DLA PIPER

Cyber-Security

Litigation and regulatory risk

Ben Johnson, Partner
Sam Millar, Partner
Commercial Fraud Lawyers Association
11 January 2016

What is Cyber-Crime?

- "***an attack on the confidentiality, integrity and accessibility of an entity's online/computer presence or networks - and information contained within***" - *Research Department of the IOSCO and the WFE*
- Four main types:
  - **Nuisance hacking**
  - **Hacking for financial gain:** from stealing customer credit card information to targeting a company's financial function to obtain its earnings report before it is publicly released so as to acquire and dump stock
  - **Advanced persistent threat:** stealthy and continuous computer hacking processes targeting a specific entity
  - **Hacktivism:** goal is to change or create a public perception about a brand, e.g. obtaining and disclosing sensitive information to the public

How might Cyber-Crime impact business – some common examples

- Attacks directly against a business in its own right to obtain information about the business or its customers or to carry out brand or financial harm (both to the business and its customers)
  - Ransom
- Attacks against Bank/Corporate customers to misappropriate funds
- Hack and harvesting of payment card details from retailers, leading to card fraud and loss for the retailer

Cyber-crime drivers

- Digital Age
  - mobile
  - cloud
  - big data
- Criminal community engagement
  - alliances
  - sophistication
  - taking advantage of Digital Age – encryption/malware

Recent Cyber-attacks

- TARGET
- SONY pictures
- Morgan Stanley
- Nuclear attack – South Korea
- ISIS – US Command twitter account
- State attacks
- Ashley Madison
- TalkTalk
- Vodafone

UK Government Response 2015

- Collaboration
- Increased resources – CERT/Operation Resilient Shield
- Regulatory focus (Bank of England/FCA/PRA)
- Law-enforcement co-ordination
- Technology companies
- Reporting/Sharing information
- Cyber-agents

Cyber-Crime is a Regulatory Priority

- **National Cyber Crime Unit:** Brings together capability from the Police Central e-Crime Unit and the SOCA cyber team
- **Operation Waking Shark 2 (2013):** industry-wide testing of the financial sectors' response to a sustained and intensive cyber-attack and to assess whether defences have improved since Operation Waking Shark 1 and 2011 Market Wide Exercise
- **FCA Business Plan (2014/15):** The FCA will work with the Treasury, the PRA and BoE to assess the UK's critical national infrastructure to cyber attacks
- **CBEST 2014 (B of E initiative), Cyber Essentials and Financial Crime Alert Service (Sep 2014) (a BBA initiative).**

Potential Claims against Businesses and Risks

- Breach of Contract
- Negligence
- Refund claims deriving from Payment Services Directive
- FOS
- Card Scheme Losses
- Class actions
- Reputational Risk
- Litigation Risk Issues

Potential Regulatory Action against a Bank/Risks

- S.90 FSMA
- Breach of Sysc 3.2.6R
- PRIN 3
- Listing rule 7.2R
- FCA/Payment Systems Regulator
- Senior Management responsibility
- EU Data Protection regulation
- Information Commissioner's Office

Mitigating the Risk

- Department for Business Innovation and Skills (BIS)
- FCA Handbook/Listing Rules
- Contractual audit
- Outsourcing
- Board Priority
- Waking Shark/Operation Resilient Shield
- IT vulnerability
- Planning
- Knowledge
- Insurance

EU Horizon Scanning

- Network and Information Security Directive
  - The cyber-security Directive
- Payment Services Directive 2
  - SecuRe Pay
- EU Data Protection Regime

Contact

- Ben Johnson
  - ben.johnson@dlapiper.com
  - 07968559314

- Sam Millar
  - sam.millar@dlapiper.com
  - 07968559238

G3

Cyber Threat Landscape

Malcolm Taylor, Executive Director
Arno Robbertse, Managing Partner
Commercial Fraud Lawyers Association
11 January 2016

