The University Of Sheffield.

Cyber Security and Strategic Alignment

Dr Jonathan Rigelsford
Joseph Pindar

2011 THE AWARDS AWARD WINNER UNIVERSITY OF THE YEAR

Acknowledgement

Global Cyber Security Center

Posteitaliane

The University Of Sheffield.

ISACA
Trust in, and value from, information systems

The authors wish to express their gratitude for the financial support of the ECIIA for the initial phase of this work

A little bit about us…

Joseph Pindar

- Principal Solution Specialist - Storage at SafeNet
- Systems Engineer at NetApp
- Worked in Cyber Security and Information Assurance for 10 years
- UK Public Sector designing secure systems & catching bad guys
- Spent 4 years working with UK & international law enforcement on Cybercrime

Dr Jonathan Rigelsford

- Senior Research Fellow / Senior Experimental Officer at the University of Sheffield
- 14 years telecommunications experience
- Industrial past
- Responsible for CRG servers and security
- Spent 3 years working on Risk Analysis for Cyber Security and Information Assurance
- Invited speaker on CS and IA in Rome, Madrid, Stockholm & Vienna.

Contents

- **Strategic Alignment:** *How Cyber Security and Information Assurance interface with other areas of the enterprise is critical to success.*
- ***Communication:*** *The importance of effectively communicating the value of Cyber Security and advantages and disadvantages of Cloud Computing throughout the enterprise.*
- ***Risk Management:*** *Specifically the lack of objective data and the difference in approach compared to other risk management organisations.*
- ***Smart Cities:*** *The benefits and risks of an integrated society.*
- ***Smart Grids:*** *Who controls the power and how we can ensure energy security.*

Fishing, Canapés & Film

Hooks: *Ideas to get you thinking and to take the bait.*

Light bites: *Easy to digest pieces of information, leaving you wanting more!*

Abre los ojos (open your eyes):
Seeing Cyber Security from our perspective.

Research Approach

What is important now?

What is impacting business now?

Interviewed security and IT experts from across UK Public Sector, Finance, Petro-chemical and IT Hardware.

Key ideas

"No such thing as 'secure' anymore."

Debora Plunkett – Head of IA at the National Security Agency U.S.

Dec. 2010 after WikiLeaks

Cybersecurity and Information Assurance are in a period of flux

- Challenges such as cloud computing
- How we consider Cybersecurity and Information Assurance
- Capable Adversaries can enter systems undetected, collect data and exfiltrate undetected.
- Proposed solutions must be **Relevant** and **Actionable**

Strategic Alignment

How Cloud computing, Cybersecurity and Information Assurance interface with other areas of the enterprise is critical to success.

Not a bolt on option.

Cybersecurity and Information Assurance are integral to the enterprise.

- They are no different to manufacturing, marketing or sales.
- Decisions should be driven from the board.

Challenges for Cybersecurity

Learn from other parts of the enterprise

- Stop looking inward – PDF expliots, XSS and SQL are important but what do they mean outside of Cyber Security and Information Assurance teams?
- There is plenty of relevant thinking from other areas of the enterprise.
- Donn Parker referred to Information Security practices as “folk art” – inward looking and having a lack of objective research.

What does ‘risk’ mean?

- Cyber Security and Information Assurance are not unique in developing an concept of risk.
- Alternative Definitions can contribute important insights.

Challenges for Cybersecurity

Communicate effectively

- In tough financial times every part of the enterprise must be delivering value.
- Perhaps more importantly, every part of the enterprise must be **seen** to be delivering value.

How to communicate these messages to the board?

How to affect the way the enterprise operates to ensure security?

Two extremes of Cybersecurity as Operational Effectiveness

- **‘No security: maximum cost savings’**
- **‘Total security: no cost savings’:**

Lessons from the Enterprise

Operational effectiveness and strategy.

Operational Effectiveness

"Performing similar activities *better* than rivals perform them"

Strategy

"being different"

Michael Porter: What is Strategy?

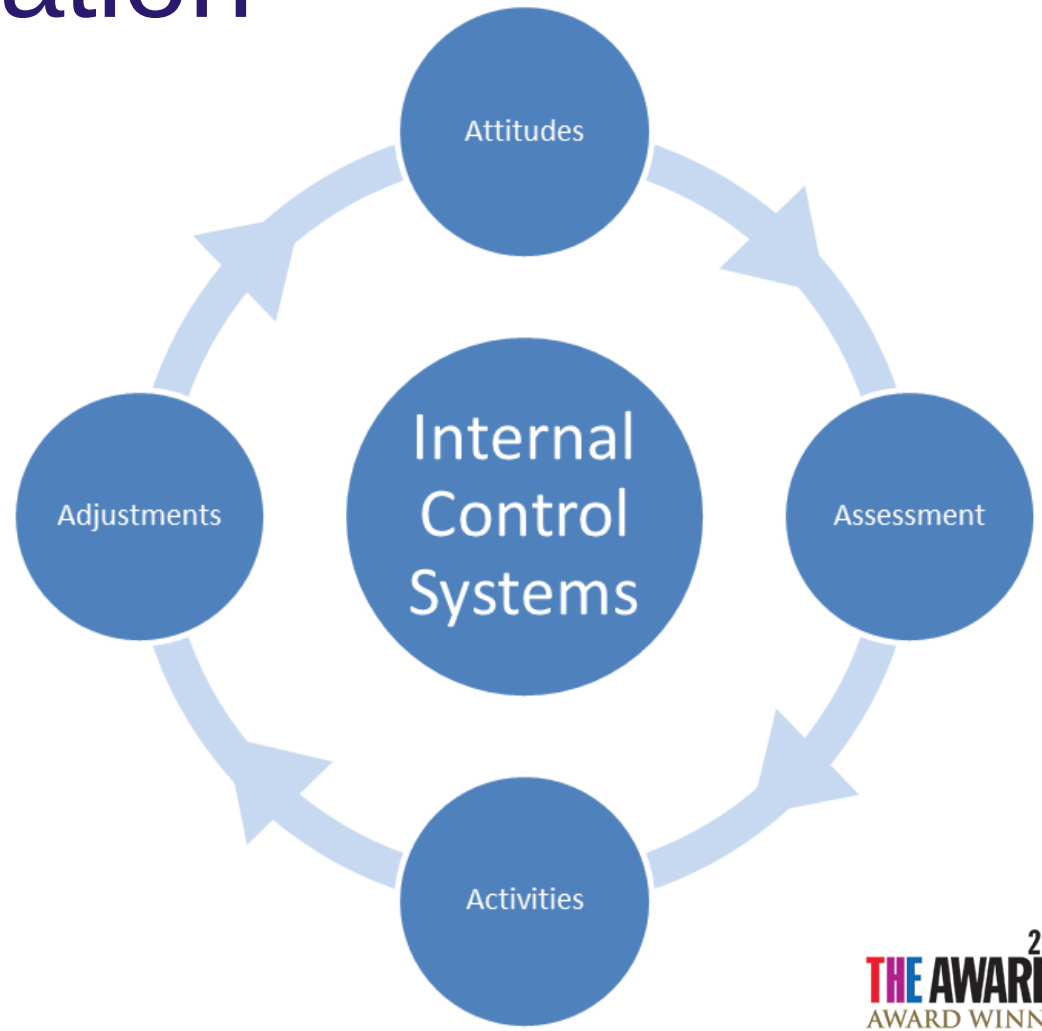
“All a company’s activities, not just a few”

Risk Management

Specifically the lack of objective data and the difference in approach compared to other risk management organisations.

