

Risk management for energy lawyers: key issues for 2015

21 April 2015

Human Rights in Business

Peter Herbel

Attorney & GM of CSR Consult

Dentons, April 21, 2015, London

Outline

Intersection of human rights and business

Human rights risks of business

Tackling human rights risks

Soft law ./ Hard law

Our Role

Intersection of Human Rights and Business

- International bill of HR: Duty of States
- Since 1948: States continue to perpetrate HR violations
- 2005 – 2011: UN mandate to John Ruggie on business and HR
- UN Framework and UN Guiding Principles: responsibility of companies

Human Rights Risks of Business

- Employees
- Suppliers
- Industry partners
- Security
- Local communities
- Host governments

Tackling Human Rights Risks: Employees

- Apply ILO conventions worldwide through management guidelines
- Human Rights Internal Guide: typical examples of risk areas and where to get help
- Confidential whistleblowing outside the hierarchy to the Ethics Committee
- Annual performance review

Tackling Human Rights Risks: Suppliers

- Contracts – fundamental purchasing principles: respect of HR and audit provisions
- Attach the Code of Conduct
- Self-assessment of supply-chain management
- Internal and external audits of your own team and of suppliers

Tackling Human Rights Risks: Industry Partners

- Know your partner: HR due diligence
- Analysis of risks and impacts of the partner on the project
- Implementing your Code of Conduct
- Rapid response when problem arises

Lackling Human Rights Risks: Private and Public Security Forces – VPSHR

- Formalized relationship between subsidiary and State
- Immediate response to HR violations
- Recruitment of private forces
- Training and audits

Tackling Human Rights Risks: Local Communities

- Socio-economic baseline studies and background reports
- Charter on indigenous and tribal peoples
- Community liaison officers and regular contacts with local stakeholders
- Grievance mechanisms

Tackling Human Rights Risks: Host Country Governments

- Respect of sovereignty and political neutrality
- Dialogue, but express your convictions on the respect of HR
- Training of public officials on HR
- No business in countries under official embargo

Soft Law ./. Hard Law

- Soft law, not so soft: constraints from financial institutions and from reputational pressure
- Some hard law, with extraterritorial application
- Reporting on CSR and HR: hard and soft in various countries
- International cooperation: knowledge exchange between public and private actors

Our Role

- UNGP apply to law firms (soft law):
due diligence, know your client
- American Bar Association, UK and others
- Clients expect advice on soft law
- Consult with experts

Sanctions

Have you done enough?
What is enough?

Andrew Cheung
April 2015

This is a known risk and we are managing it

\$8,900,000,000

- This is the fine that BNP Paribas received from the US authorities in July last year.
- Overall OFAC levied over \$1.2b of fines last year.
- 2015 has already gotten off to a good start. In March alone Commerzbank receiving \$258m fine for processing sanctioned payments through the US and Texas energy giant Schlumberger agreeing to pay £232m for Sudanese sanctions violations.

In summary, 2014 saw increasing compliance burdens coupled with increasingly stringent enforcement measures in an environment where regulatory expectations remain both increasing and not clearly articulated. Taken together, it appears that compliance-related risk has increased substantially when measured against periods prior to 2014.

We don't breach, and would know if we were breaching, sanctions

- Sanctions violations are not always straight-forward and are changing rapidly.
- 27 different regimes on UK Treasury website - 18 were updated last year, and 5 of which were updated in the past 2 months.
- They are often multi-layered being imposed through overlapping and amending separate pieces of regulation.
- The main sanctions regimes are the EU and US, which are themselves different in many material respects, but there are also others that could apply - Australia, Canada, Dubai etc.
- Sanctions can conflict, sometimes deliberately.
- For targeted sanctions do you know who you're doing business with and does your front line staff know, with a paper trail to prove it?

We know who we do business with

- More than simply using a third party information services provider or relying on "local knowledge of local offices".
- Need to undertake ongoing monitoring on the basis of an established risk management framework.
- Sanctioned individuals are still doing business using agents.
- Consider ownership & control tests for designated persons.



Don't worry, we have policies in place to manage this

- How good are those policies and procedures?
- How can you demonstrate that they are followed and understood?
- More importantly, how do policies translate into your risk culture? What does that even mean and how could you demonstrate it to an interested regulator?
- If we called your CEO or Chairperson would they be able to describe it?

Regulators in 2014 focused increasingly on the culture of compliance in organisations and, in particular, the "tone from the top" on risk management and regulatory compliance. For regulators it will no longer be enough for you to simply have a policy or procedure or even apparently robust risk management framework. You and your management need to show how you bring these to life through training, education, incentives and other measures to promote not just compliance but responsible business practices.

