Proactive Cyber Risk Management

Eireann Leverett
Senior Risk Researcher
Published Scenarios

- Lockheed Martin
  - UK Distribution Substations
- RMS (Explicit cover)
  - Cloud
  - DDoS
  - Breach
  - FinFraud
  - Ransomware
- Talbot (Silent Cover)
  - Off Shore Oil & Gas
  - Aircraft
  - Electricity Cyber Terrorism
  - On Shore Oil & Gas
We measured the cost of impacts

GDP@Risk
TWHours@Risk
CBI
Event Cancellation
In 2015 we made new models

- Of generation facility infection
- Of cyber-events:
  - Ransomware
  - DDoS
  - Financial Fraud
  - Cloud Compromise
  - Breach
- Of financial impacts
  - I/O analysis of critical infrastructure interdependency
Now we’d like focus on cyber metrics and data pools

We are stewarding an ever changing landscape of internet infrastructures and enterprise machines.

- We need to map and record that change
  - With metrics boards can understand
- That change, changes our vulnerability
- Data Pooling (good role for academia)
- Instead of begging for data:
  - Make it
  - Derive it
  - Listen to the internet
  - AUTOMATE
- Cyber isn’t solved on paper
Our new focus is on gathering/sharing data

- How big could a breach be?
  - Is a function of data storage
- How big could a DDoS be?
  - Is a function of potential bandwidth and computation
- How big is the ransomware industry
  - Is measurable if we study the malware
- How will we measure these changes over time?
- How do we estimate and find these natural limits?
Passive or Proactive Cyber?

- The models we are currently creating are passive.
- This assumes historical precedents are normative.
- We know that in cyber historical limits are exceeded almost yearly.

- What if we assume
  - Rectifying actions
  - Incentivising security
  - Collaborative defense
What does Proactive look like?

Lobbying regulatory changes

Underwriters Labs

Selection pressure for B2B relations

Legal pressure on malware hosting

Limited Software Liability

Training Underwriters

Technical measures that scale cheaply

Indicator of Compromise sharing

All of these approaches are research subject opportunities themselves!
Three models view

- Impact Layers:
  - National
  - Organisational
  - Sectoral
  - Machines/People
Let’s talk about the Ukraine incident

- On December 23rd, 2015, around half of the homes in the Ivano-Frankivsk region in Ukraine (population around 1.4 million) were left without electricity for a few hours.
- 3 substations affected, no known physical damage
- The incident is confirmed
- The malware as causal not yet fully in the public domain.
- I will not speculate on attribution, nor should you.
Frequency and Severity of malicious power outages

- If substations have been digitised for 30 years...
- So this might be a 1-in-30 event

- Ukraine uses: 3,957.88 KWH per capita
- \(3957.88 \times 6 \times 500,000 = 11,873,640,000\) kWh

- Roughly a 1 in 20 year or 1 in 25 year event by that method.

- Only time will tell how frequent they can get.
Centre for Risk Studies

UNIVERSITY OF CAMBRIDGE
Judge Business School

Eireann Leverett
Senior Risk Researcher
eireann.leverett@cantab.net