

Financial institutions
Energy
Infrastructure, mining and commodities
Transport
Technology and innovation
Life sciences and healthcare

 **NORTON ROSE FULBRIGHT**

InsureTech 2015: Addressing cybersecurity and fraud in the ME insurance industry

Dino Wilkinson

Partner

Norton Rose Fulbright (Middle East) LLP

3 February 2015



The growing challenge of cyber risks

From the IT department to the boardroom...

Loss or disclosure of sensitive internal or customer information poses multiple threats to an organisation:



Share price



Reputation

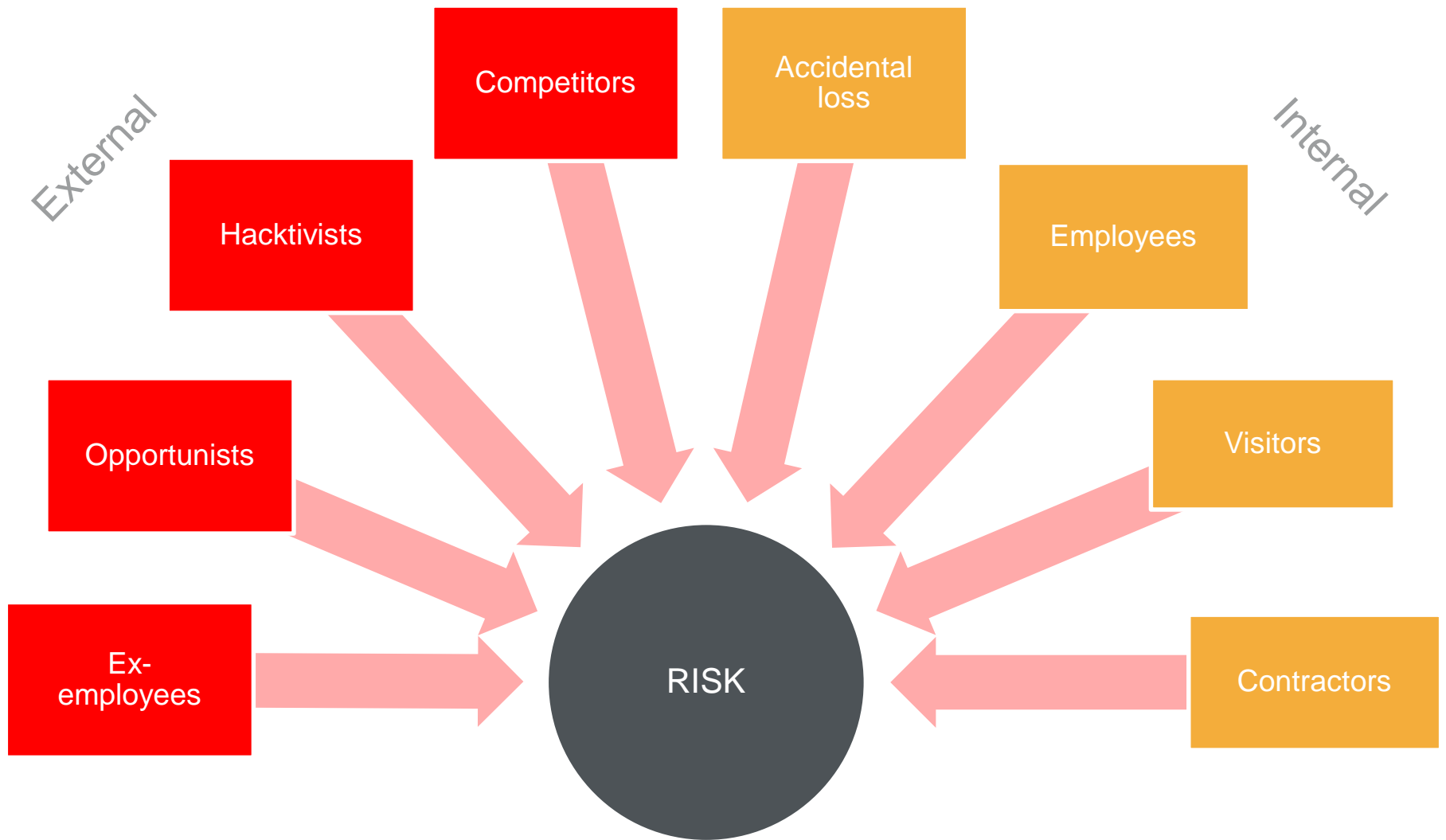


Business



Existence

Sources of risk



Legal exposures from a cyber attack



International legal and regulatory frameworks

General

- Data privacy, including cross-border data flows
- Data security and asset protection obligations (esp. regulated sectors)
- Computer crime laws
- Commercial and online fraud
- Intellectual property
- Employment laws
- Monitoring and investigatory powers

International legal and regulatory frameworks

USA

- More than 50 statutes addressing aspects of cybersecurity
- No single overarching legislation in place
- Key legislation includes:
 - Counterfeit Access Device and Computer Fraud and Abuse Act 1984
 - Electronic Communications Privacy Act 1986
 - Computer Security Act 1987
 - Homeland Security Act 2002
 - Identity Theft Enforcement and Restitution Act of 2008 (ITERA)
 - US PATRIOT Act
- Sector and issue-specific laws, e.g. internet fraud, software piracy, IP theft, online securities fraud etc.
- State laws on cyberstalking, cyber harassment, cyber bullying

International legal and regulatory frameworks

United Kingdom

- Computer Misuse Act 1990
- Data Protection Act 1998
- Privacy and Electronic Communications (EC Directive) Regulations 2003
- National Hi-Tech Crime Unit / Serious Organised Crime Agency
- European Cybercrime Directive?
- New EU Data Protection Directive?
- Serious Crime Bill 2014

International legal and regulatory frameworks

Middle East

- Bahrain:
 - Penal Code; Telecoms Law; CBB obligations
 - Proposed cyber crimes law
- UAE:
 - Penal Code; Cyber Crimes Law 2006 (updated in 2012); Cabinet Resolution 21 of 2013 on IT security in federal government
 - Establishment of National Electronic Security Agency
- KSA:
 - SAMA regulations on data export
- Qatar:
 - New cyber crime prevention law adopted September 2014

The logo consists of a stylized, upward-pointing chevron shape in a gold color, positioned above the first letter of the text.

NORTON ROSE FULBRIGHT

Disclaimer

Norton Rose Fulbright US LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP and Norton Rose Fulbright South Africa Inc are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients.

References to 'Norton Rose Fulbright', 'the law firm' and 'legal practice' are to one or more of the Norton Rose Fulbright members or to one of their respective affiliates (together 'Norton Rose Fulbright entity/entities'). No individual who is a member, partner, shareholder, director, employee or consultant of, in or to any Norton Rose Fulbright entity (whether or not such individual is described as a 'partner') accepts or assumes responsibility, or has any liability, to any person in respect of this communication. Any reference to a partner or director is to a member, employee or consultant with equivalent standing and qualifications of the relevant Norton Rose Fulbright entity.

The purpose of this communication is to provide general information of a legal nature. It does not contain a full analysis of the law nor does it constitute an opinion of any Norton Rose Fulbright entity on the points of law discussed. You must take specific legal advice on any particular matter which concerns you. If you require any advice or further information, please speak to your usual contact at Norton Rose Fulbright.