G3

The cyber threat - Who

- State actors
- Criminals
- Ideologues
- The misguided

G3

The cyber threat - Why

- Commercial gain
- Financial gain
- Political advantage
- Fun

G3

The cyber threat - Where

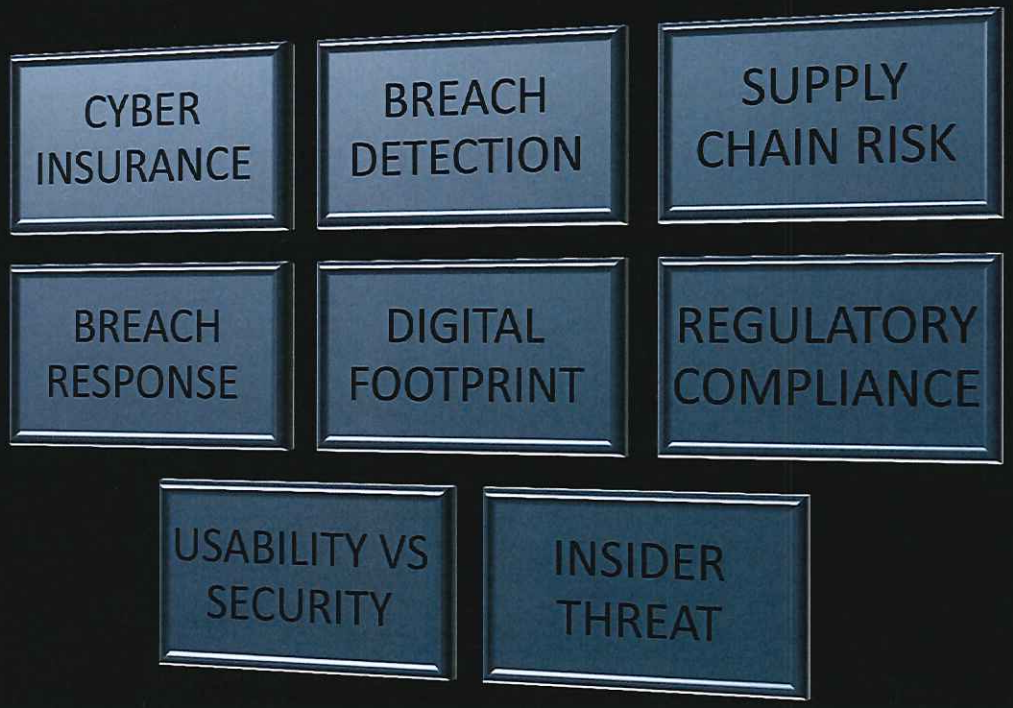
- State actors will consolidate, evolve and increase for commercial reasons (EWB not National Security)
- Criminal activity will continue to increase – 38% growth last year
- Bespoke, tailored and targeted
- The sophistication of social engineering increases
- Cyber terrorism – Islamic State

G3

What is cyber space?

G3

Cyber hot topics



G3

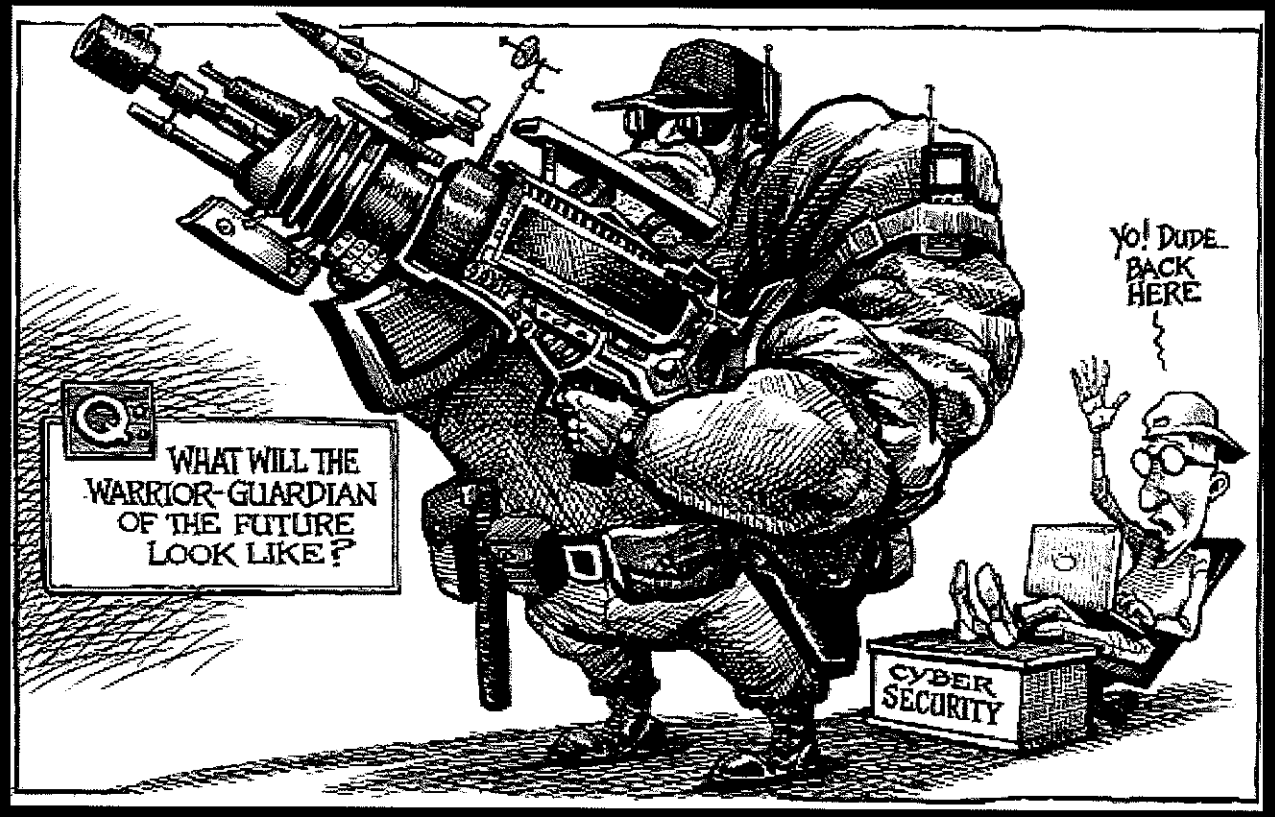
UK Government response

G3

Defence begins at home

- Choose a good password – K3ntL10n!
- Enable the highest authentication level – 2FA
- Prioritise sensitive accounts
- Keep software applications up to date. Seek expert advice
- Be vigilant
- Take inventory of your digital footprint. And that of your family

Questions



G3