We're not in the US/EU so their sanctions don't apply

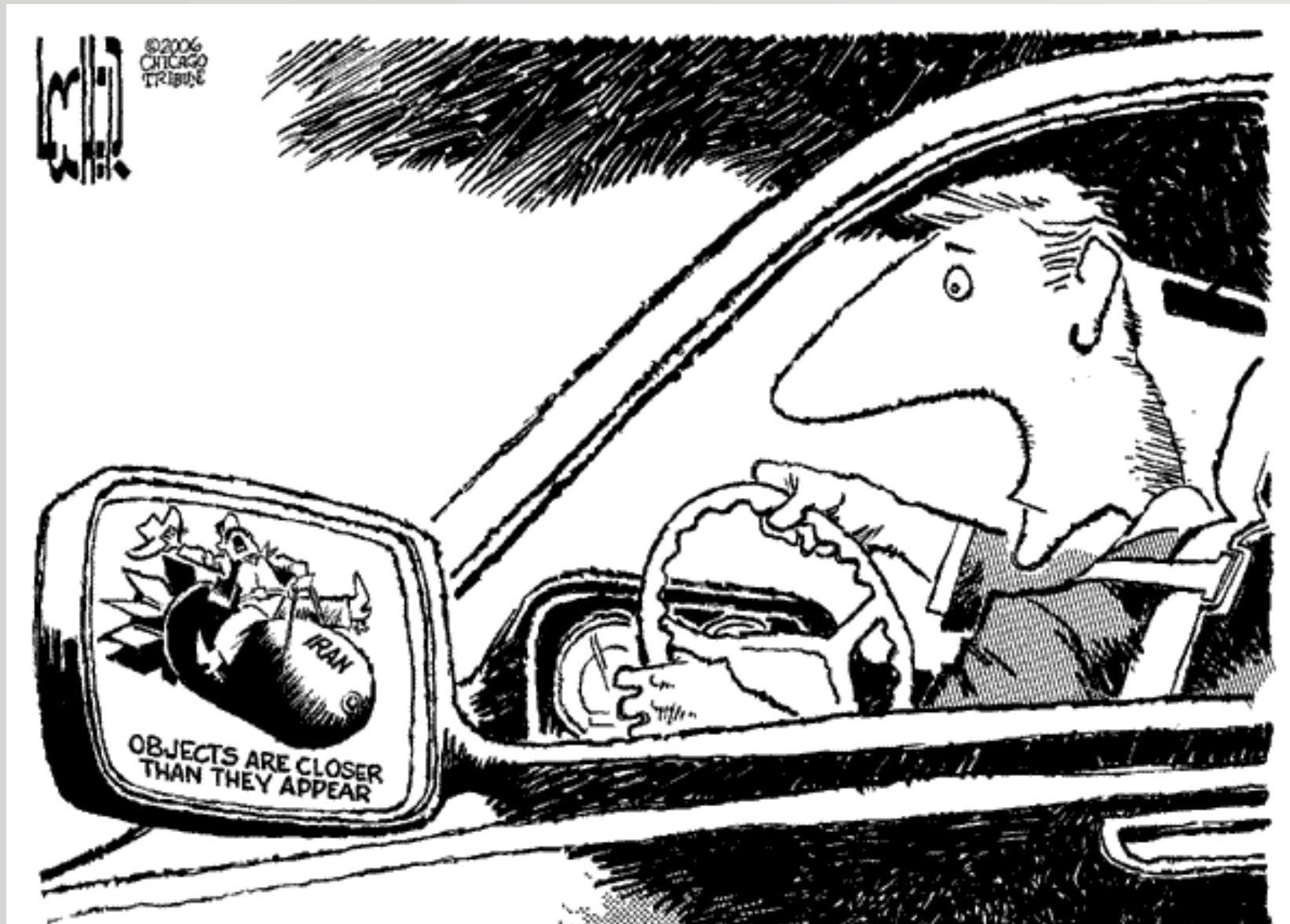
- Sanctions can apply to your organisation in a myriad of indirect ways.
- Before undertaking any business which you know or suspect may breach a country's sanctions regime, you need to carefully consider the following:

- **Nationality of project team**
- **Nationality of management**
- **Nationality / place of incorporation of shareholders**
- **Business partners and acquired assets**

- **Insurers**
- **Financiers**
- **Key clients - government or key government suppliers**
- **Changes in the law...**

End

Next, a closer look at Iranian sanctions & business



Energy Summit Iran Sanctions and Post Sanctions issues

Ramin Hariri

London 22 April 2015

The current EU Regulation/ Sanctions laws against Iran

- **Joint Comprehensive Plan of Action (JCPA) dated 2 April 2015**
- **Practical issues with the JCPA**
- **Post sanctions issues: legal framework of Foreign Investment in Iran (FDIs)**
- **Post Sanctions issues: Main legal challenges for FDIs in Iran**
- **DENTONS Six Steps Approach to FDI in Iran**

Joint Comprehensive Plan of Action (JCPA)

2 April 2015

- Iran will **receive sanctions relief**, if it verifiably abides by its commitments.
- U.S. and E.U. **nuclear-related sanctions will be suspended** after the IAEA has verified that Iran has taken all of its key nuclear-related steps. **If at any time Iran fails to fulfill its commitments, these sanctions will snap back into place.**
- The architecture of U.S. nuclear-related sanctions on Iran will be retained for much of the duration of the deal and allow for snap-back of sanctions in the event of significant non-performance.
- **All past UN Security Council resolutions on the Iran nuclear issue will be lifted simultaneous with the completion**, by Iran, of nuclear-related actions addressing all key concerns (enrichment, Fordow, Arak, PMD, and transparency).

