Governments are worried

Why it Matters - It is a real problem and it is pervasive
I wasn't always a cyber Geek

5 Key strands of context

1. It's not just Hype: Cyber really is a pervasive problem
2. It's probably going to get worse before it gets better
3. Cyber is a Board Room issue - don't leave it to the Geeks
5. Don't get hung up on motivation it’s dangerous - you can be a victim without being the target

Wapiganapo tembonyasi huumia.

When elephants fight the grass (reeds) gets hurt.
Real World Examples

DHS (Dept of Homeland Security) announced Oct. 29 (2014) that several industrial control systems -- vendor-issued programs used by private companies to manage internal systems -- had been infected by a variant of a Trojan horse malware program called BlackEnergy. Infected programs such as GE Cimplicity, Siemens WinCC and Advantech/Broadwin WebAccess have been used by companies responsible for portions of the country's critical infrastructure, including "water, energy, property management and industrial control systems vendors" according to DHS.

NSM warned 300 Norwegian Oil Companies they had been compromised successfully.
Cyber Vulnerabilities For Energy

Vulnerabilities in Transmission
- Infrastructure Vulnerability
- SCADA and PLC control vulnerabilities
- Static Data Pools
- Field Equipment
- Remote Telemetry
- CCTV Vulnerabilities

Vulnerabilities in Field Engineering
- Field Equipment
- Connectivity
- Mobile Device
- Telemetry and Wireless Comms
- Usage Data
- Personal Data

Vulnerabilities in Construction Projects
- BIM
- 3rd Party Vulnerabilities
- Static Data Pool Vulnerability

Vulnerabilities in Generation
- Load-balancing
- 2-way grid management
- Metering strategy
- Demand Side Management
- Hydro release management
- Wind Farm optimisation

Vulnerabilities in DMOS
- Real-time Pipeline Monitoring
  (Energetic Bear & Dark Energy)
- SCADA Vulnerabilities
- Physical damage through interference with
  Flow Rate
  Pressure and temperature sensors

Vulnerabilities in Headquarters
- Sensitive Statutory Information
- Regulatory Information
- Personally Identifiable Information
- Market Sensitive Information
- Payment and Settlement Accounts
- Web attacks
- Sensitive Environmental Data

Vulnerabilities in Customer Engagement
- Personally Identifiable Information
- Payment and Accounts
- Meter reading trust
- Bridging OT and IT boundary
Energy Threat Actors

Russia in particular
Analytics Raids
Reserves Estimates
Pricing Assumptions
Product Launch Market Manipulation
Sensitive Commercial Data Theft
IP Theft Product, Process, Design Eng

Terrorism

Destruction of Infrastructure
Consignment Hijacking
Critical Personnel Data (K&R)
Port Operation Interruption

Supply Chain Increases Exposure

Cloud Service Provision
Analytics Raids
Reputation Risk
Insider Threat
Facilities Management
Vulnerabilities

IP Theft
Analytics Raids
Deal derived Market Manipulation
Personal Data Theft
Financial Theft
Commodities Hedges

Organised Criminality

HWI Personal Data Theft
Technical Data theft
Investment exposure
Environmental activism

Competition

Analytics Raids
Product Launch Market Manipulation
Sensitive Commercial Data Theft
IP Theft Product, Process, Design Eng

Hacktivist

Nation State Actors

Insider Threat
Facilities Management
Vulnerabilities

Willis
Threat Actors targeting Renewables

State Actors
- Russia – Energetic Bear (HAVEX)
- China – Attack scenario Surveillance
- Disruption of two way grid
- Disruption of Efficiency Management
- Disruption of Solar Ramp Mitigation
- Capital Infrastructure Projects
- Iran – CNI Surveillance
- Grid Back-up disruption

Competitors
- Metering strategy
- Demand Side Management
- Wind Plant Optimisation
- Pre Regulator K calculations
- License sensitive information

Organised Criminality
- Altered data at the meter (billing)
- Market Sensitive commercial Information
- Personal payment details
- Settlement Accounts
- Sensitive Competitive information
- Web Site vulnerabilities for PII

Terrorist Actors
- Altered Data at the inverter (photo voltaic load balancing)
- Disruption of two way grid
- Disruption of Efficiency Management
- Both exploiting remote access vulnerabilities:
  - Telemetry; Remote Field Equipment,
  - Transfer Stations; Pipework; Sensors, PLCs, SCADA

Hacktivist (Environmental Lobby)
- Investment and cost information
- Leakage information
- Pricing Data
- Company Leadership Personal Data
- Waste Treatment effectiveness statistics

Supply Chain
- OEM Relationship
- 3rd Party Engineering Service Provision
- Condition Monitoring and Reliability
- Field Engineering service provision (Laptops/tablets)
- PII
- Remote connectivity and telematics

INSIDERS
What we are about
Empowering the quantification of Cyber Exposure

• Stimulating a dialogue to answer three key questions

1. Do we understand our cyber vulnerabilities in Beyond Connectivity Services?

2. How will we quantify the incremental exposure of these cyber vulnerabilities on our existing risk portfolio?

3. Are there new cyber specific exposures not currently addressed as we launch our beyond connectivity value adding service partnerships?

• In order to inform the Risk Balance solution decision within the context of your risk tolerance, reconciling:

  • Risk Mitigation spend
  • Retained Risk and funding
  • Risk Transfer
We build a Cyber Risk exposure model that demonstrates the amplification effect of Cyber Risk exposure on other enterprise risks (this is informed by our Cyber-specific Questionnaire and our assessment of your technical exposures).

