Policy Session 4
Identifying Risk: An abundance of Potential Shock Waves

Ray Stanton

Interim Group CiSO & Director Digital Risk, National Grid &,

Group CiSO/CiRO, Redwood Technologies Group

9th May 2017

Agenda items covered during this brief presentation

- Evolution of Global Risks
- The challenge(s) we face
- Some advice

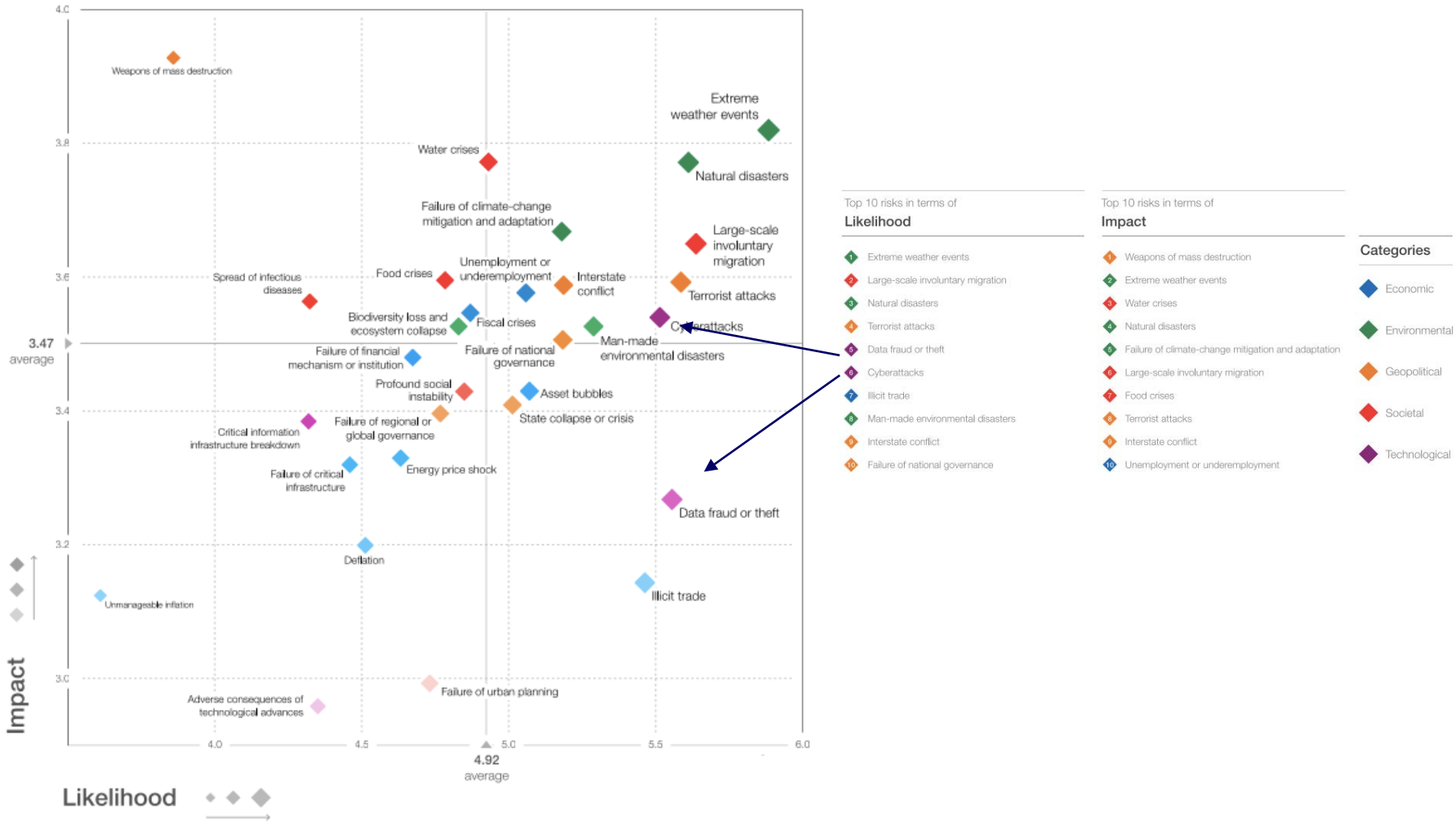
Context & Perspectives

- *The reason I love this industry so much, is the same reason the challenge we face is outpacing all other technological challenges today – complexity.*
- A huge skills gap exists for driving complex programmes to implement controls around digital initiatives, privacy by design, risk assessments, these gaps exist – everywhere.
- Therefore, we need to be practical and pragmatic.