Risks & Mitigation

- Financial risk
- Operational risk
- Compliance risk
- Inherent risk
- Control risk
- Detection risk



What does ‘risk’ mean?

Risk = Probability x Impact

Could be great…

…But

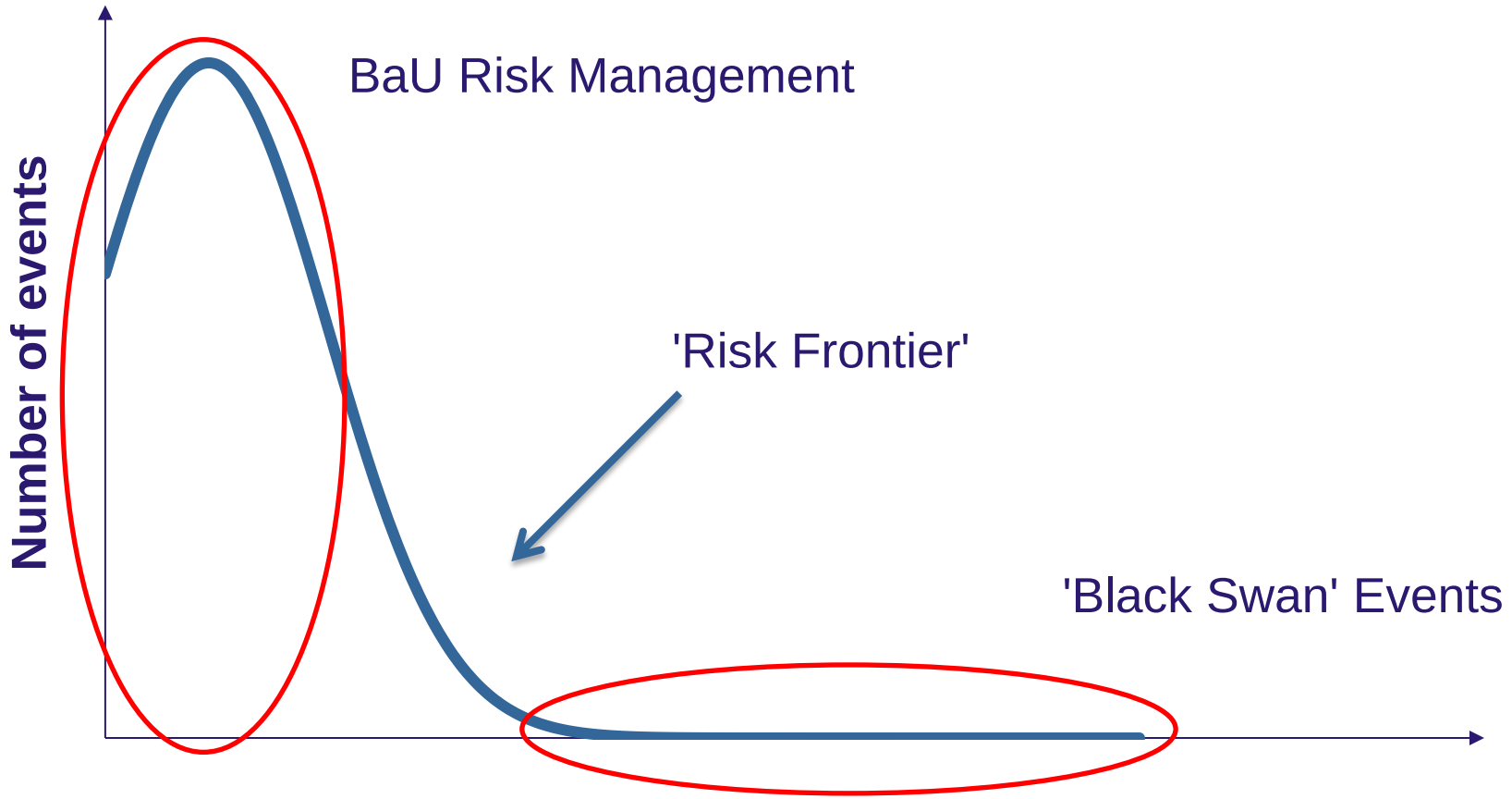
"The numbers are too poor to even lie with" (Geer)

The University Of Sheffield.

Risk = Danger & Opportunity

Accepting a given amount of risk for an expected amount of return.

The Risk Frontier



Questions to ask when considering risk…

- What is our risk appetite?
- What is the perceived threat to our organisation?
- What is the actual historical threat?
- What is the cost to our business if we do nothing?

Effective Communication

The importance of effectively communicating the value of Cyber Security and its advantages and disadvantages throughout the enterprise.

“Communication is what the listener perceives”

Peter Drucker

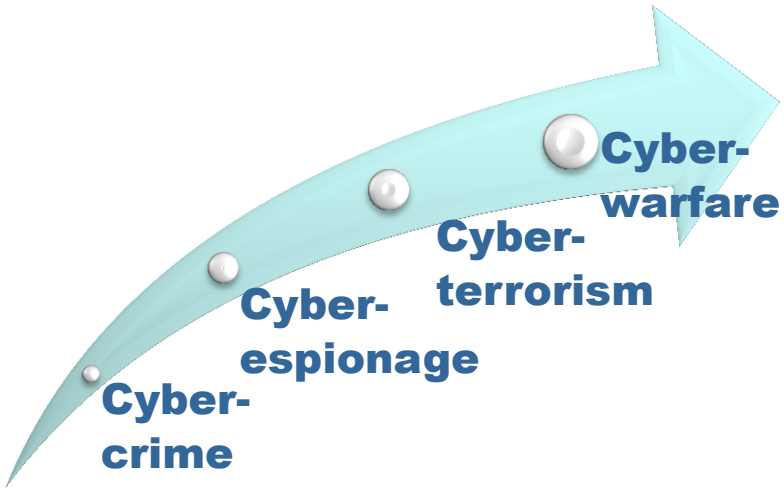
Must differentiate the message depending on the audience:

- *Front-line employees* – ***“what is in it for me?”***
- *The board* – ***“what is the benefit to the enterprise?”***

Effective communication?

