DAC beachcroft

STRUCTURING A CYBER PROGRAMME

Kenneth McKenzie, Partner Global Group,
DAC Beachcroft LLP

Developing Environment

- Data protection
- Business integrity
- Critical infrastructure

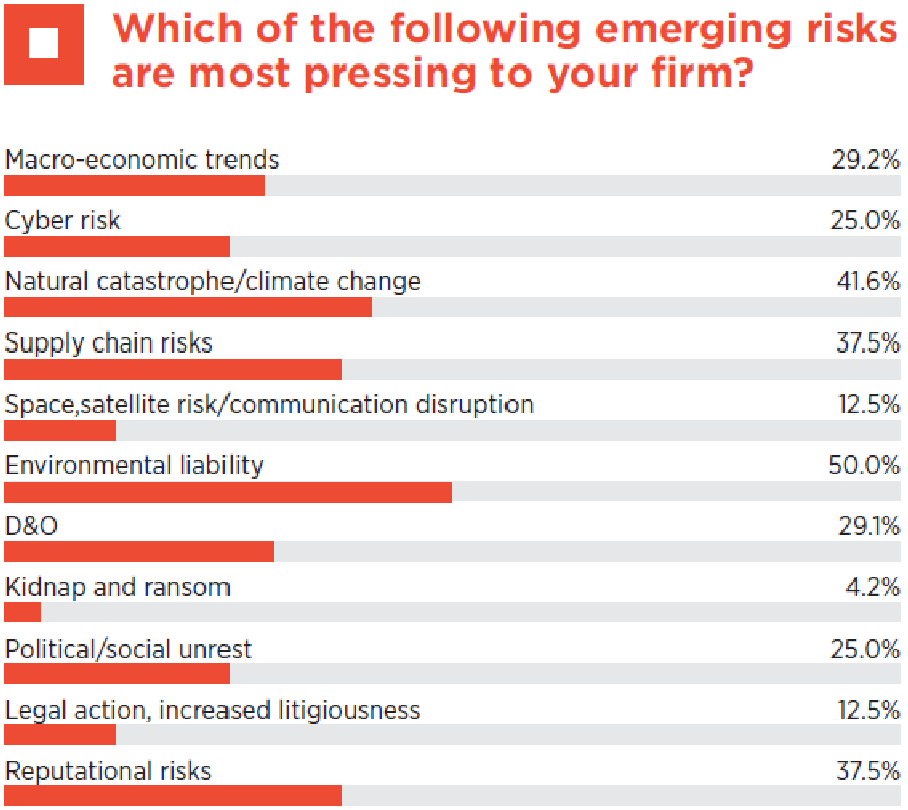
  SEC
  EU
  NIST/NIS
  ISO

“We operate in a complex computing environment and the threat of cyber attack against our industry remains high”
(Centrica)

What are the risks?

- Effective and secure information systems are essential for efficient management and accurate billing of customers, upstream operations and energy trading and hedging activities. The confidentiality, integrity and availability of our information systems could be affected by:
- accidental or deliberate exposure of share-price sensitive information, customer or employee and contractor personal data;
- viral effect of employees, crusader consumers or 'hacktivist' groups using social media channels that expose the Group to legal liabilities, damage our reputation or disclose confidential information;
- accidental or deliberate changes to financial and other data the Group relies on;
- lack of availability of systems due to inadequate infrastructure and data-recovery processes;
- an external online attack that renders the Group unable to conduct normal business activities and/or results in the loss or exposure of personal data, intellectual property or other confidential information or the disruption of control systems;
- the threat of cyber attacks against our industry continues to escalate to similar levels experienced by government agencies and financial institutions. There could be multiple sources of motivation for these attacks. These risks, however, which could arise from inadequate or inconsistent implementation of IT security controls, could seriously affect the Group's reputation, lead to legal action and/or outages that could cause financial and operational loss. The US and EU data privacy proposals increase the implications of such risks materialising, due to proposals around public notification of any data breach and the scale of associated fines for non-compliance.

Lat Am Insurance Review Survey – 60% with annual spend over US$4m



- **Bpas**
  - ICO fine £200,000 (max possible now £500,000) for abortion charity – 10,000 records stolen; hacker "rewarded" though imprisoned

- **Morrisons**
  - payroll data of 100,000 staff leaked by unknown employee

  - **bitCoin Mt Gox Exchange Bankruptcy**

Target

- US on-line shopping giant

- 70m customers debit & credit cards breached
- $100m XS $10m cyber cover
- $65m D&O cover – enough?
- SIR $10m

- Numerous actions under way

Target Share Price 2013/14

Conventional GL and BI policies don't cover

- Non-physical damage (Sony v Zurich)
- Cyber related BI
- Data loss, first or third party
- Reputation protection or damage
- Cyber extortion
- D&O typically will respond (cf Target) but will it be enough?

Cyber – First Party

- Reputational / Brand Damage: Loss of Revenue and Crisis Management costs following a number of triggers including: Data Breach and disgrace of key individuals. – typically a separate policy
- Network Breakdown: Loss of revenue following outage caused by computer attack, operator error, or loss of data including failure of outsourced elements
- Loss of critical I.P. - typically a separate policy (where unreadable but not physical damage)
- Costs of re-constituting data following accidental deletion or damage to hardware containing the data, ordinarily from non physical damage perils
- Remediation Costs:
  Notification, Credit Monitoring, Forensics, PR, Regulatory Defence Costs, Fines and Penalties (where insurable)

Key Features: Cover

- No inner limits for Remediation Costs
- Voluntary Notification
- W/W Jurisdiction and Geographical Limits
- Limited Payment Card Industry (PCI) Fines – some full limits but not standard
- CAN-SPAM Act 2003 exclusion – criminal and civil exposure of e-marketers

Third Party

Network Security Liability

- Negligent or inadvertent onward Transmission of Virus or Malware
- "Unauthorised Access" - unauthorised use of your network to launch a DDOS (Distributed Denial of Service Attack) or other action by persons not authorised to do so
- "Unauthorised Use" - unauthorised use of your network to launch a DDOS or other action by employees or other authorised persons

Data Breach

- Loss/possible unauthorised escape of (Sensitive) Personal Data (E.U.), PII/SPII/(e)PHI (U.S.), or any data relating to individuals that is controlled by legislation anywhere in the world. Mandatory reporting in 46 US states
- Definitions

  Personal Data
  PII (Personally Identifiable Information)
  PHI (HIPAA) (Personal Health Info)
- General Data Protection Regulation (E.U.)
- SEC, NIST, NIS Guidance

Privacy

Breach of legislation anywhere in the world governing COLLECTION, RETENTION, PROCESSING AND DESTRUCTION of personal/ sensitive data.

Not restricted to the US and EU, also Australia.

South Africa, Singapore, Brazil & China are introducing stricter privacy bills and Indonesia probable.

Extortion

- The threatened revealing of Personal Data/PII or sensitive trade information
  or
- The threat of interrupting operations through a targeted DoS attack
  or
- Ransom
- Increasing activity, low value losses.

Quantum/limits

- No cat cover – max $200 - 300m? $500m?
- Demand, but no capacity, for more especially in highly automated, e.g. utilities, oil & gas – post-Target squeeze (new facilities?).
- UK annual cost $27bn
- Average claim $3m/US$9m
- Worldwide capacity?


DAC beachcroft