The Role of the Board and Legal Team Before and After a Cyber Breach

British Chamber of Commerce Briefing

Andrew Beckett

20th April 2017

About Kroll

Kroll

Kroll Background

Kroll is the leading global provider of risk solutions. For more than 40 years, Kroll has helped clients make confident risk management decisions about people, assets, operations, and security through a wide range of investigations, cyber security, due diligence and compliance, physical and operational security, and data and information management services.

Kroll

Compliance

- Enhanced Due Diligence
- Screening and Monitoring
- Remediation and Special Research Projects
- 3rd Party Screening and Management Tool
- AML & ABAC program design/consulting
- Geopolitical and Country Risk Reports

Investigations & Disputes

- Investigations
  - Fraud & Internal
  - Financial
  - Cyber
  - Regulatory
- Forensic Accounting
- Asset Searches & Recovery
- Intellectual Property
- Litigation & Disputes

Cyber Security

- Security and Risk Assessment
- Policy Review and Design
- Penetration Testing
- Vulnerability Scanning
- Third Party Reviews
- Computer Forensics
- Data Breach
  - Incident Response
  - Notification
  - Remediation

Security Risk Management

- Security
- Operational Security Services
- Security Design and Engineering
- Resilience Consulting

Kroll

Global Coverage

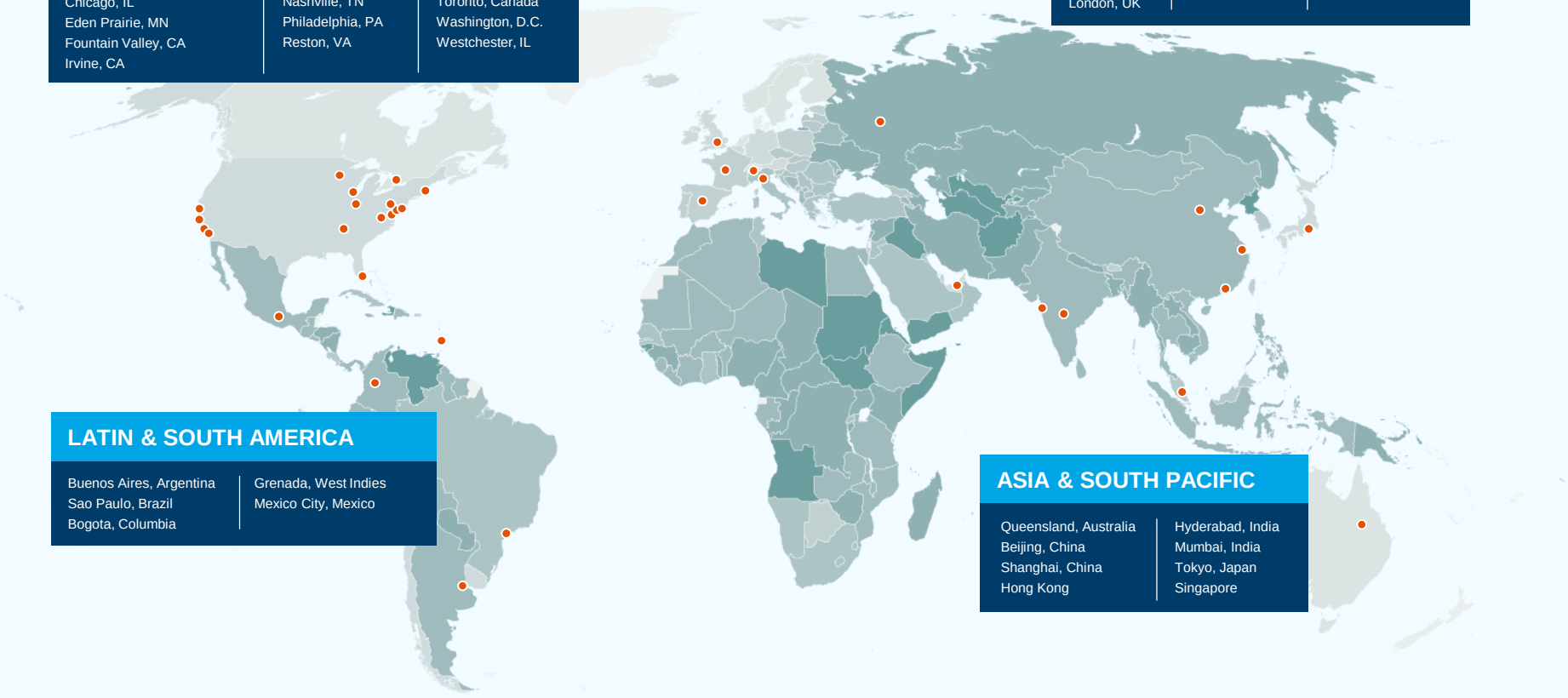
Over 1,800 employees in more than 37 offices in 22 countries