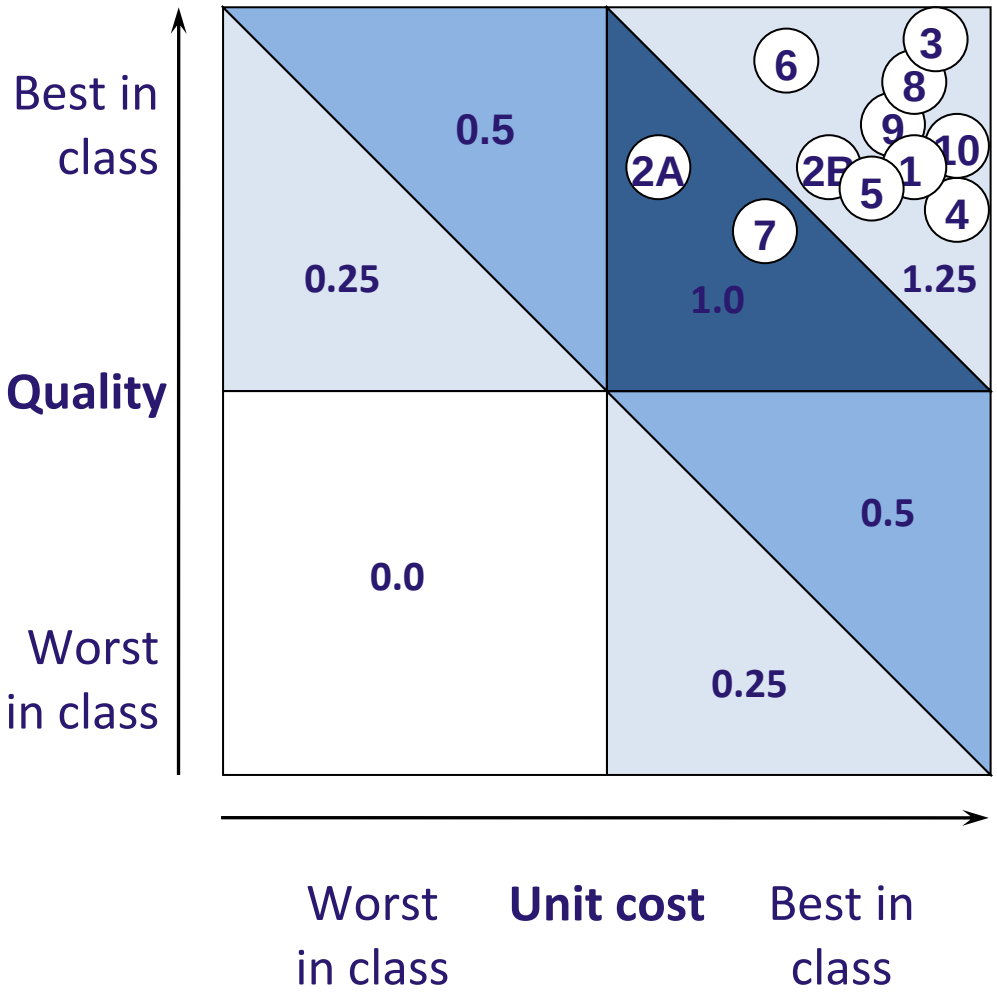
Collections of ‘badness’

Spectrum of fear



Communicating to the board

Security Service	Cost Metrics	Service Level Metrics
Secure Remote Working (Laptop, HDD Encryption & VPN)	• Cost per Laptop • Cost per MB transferred	• Hours of Downtime • Time to Install • Time to Problem Resolution • Performance
Perimeter Protection (Firewalls, Email Scanning & IDS)	• Cost per Mailbox • # of Mailboxes • Cost per MB transferred	• Hours of Downtime • Message Delivery Time • Performance

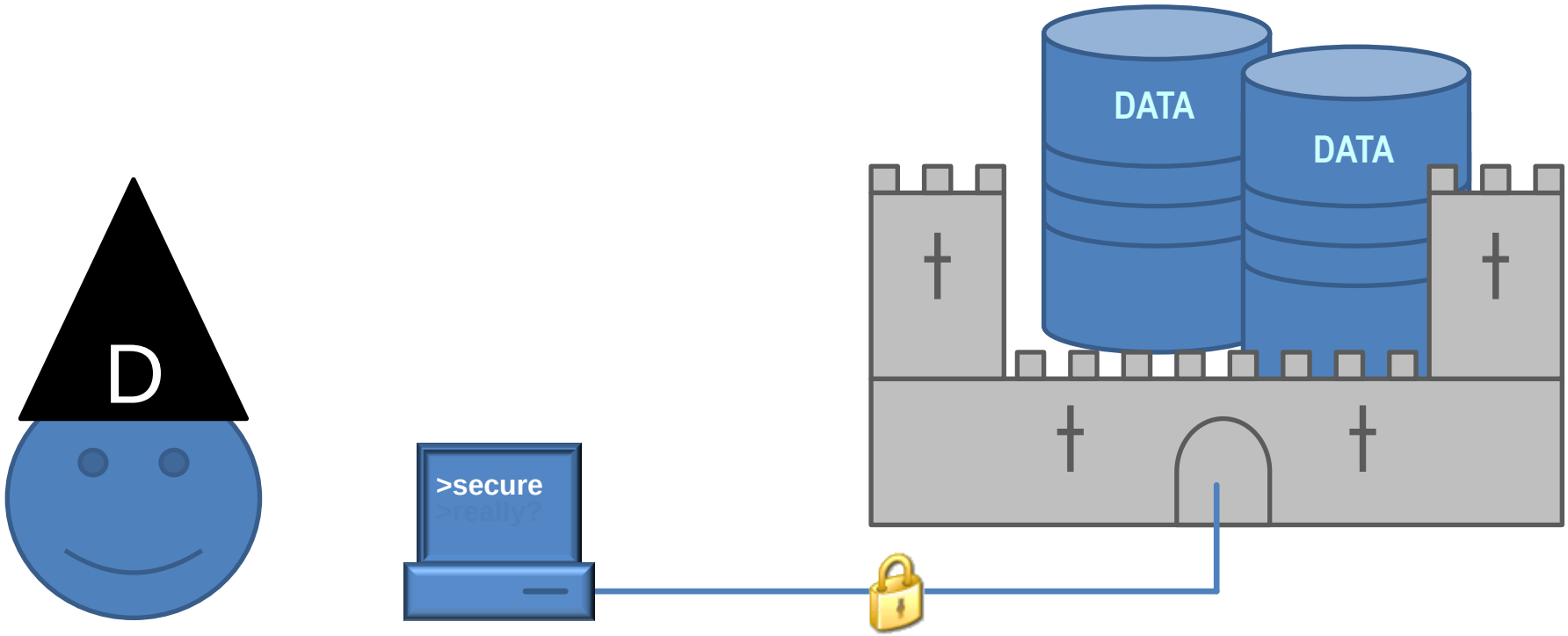


IT products and services

1. E-mail
2A. Laptop
2B. Desktop
3. PBX+VM
4. Enterprise business computing
5. Engineering computing
6. Flex computing
7. Manufacturing computing
8. Mainframe
9. WAN
10. Computing platform

Alternatively….

