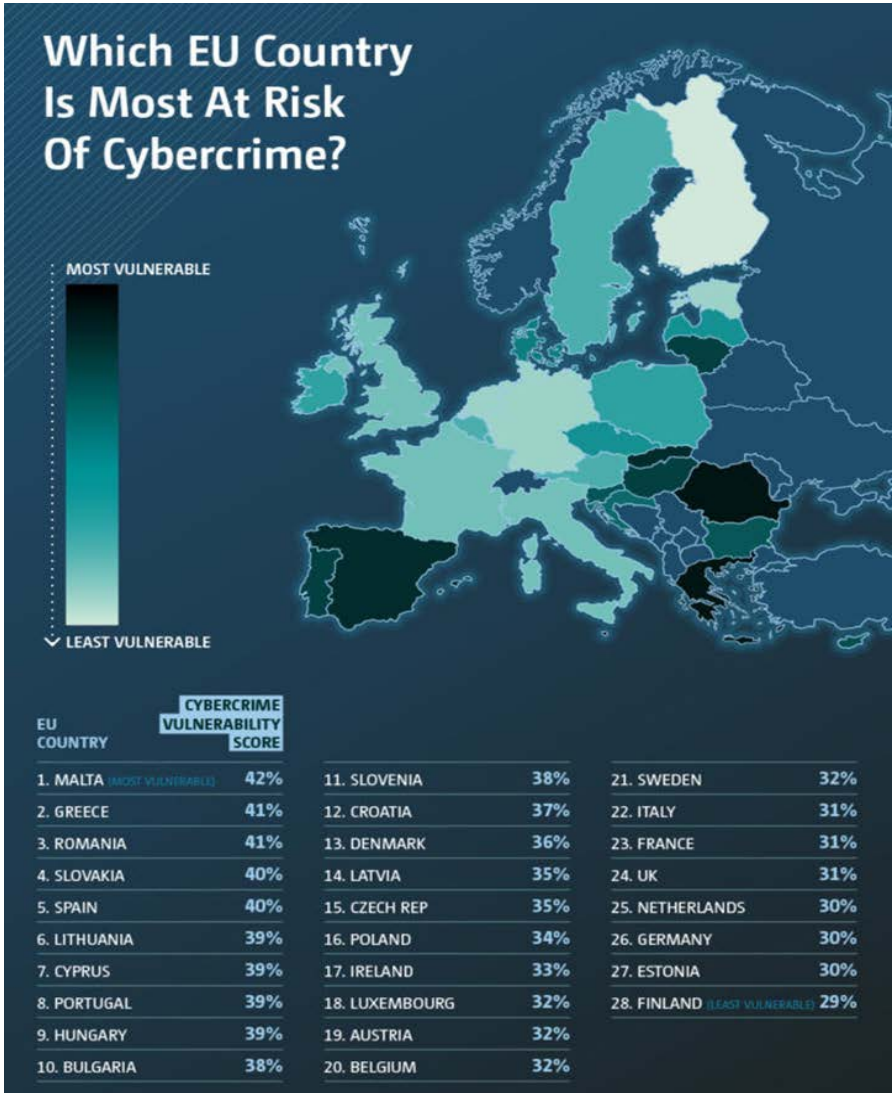
So what can be done

- Have a security plan as strong as your Health and Safety plan – if not stronger
- Understand and use AI as a key tool for your cyber security planning.
- Become hackers – or employ them, to test your systems and look for back doors, loopholes and access areas.
- Work with your supplier and partners to they comply to your cyber security rules
- Take it seriously – don't wait for a breach to take action



Have a plan

- How is AI being used in your business and do you have a deep understanding of how it is used and where it can be compromised?
- Know in detail what your key assets are and how they can be protected.
- Plan protection breaches regularly and be in a state of awareness if they should ever be attacked.
- Manage IoT and anyone that can access your data.
- Brief your supply chain they MUST comply to your rules – never the other way round.



EU COUNTRY	CYBERCRIME VULNERABILITY SCORE
1. MALTA (MOST VULNERABLE)	42%
2. GREECE	41%
3. ROMANIA	41%
4. SLOVAKIA	40%
5. SPAIN	40%
6. LITHUANIA	39%
7. CYPRUS	39%
8. PORTUGAL	39%
9. HUNGARY	39%
10. BULGARIA	38%
11. SLOVENIA	38%
12. CROATIA	37%
13. DENMARK	36%
14. LATVIA	35%
15. CZECH REP	35%
16. POLAND	34%
17. IRELAND	33%
18. LUXEMBOURG	32%
19. AUSTRIA	32%
20. BELGIUM	32%
21. SWEDEN	32%
22. ITALY	31%
23. FRANCE	31%
24. UK	31%
25. NETHERLANDS	30%
26. GERMANY	30%
27. ESTONIA	30%
28. FINLAND (LEAST VULNERABLE)	29%

When did you last hack your business?

Test you data access protocols to the point where it becomes a part of your business

Condition Blues

This is your IT and security teams trying to hack into your own systems – looking for loopholes and access points, weaknesses.

Condition Reds

Using an external "hack team" to try and break into your system – be VERY selective here

Condition Whites

This involves your supply chain and a duality between your systems and theirs.

Keep up to date and collaborate within the industry to make cyber security an industry standard

…and what are ORE Catapult doing?

- We run an operational turbine in Scotland as well as highly valuable assets generating copious data – so it's a part of what we do – 24/7.
- We are trusted to run industry joint programmes such as SPARTA and WEBS where we manage GW's of operational sensitive data for a high percentage of the off and on-shore operators.
- In early summer we will be hosting round tables with industry and outside expertise for a lessons learning programme and to start wider industry collaboration and develop best practice. As well as actively supporting WindEurope with their data leadership.
- **Please get involved!**

Thank you for listening, please don't have nightmares!

Any questions?

Where to find us

Contact us

GLASGOW
Inovo
121 GeorgeStreet
Glasgow
G1 1RD

T +44 (0)333 004 1400

BLYTH
National Renewable Energy Centre
Offshore House
Albert Street
Blyth, Northumberland
NE24 1LZ

T +44 (0)1670 359 555

LEVENMOUTH
Fife Renewables Innovation Centre (FRIC)
Ajax Way
Leven
KY8 3RS

T +44 (0)1670 359 555

HULL
O&M Centre of Excellence
Ergo Centre
Bridgehead Business Park
Meadow Road, Hessle
HU13 0GD