Cyber Risk can amplify another risk’s severity and/or frequency. In certain cases it can also enable new risks.

The level of amplification is determined by the *Cyber Vulnerability Level (CVL)* of the enterprise.

The Cyber Vulnerability Level is comprised of 4 Key Elements and each element represents a different pillar in the anatomy of a firm’s Cyber Vulnerability, namely:

- **E1.** Assessment of sophistication of segmentation of critical digital assets
- **E2.** Assessment of sophistication of threat understanding and intelligence
- **E3.** Assessment of ability to identify critical cyber defence controls
- **E4.** Assessment of the sophistication of definition and policing of measures of effectiveness of the outcomes from the targeted controls
Then we use real examples from your risk register to demonstrate cyber impact on exposure and visualise it.

### Risk Amplification Example (table)

Each level of Cyber Vulnerability will have a distinct effect on Operational Risks.

<table>
<thead>
<tr>
<th>Cyber Vulnerability Level</th>
<th>Risk 1</th>
<th>Risk 2</th>
<th>Risk 3</th>
<th>Production Interruption Risk</th>
<th>Russian Market Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk exposure severity index</td>
<td>1.06</td>
<td>2</td>
<td>1</td>
<td>8</td>
<td>10</td>
</tr>
</tbody>
</table>

Risk severely affected?

- NO
- NO
- YES
- NO
- YES
- YES

By how much (weighting factor)

- N/A
- N/A
- 1.1
- N/A
- 1.4
- 2
- 1.2

New Risk exposure

- 1.06
- 2
- 1.1
- 8
- 14
- 0.2
- 0.8

Risk Exposure Frequency

- 0.026
- 0.026
- 0.01
- 0.026
- 0.026
- 0.01
- 0.1

Risk Frequency affected?

- NO
- NO
- YES
- YES
- YES
- YES
- NO

By how much (weighting factor)

- N/A
- N/A
- 1.1
- 1.4
- 1.2
- 1.6
- N/A

New Risk frequency

- 0.026
- 0.026
- 0.011
- 0.006
- 0.002
- 0.01
- 0.1

### Risk Amplification example (graph)

**Cyber effect on Enterprise Risks**

- Risks affected by Cyber Risk (before)
- Risks affected by Cyber Risk (after)
- Unaffected risks
- Aggregate movement
- One dimension movement

**Production Interruption Risk**

- Russian Market Risk

**Severity Index**

- Frequency (events per year)
REFLECTIONS ON THE CYBER INSURANCE MARKET

3 strands of Institutional Challenge
Cyber vulnerabilities and risk transfer: Development of the insurance market

Capacity

- Many insurers are moving into cyber insurance, but appetite between players varies substantially especially in the Energy sector
- Not every insurer is keen to write primary insurance in every sector
- Market for stand-alone Cyber insurance is in its infancy although growing: US business will be USD 1.5 billion in 2014, London USD 235 million
- Capacity has not yet evolved to the levels the risk and threat require: limit in the US is USD 500 million, in London USD 300 million
- Total global market for stand-alone cyber insurance is likely to grow to $8-10 billion in next 5 years
  - US market continues to grow rapidly in 2015 with very substantial growth around retail POS and healthcare services
  - European market seeing increased take up of cyber insurance solutions 2015
  - Asia Pac is lagging although Singapore and Australia are relative hotspots

Solutions

- There are many products for 3rd and 1st party risk related to privacy, but only five looking at 1st party BI risk and physical BI risk
- Most cyber capacity for first or third party critical infrastructure protection is provided as an extension of traditional P&C products often with small and inadequate limits
- Perimeter for cyber relative to other risk cover areas is not yet clearly understood
- Legislative developments in the US and the EU (General Data Protection Regulation) will drive greater demand for relevant cover

Product portfolio is still thin and non-standardized...
Cyber vulnerabilities and risk transfer: Underwriting challenges and emerging issues

Emerging issues

- Technology evolution – particularly cloud adoption – is amplifying risk levels
- Aggregation issues from cloud services are starting to worry insurers – some are starting to map these exposures, while others shy away from covering them
- The large data breaches in the US have had some influence on the ability to insure payment activities in Europe

Underwriting challenges

- As many insurers are cautious about covering the Energy sector, they
  - Expect higher retention levels
  - Expect an in-depth understanding by the clients of what cyber risks they are exposed to
  - Expect a proactive risk management stance from the client
- Ability to quantify potential losses and total cyber driven exposure doesn’t match the sophistication of the threat
  - The current product proposal forms are rudimentary and don’t generate a material assessment of vulnerability for BI but for privacy they are more adequate
  - Aggregation across the underwriters’ portfolios is a major issue for their book – the nightmare scenario often used as the example is IBM Global Services being hit
  - Lack of comprehensive actuarial data points and generally incomplete data leads underwriters to cautionary stance in absence of a rigorous bespoke assessment method to fill the data gap
What a captive response might look like

Combing cyber-attack underwriting expertise in the global insurance markets

Support for our offering is really beginning to take hold in the London market - the PV market in particular is showing real signs of interest in covering cyber-attacks, albeit at the moment on an excess basis.

Today a client asked me: I hear London is developing some capability for this cover - is this something I need to know about? It doesn’t appear to be happening in the US because Lloyd’s, with its syndicates and its joined-up approach, is the best place to offer this cover. If London wants to retain its competitive advantage, it needs to make sure it offers new products such as this.

Source: Willis