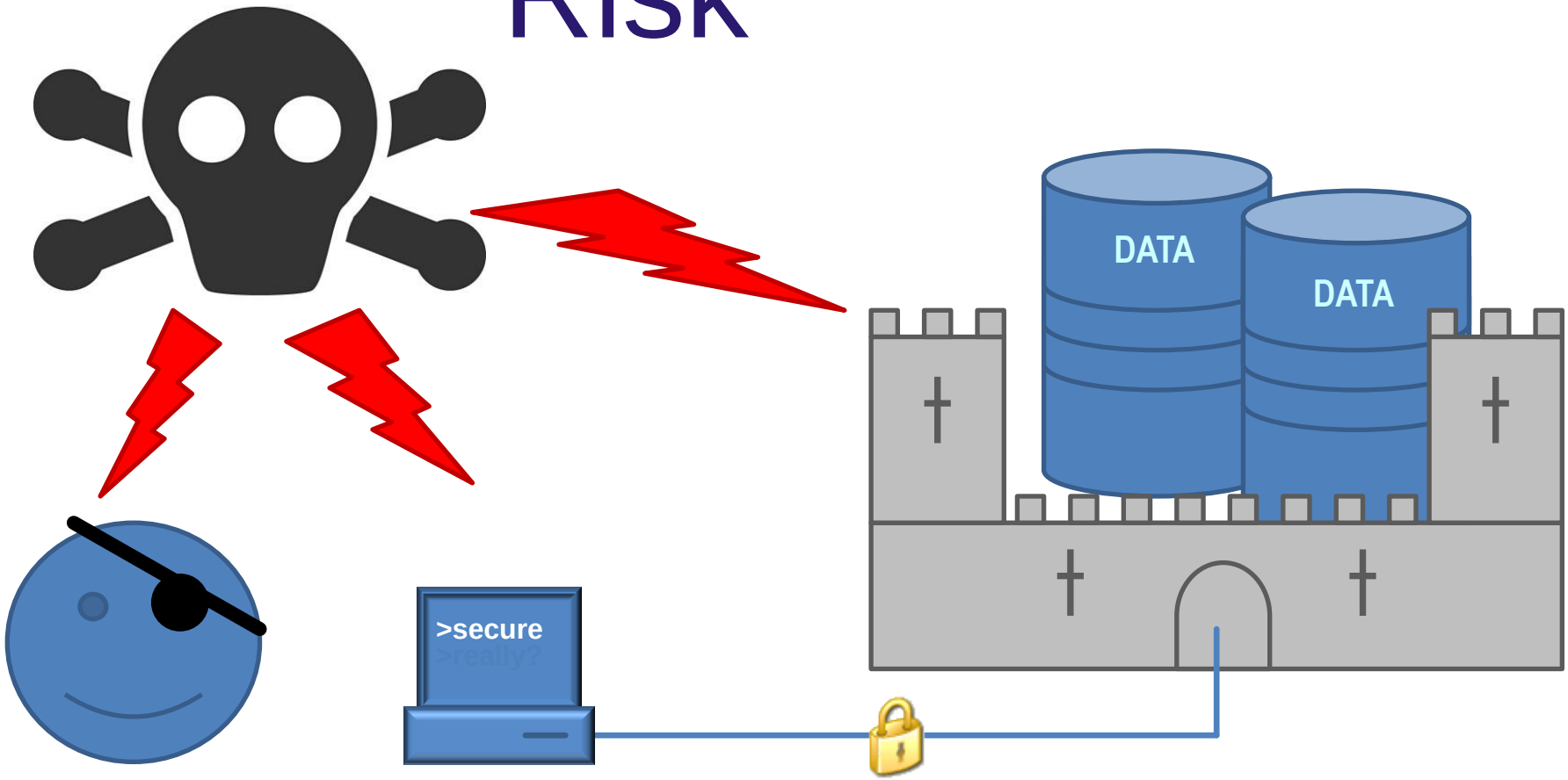
Cybersecurity & Risk



User error: accidental/malicious.

The University Of Sheffield.

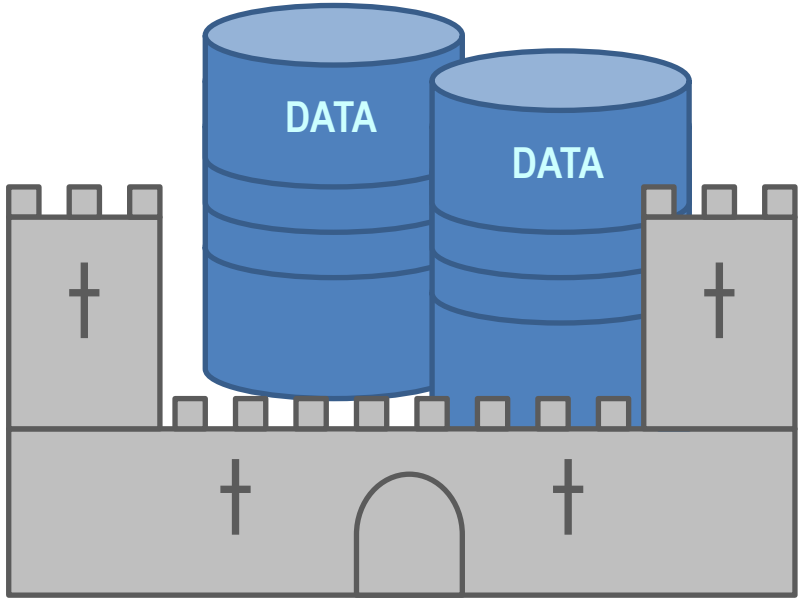
Cybersecurity & Risk



Coercion/Infiltration.

The University Of Sheffield.