NORTH AMERICA

New York, NY *(Headquarters)*
Boston, MA
Chicago, IL
Eden Prairie, MN
Fountain Valley, CA
Irvine, CA
Los Angeles, CA
Miami, FL
Nashville, TN
Philadelphia, PA
Reston, VA
San Francisco, CA
Secaucus, NJ
Toronto, Canada
Washington, D.C.
Westchester, IL

EUROPE, MIDDLE EAST, & AFRICA

Paris, France
Milan, Italy
London, UK
Moscow, Russia
Madrid, Spain
Schweiz, Switzerland
Dubai, UAE



LATIN & SOUTH AMERICA

Buenos Aires, Argentina
Sao Paulo, Brazil
Bogota, Columbia
Grenada, West Indies
Mexico City, Mexico

ASIA & SOUTH PACIFIC

Queensland, Australia
Beijing, China
Shanghai, China
Hong Kong
Hyderabad, India
Mumbai, India
Tokyo, Japan
Singapore

Kroll

The Economics of e-crime

- Estimated income from e-Crime
  - $3 Trillion in 2016 (Cost to victims >$8Tr)
- Advantages
  - Less people involved – less chance of leaks or infiltration
  - Offences can be committed from another country
  - Significantly less chance of being caught
  - Penalties lower than for drugs offences
  - Cost overheads much lower
  - Money stolen is electronic and easier to move than cash

Global view

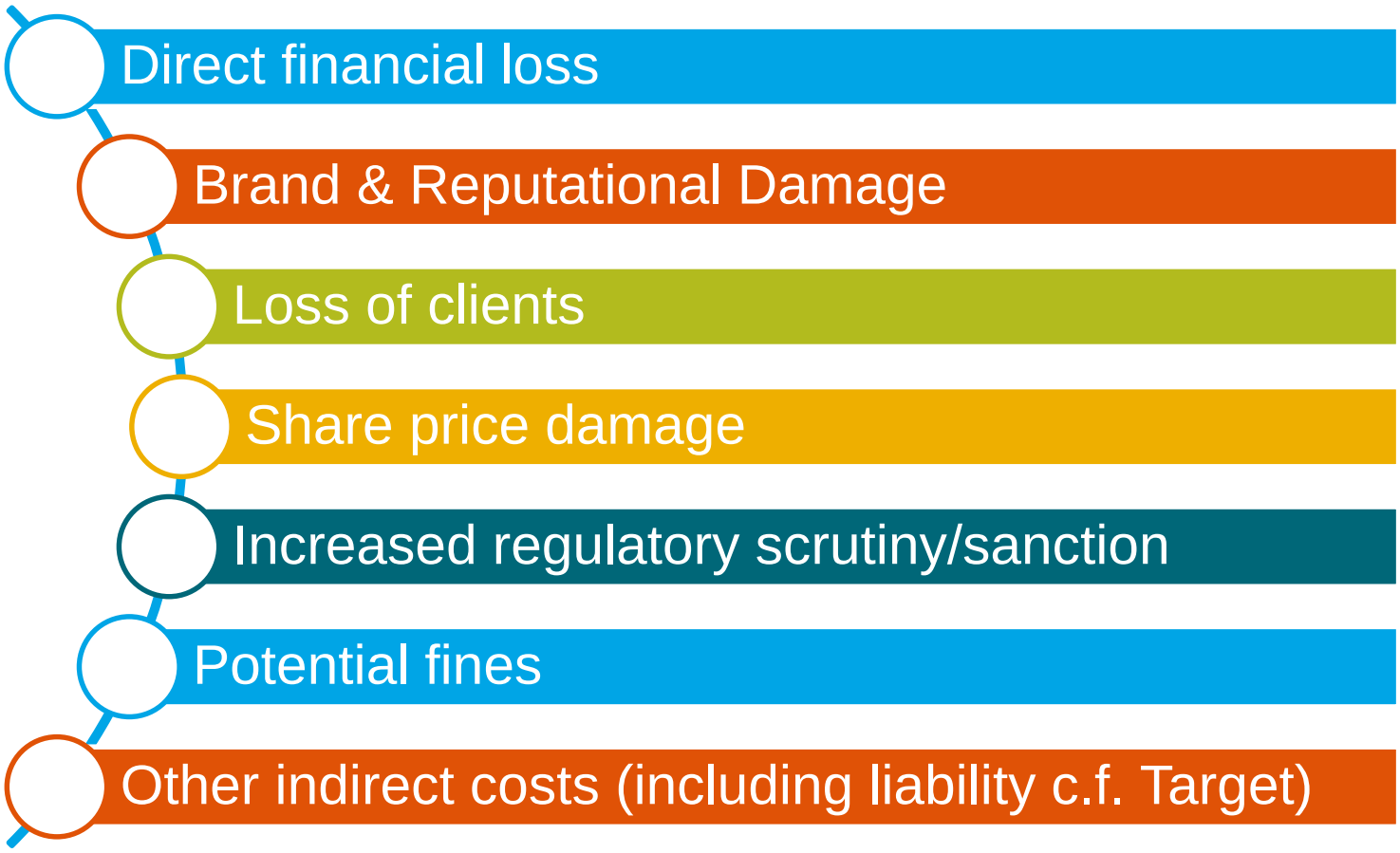
- In 2016, Cybercrime jumped to the second most reported crime, 34% of organisations surveyed stated that they think they will be affected by cybercrime in the next two years.
- A Ponemon report stated that in 2016 the average total cost of a data breach in the UK was $ 4 million or $158 per record stolen.
- In 2016, the M-Trends 2017 report identified three new trends;
  - Increased sophistication of attacks on Financial Services
  - New campaigns, old techniques
  - Intelligence sharing reduces time to discovery
- Increasingly Cyber attacks are posing a risk to national security and is listed as a Tier 1 Threat.
- 44% of responders cited in the Kroll Global Fraud and Risk Report stated that insiders were perpetrators of a cyber incident whilst a UK government survey in 2016 found that staff were implicated in a breach 81% of the time.