- *For the sake of todays debate, **'cyber'** is defined as the need and challenge to manage risk associated with **'digital'** initiatives, including technology, process and procedures.*

The Evolving Global Risks landscape 2017

Figure 3: The Global Risks Landscape 2017



Acknowledgement WEF GRR 2017

Collaboration Driving Future Business growth

“The simple truth is that the most adaptive, agile, and responsive companies are almost always the most in touch.

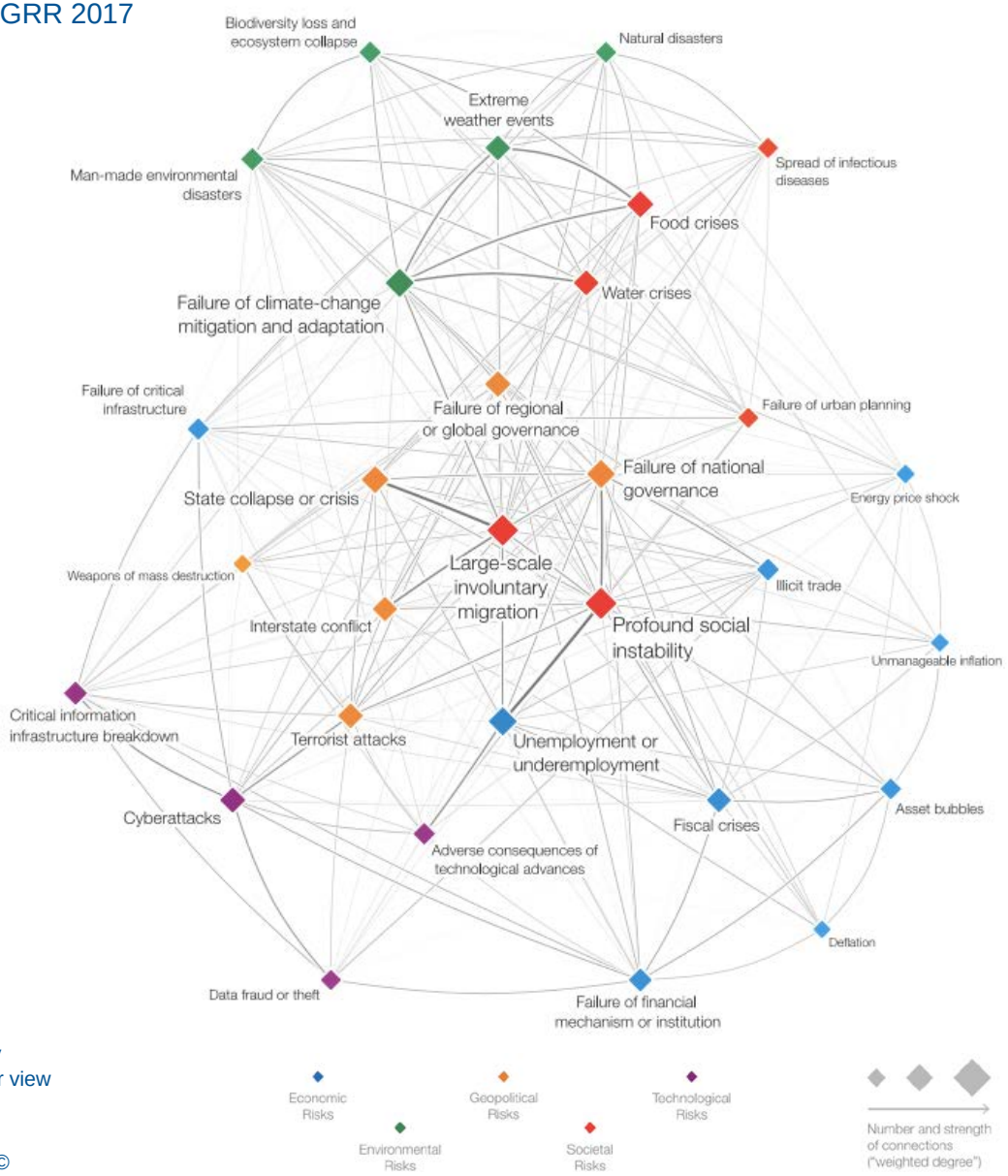
The companies that are the most in touch tend to be the most collaborative.