Security & Cost



$

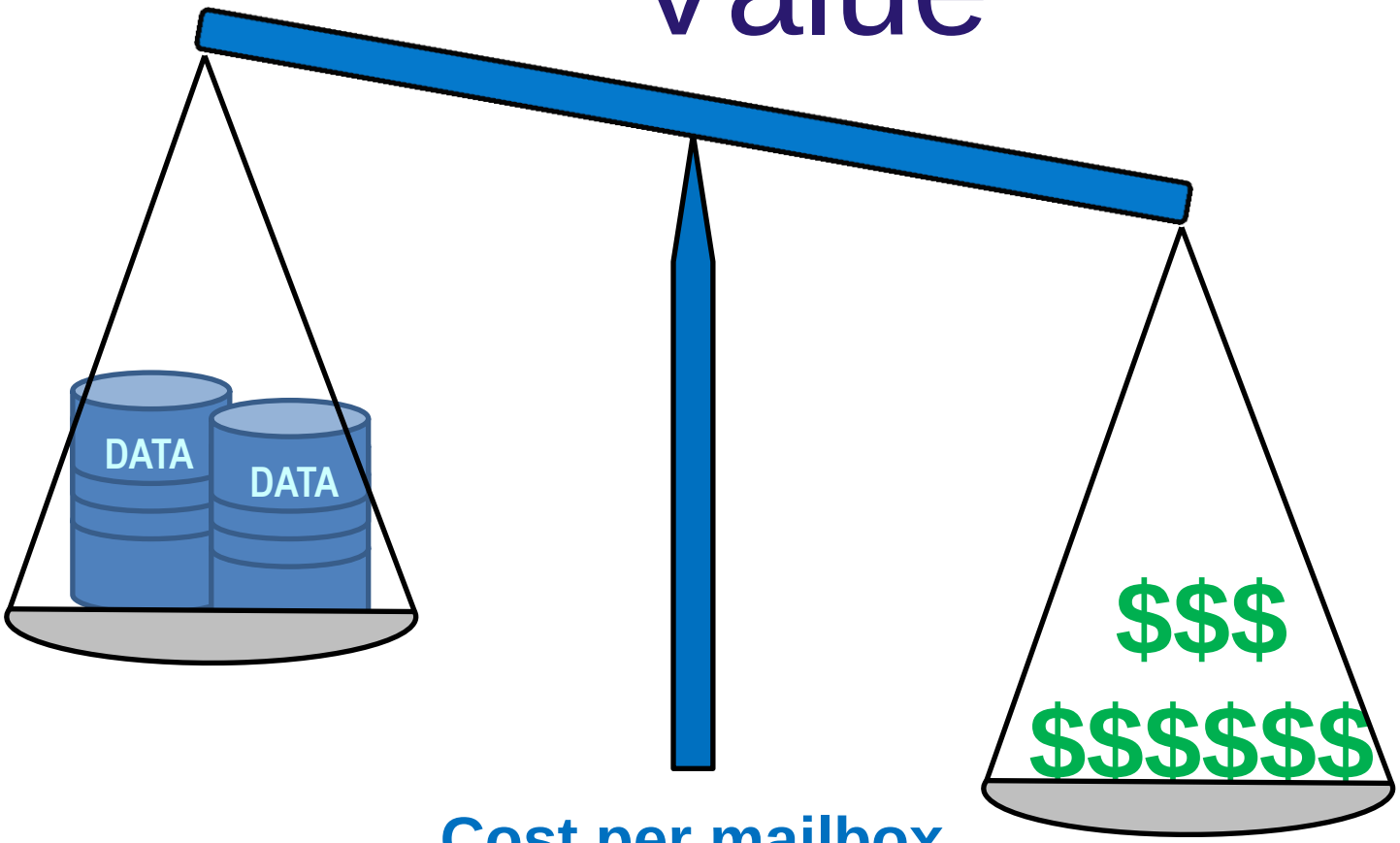
$$$$$$

A higher level of security will cost more.

2011 THE AWARDS AWARD WINNER UNIVERSITY OF THE YEAR

The University Of Sheffield.

Cost Metrics: Value



Cost per mailbox.

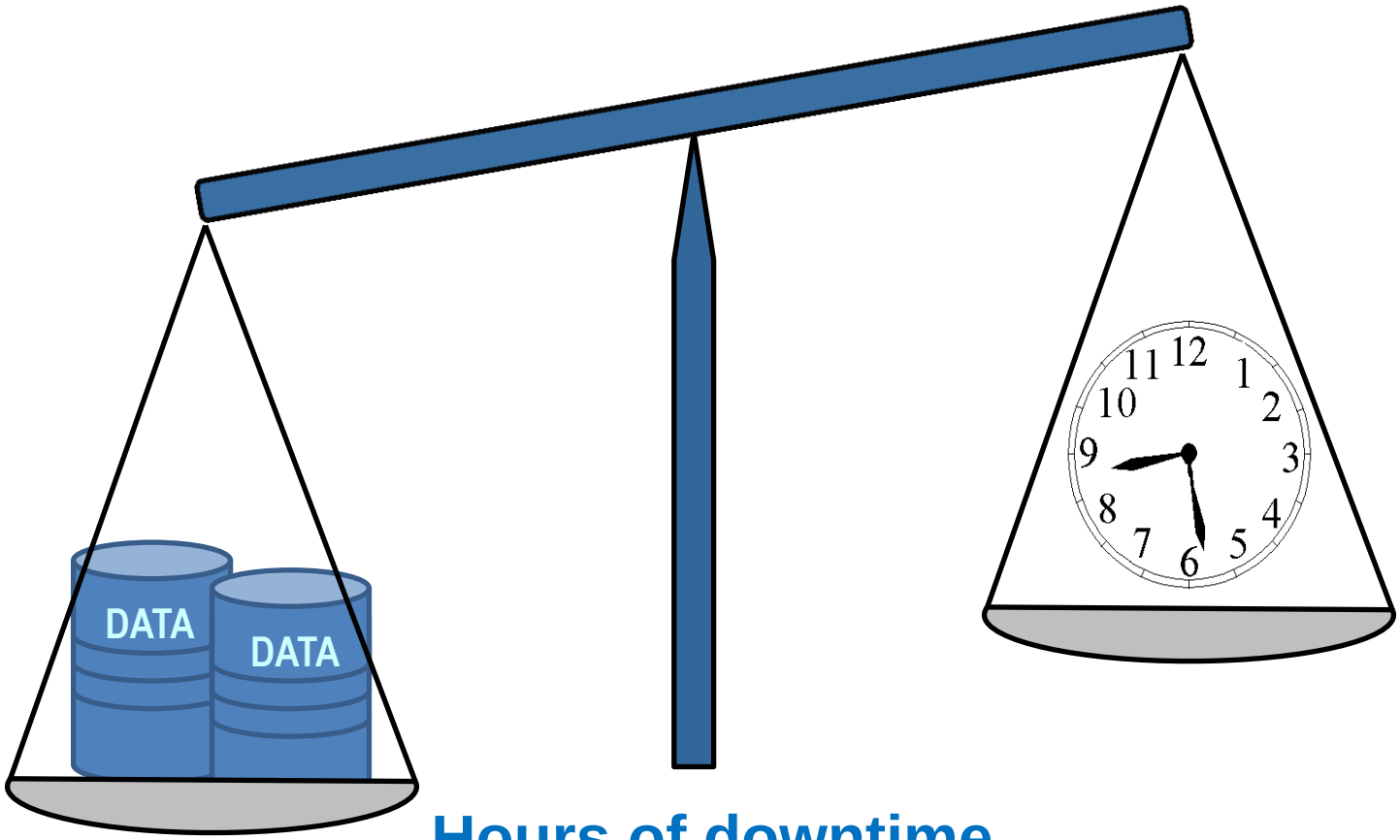
Cost per MB transferred.