Reported Breaches 2016 by Industry Sector

Source M-Trends 2017

Industry	America	APAC	EMEA	Total
Financial	15%	31%	36%	19%
Retail and Hospitality	15%	7%	10%	13%
High Tech	12%	7%	2%	10%
Healthcare	12%	2%	0%	9%
Business and Professional Services	10%	5%	3%	9%
Government	8%	5%	16%	9%
Manufacturing	5%	7%	5%	5%
Media and Entertainment	5%	7%	2%	5%
Energy	3%	10%	3%	4%
Construction and Engineering	3%	2%	7%	3%
Education	3%	0%	2%	3%
Telecommunications	2%	9%	5%	3%
Transportation and Logistics	2%	5%	7%	3%
Not for profit	2%	0%	0%	2%
Biotechnology and Pharmaceuticals	2%	3%	2%	2%
Other	1%	0%	0%	0%

Impacts of a Breach



Role of the Board/Legal Department Pre-Breach

- The Board and Legal team have an important (central) role to play both pre and post incident. Put in place measures to ensure that GC is the first port of call in the event of a potential issue and establish clear guidance on what kinds of incidents need to be reported to legal and when.
- Contracts with customers and vendors increasingly allocate liability. Also define expectations – explicitly or implicitly – as to how it will be handled and financial consequences.
- These days, a companies crown jewels are its data – whether it's customer data or latest R&D. Regulators, the Board and Shareholders are interested in how they are protected and how risks have been addressed. Need to think how you will deal with legal proceedings that often follow a breach.

Kroll

Role of the Board/Legal Department Pre-Breach

- Not all breaches are caused by external threats. How are you set to handle the malicious insider, the server that is replaced without being wiped, the mislaid documents or laptop?
- Review the provisions of your cyber insurance and understand the cover. Lots of policies have exclusions which mean you may not have the cover you thought. What direct costs are covered in terms of restoring network security, investigating the attack and obtaining legal advice on notification and data protection issues? Be proactive in ensuring that the right cover is in place and understand the exclusions and excess.
- Address the language barrier. Make sure you understand the language your IT team will use when discussing an actual or potential breach.

Role of the Board/Legal Department Post-Breach

- GC often take a project management role following an incident – experts work through counsel (privilege).
- Legal Team must be able to advise the Board on the complex multi-jurisdictional notification, investigation, litigation and remedial issues that arise following a breach.
- Oversee Crisis Communications – ensure accuracy and legal impact of statements made.
- Know your rights as a cyber-crime victim: US Computer Fraud and Abuse Act provides that an individual who suffers damage or loss “may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief” but other legal redress is available in different jurisdictions.

Kroll

Questions?

Kroll