And the most collaborative – the companies that are the best at creating, finding, and reapplying great ideas – are those that sustain growth over the long term”

A. G. Lafley, Procter and Gamble CEO

The Global Risks Interconnectivity impact 2017

Acknowledgement WEF GRR 2017



Survey respondents were asked to identify
Between 3 & 6 risks interconnected in their view

Evolving threats – for insight

- One of the Five Factors Exacerbating Geopolitical Risks (WEF 2017 GRR Report)
  - *'Cyberspace is a domain of conflict'*
- ASIA Pacific continues to be the hotbed of organized threats:
  - three weeks ago we saw details release of a super intelligent, long term (five year) progamme of attack (Cloud Hopper)
  - Targeted managed services providers to get to end targets
  - One of many new breed threats
- BRIC countries continue to lead the way in all areas of threats
- SME(B)s across the globe continue to be targets for 'whaling' attempts, phishing and social engineering of CFO's & CEOs to release funds
- Phishing and malware is the current #1 global threat to all organizations, beyond those dealing with targeted nation state attacks
- For FIS specifically, an example; attacks on trading systems – targeting the resilient network systems used & the trading turret systems

New EU data rules – Aims & Challenges

- Regulation not Directive (but with carve-outs)
- Data protection by design/default
- Data Protection Impact Assessments (aka PIAs)
- Suppliers outside EU in scope
- Toughened (local not centralised) enforcement bodies - audits & dawn raids
- Breach reporting in 72 hours
- Distinction between processor and controller diminishes
- The need for dedicated and named Data Protection Officers
- Transfers to 3rd countries

Adapted from and acknowledgement to Cordery Legal & Compliance

The response, Technological, Procedural and People

- Evolving technologies like AI to determine threats e.g. IBM Watson
  - *Alan Turing posited in 1951: "If a machine can think, it might think more intelligently than we do. ... [T]his new danger ... is certainly something which can give us anxiety."*
    - Today we are using this intelligence to defend and attack
- Global industry initiatives – Forum of Incident Response – FIRST (*CERTS)
- Collaborative industry groups – in the US – FSISAC
- Cloud Security Alliance
- The Payment Card Industry Digital Security Standards
- Growth in Professional Industry bodies; ISACA, ISC2, CISM..
- Many others initiatives..

**Computer Emergency Response Teams*

Some advice to take away

Three questions you should think of asking:

- Who is truly accountable in your organisation for Security (Cyber or Information Security) and what are their plans to deal with todays and tomorrows threat horizons e.g. 12-18 months?

- What threat scenarios (war gaming) have been tested/are to be tested – up to the highest levels in the organization – past evidence proves CEOs/Boards/SIDs all need engaging before, not when it happens. It will happen!

- What are the visible board / executive metrics & KRIs used to demonstrate informed decision making and management controls are in place, to reduce the likelihood at least of ***'something'*** occurring. Including how these feed into your group risk registers.

**Computer Emergency Response Teams*

Additional information & thank you

- EU Cyber Security – www.bit.ly/eucyber
- Right to be forgotten – http://bit.ly/1tB8Osb
- What the Romans teach us about cybersecurity - https://theanalogiesproject.org/the-analogies/romans-teach-us-cybersecurity/

- ray.stanton@nationalgrid.com
- rstantonuk@gmail.com