Know the worth of what you are trying to protect.

2011 THE AWARDS AWARD WINNER UNIVERSITY OF THE YEAR

The University Of Sheffield.

Service Level: Timeliness



Hours of downtime.
Time to problem resolution.
Performance.

Smart Grids

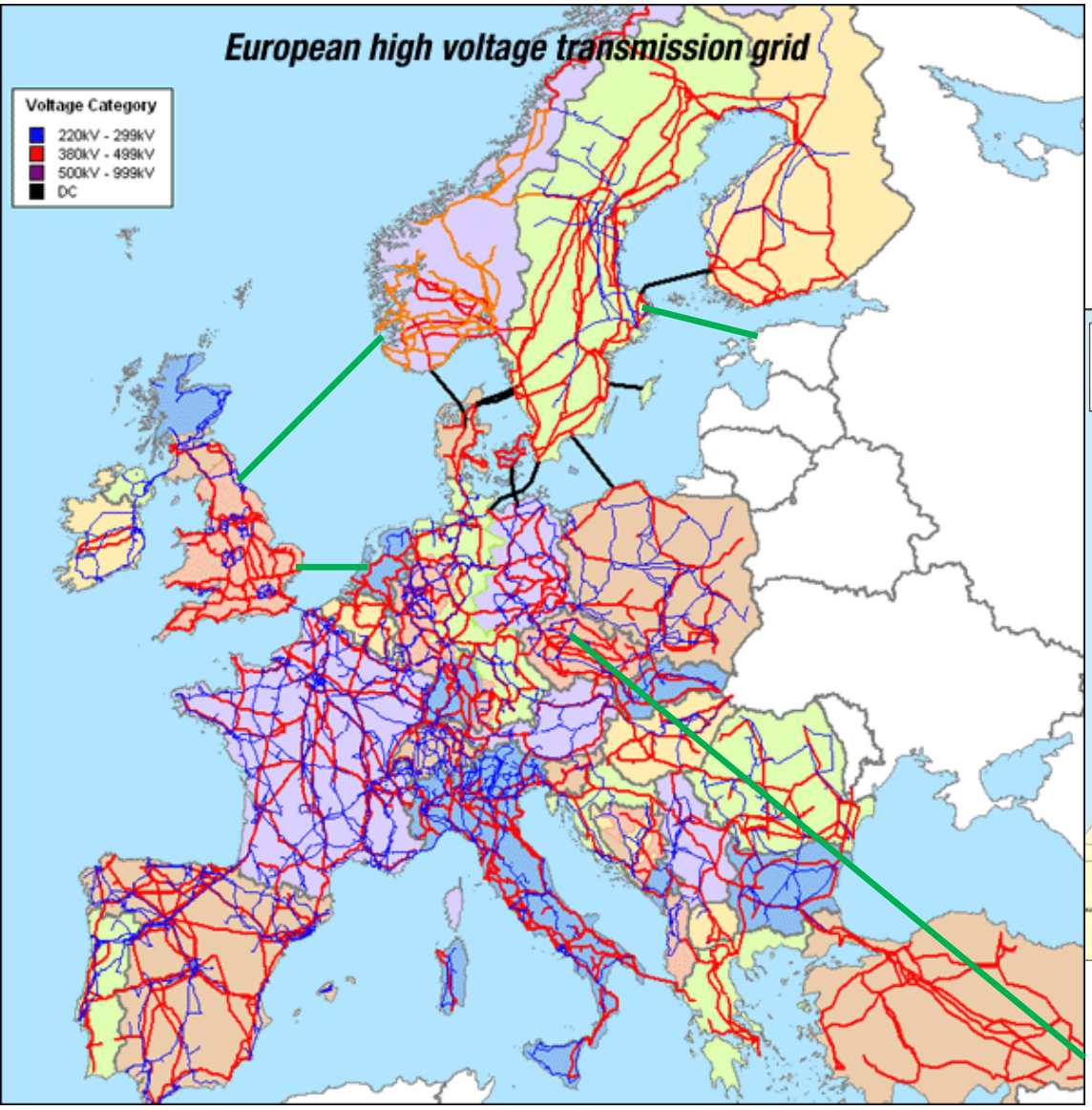
Who controls the power and how we can ensure energy security?

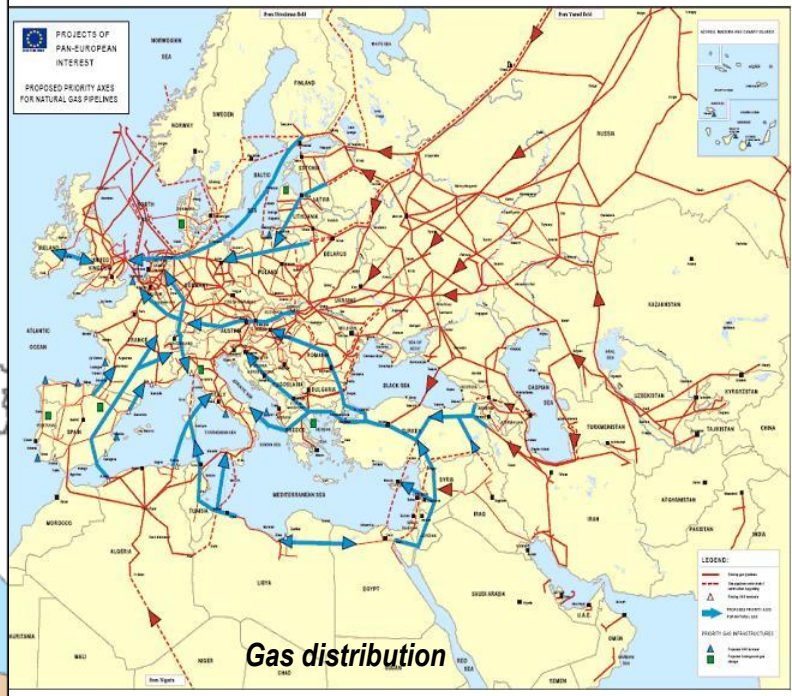
Why use smart grids?

- They provide the opportunity for more reliable transmission of energy and reduced operational energy overheads through intelligent load balancing, and internationally shared resources.
- Historically, spikes or surges in energy consumption were mitigated by having an auxiliary supply available, to provide surplus overhead energy to account for these events.
- Traditional methods are highly inefficient as the surplus energy is wasted.
- More recently fast response gas or hydro turbines have been used to compensate for predictable short duration high demand energy spikes.

The University Of Sheffield.

Energy distribution



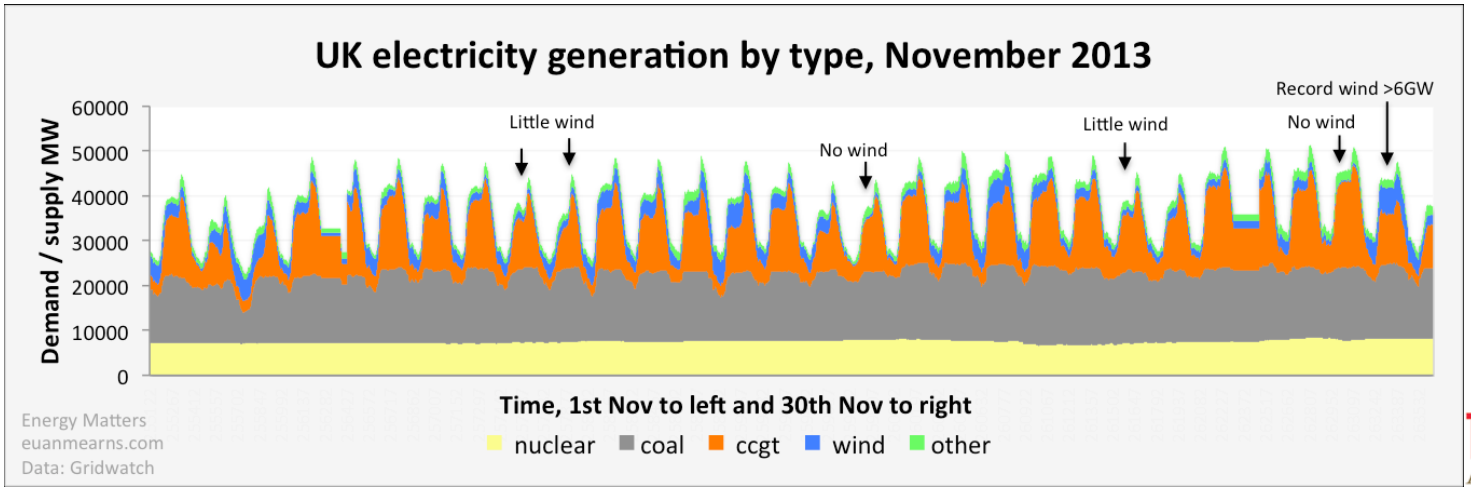


Gas distribution

2011 THE AWARDS AWARD WINNER UNIVERSITY OF THE YEAR

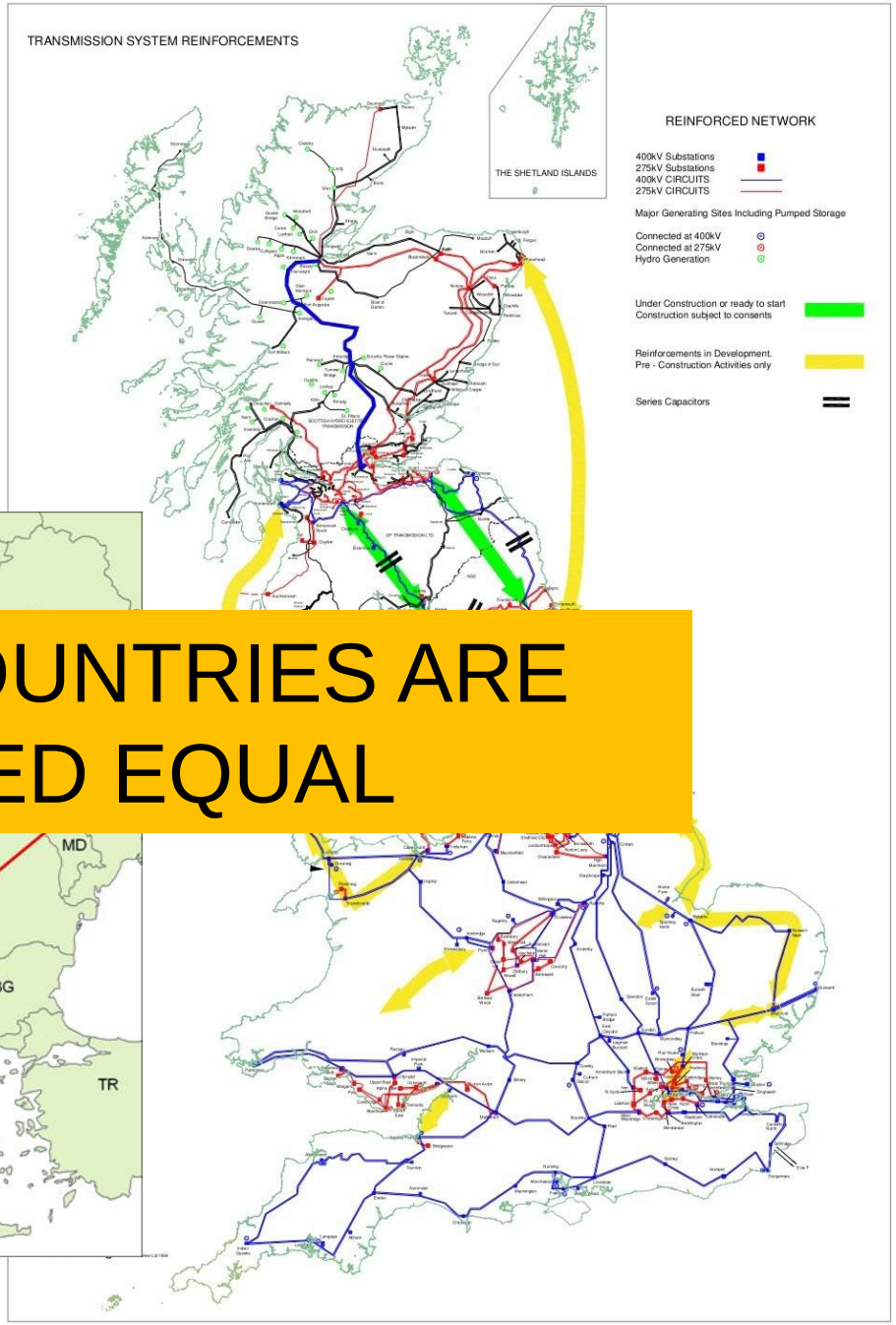
Smart Grids

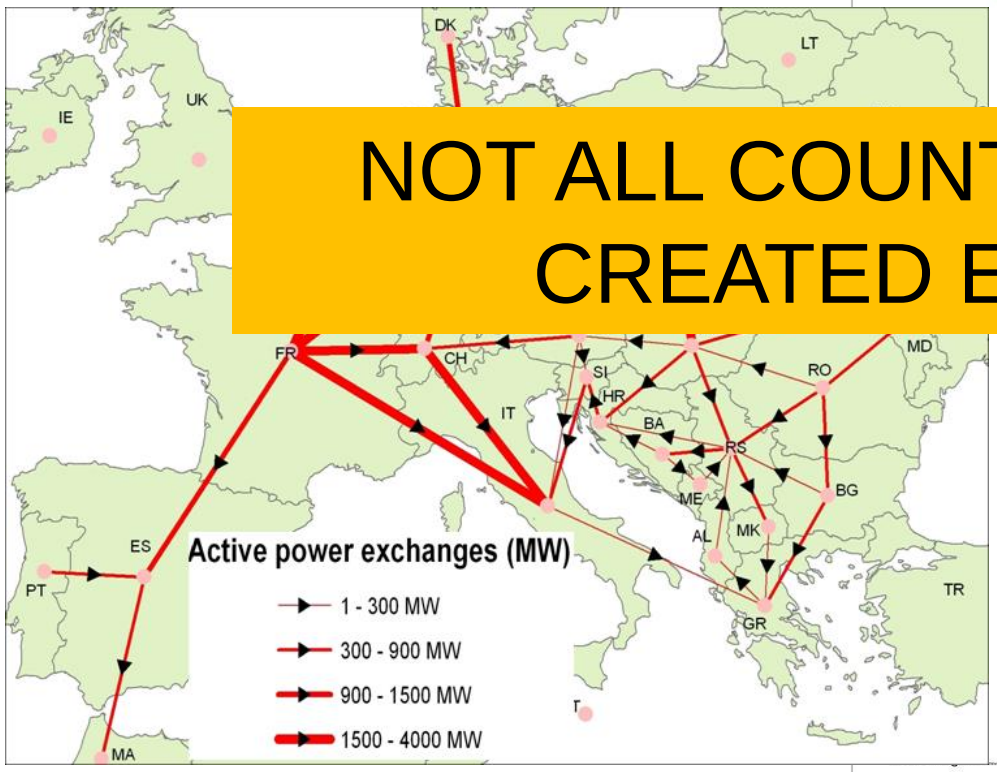
- With increased use of renewable energy generation, supply is much harder to predict due to changes in the weather etc for solar and wind generation.
- Smart Grids therefore have a key role to play in our energy future.
- This poses several significant challenges to Cyber Security.



The University Of Sheffield.

A problem...

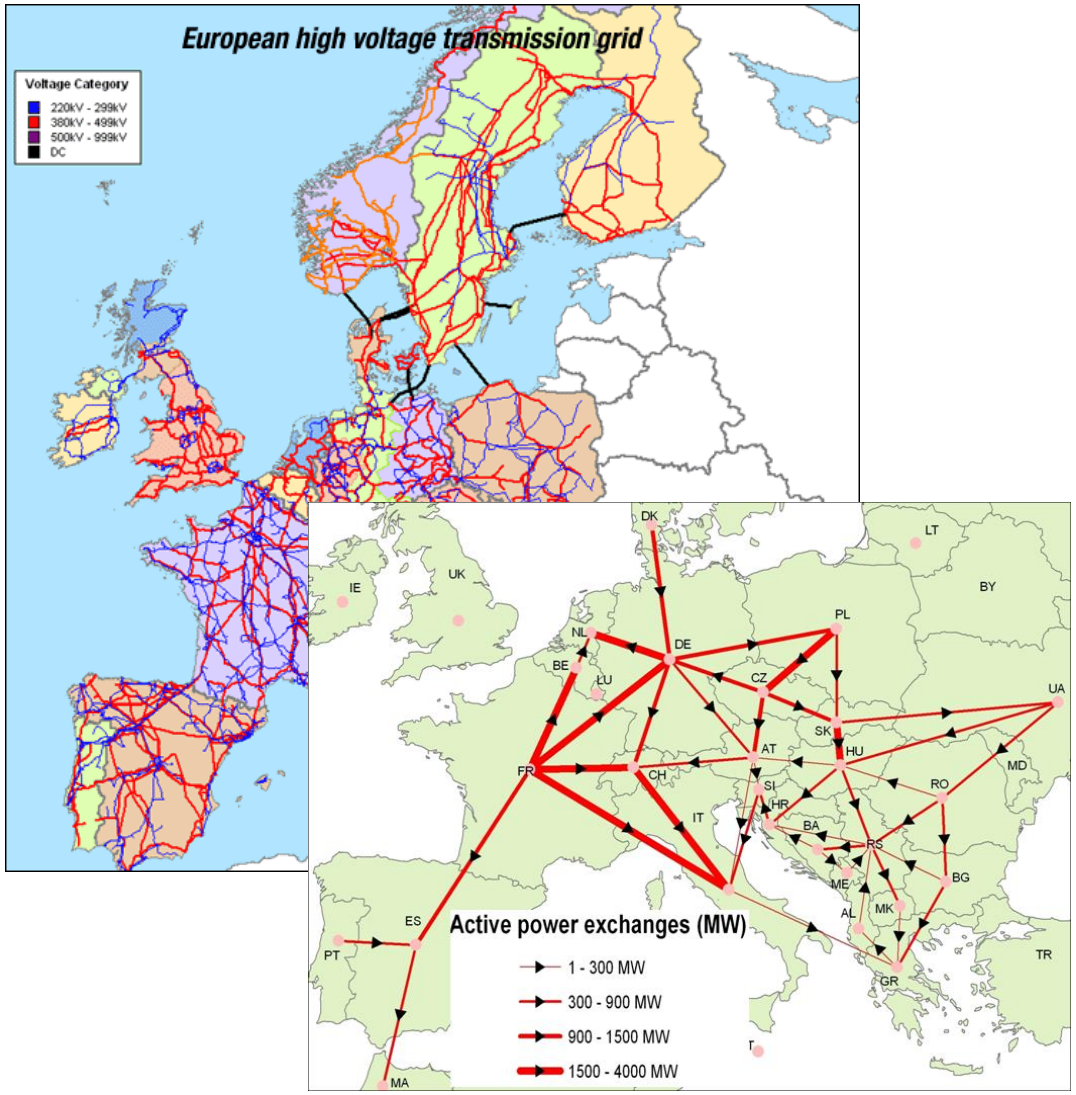




NOT ALL COUNTRIES ARE CREATED EQUAL

The University Of Sheffield.

Who is responsible?



If any national grid fails due to a cyber security attack then the entire gross domestic product (GDP) of the country and its neighbours are at risk.

2011 THE AWARDS AWARD WINNER UNIVERSITY OF THE YEAR

Some difficult questions

- How do we protect our domestic energy grids?
- How do our decisions impact those of our neighbours?
- What is the risk of failure?

A Robust Cyber Security Policy

- Smart grids result in hard and soft targets
- This requires a well defined and robust cyber security policy
- An understanding of the risk
- Effective communication at all levels

Summary

What you should have learnt!

Key Points

- No such thing as ‘secure’
- Learn from other parts of the enterprise
- Cyber Security and Information Assurance are in a period of flux
- Risk is both Danger and Opportunity
- Communication is what the listener perceives
- Smart Grids provide a great opportunity
- Smart grids also have the potential for catastrophic failure
- Ask difficult questions

The University Of Sheffield.

To Discover And Understand.

2011 THE AWARDS AWARD WINNER UNIVERSITY OF THE YEAR

Questions?

j.m.rigelsford@sheffield.ac.uk