Joint Comprehensive Plan of Action (JCPA)

2 April 2015

- However, core provisions in the **UN Security Council resolutions** – those that deal with **transfers of sensitive technologies and activities** – will be re-established by a new UN Security Council resolution that will endorse the JCPA and urge its full implementation.
- It will also create the procurement channel mentioned above, which will serve as a key transparency measure. Important **restrictions on conventional arms and ballistic missiles**, as well as provisions that allow for related **cargo inspections and asset freezes**, will also be incorporated by this new resolution.
- **A dispute resolution process** will be specified, which enables any JCPA participant, to seek to resolve disagreements about the performance of JCPA commitments.
- U.S. sanctions on Iran for **terrorism, human rights abuses, and ballistic missiles will remain in place** under the deal.

Post sanctions issues: Legal framework of foreign direct investment (FDI) in Iran

- **Foreign Investment Promotion and Protection Act "FIPPA"** : to promote and protect foreign investment in Iran grants protection equivalent to Bilateral Investment Treaties
- **Act on Management of State Services**: to promote the privatization and to allow private sectors to take part and invest in many economic sectors listed in Article 44 of the Constitution
- **Act of Execution of the General Policies**: to limit participation of Public non-governmental entities/institutions and their affiliates/subsidiaries in the market share of any goods or services
- **Act on Removal of some of the Production Barriers and Industrial Investment (including the Act re Standard and Industrial Researches' Institution, Labour Act & Mines Act)** were modified/added in order to facilitate and promote the matter of local industrial productions
- **Act on Removal of some of the Production Barriers and Industrial Investment** to ease administrative process for foreign investment (corporate, labour, visas, etc.)
- **Act on International Commercial Arbitration** to ease execution of foreign awards

Post Sanctions issues: Main legal challenges for FDIs in Iran

- Re-activation, substitution, compensation, settlement of disputes, ... issues in relation to the previous **contracts suspended or terminated further to the US/ EU sanctions**

And for new FDIs:

- Interpretation of Principles set forth by **the Iranian Constitution** (Articles 44 and 81)
- Opacity of **the Public non-governmental entities/institutions** in terms of financial information
- Compliance of international contracts with the **general principles of Iran contract law**, in particular Sharia rules applying to banking and finance
- No major systematic protection of **IP rights** is provided based on the current enactments in Iran
- Lengthy, complicated and time consuming **administrative/executive procedures** and proceedings before the **Iranian state courts**

DENTONS Six Steps Approach to FDI in Iran

- Step 1: Ensure that the Project is permissible under EU / US Regulations
- Step 2: Ensure that US sanctions against Iran do not apply either directly or indirectly to the Project
- Step 3: Ensure that the parties involved in the Project are not “Designated Entities” (DE) under EU Regulation or Specific Designated Nationals (SDN) under the US Regulation
- Step 4: Ensure that the payment channel is permissible under the applicable laws
- Step 5: Government clearance and export licenses
- Step 6: Assistance in relation to FDIs/projects in Iran

Global Energy Summit 2015: Cyber-security and the Energy Industry

Karl V. Hopkins

Dentons

Partner

(202) 408-9225

karl.hopkins@dentons.com

Cyber Risk Overview

- Increasing cyber threat
- All business sectors vulnerable
- Variety of data subject to attack
- High consequences when breach occurs
- Senior management issue
- Our solutions
- Way forward



Cyber Threat by the Numbers

- Stealing up to a terabyte of data each day - resulting in global losses of hundreds of billions of dollars
 - 1 TB = 1×10^{12} bytes
 - 1 TB = 17,000 hours of listening to music on your iPod
- Average U.S. company faces two successful cyber attacks every week - roughly 104 per year...and this number is growing

Cyber Threat

“[The loss of industrial information and intellectual property through cyber espionage constitutes] the greatest transfer of wealth in human history.”

“We have irrefutable evidence that foreign powers have placed malware in US critical infrastructure to allow them to cause damage or destruction at some point in the future.”

Gen. Keith Alexander

Director, National Security Agency

“In our experience in conducting hundreds of vulnerability assessments in the private sector, in no case have we ever found the operations network, the SCADA system or energy management system separated from the enterprise network. On average, we see 11 direct connections between those networks. In some extreme cases, we have identified up to 250 connections between the actual producing network and the enterprise network.”

Sean McGurk

Former Director, National Cybersecurity and Communications Integration Center, US Department of Homeland Security

Cyber Risk for the Energy Sector

Corporate Systems

- Exposure of Intellectual Property, R&D, Trade Secrets
- Theft of bid data, M&A strategy, financial documents
- Loss of productivity
- Loss of personal identifiable information (medical, identity)

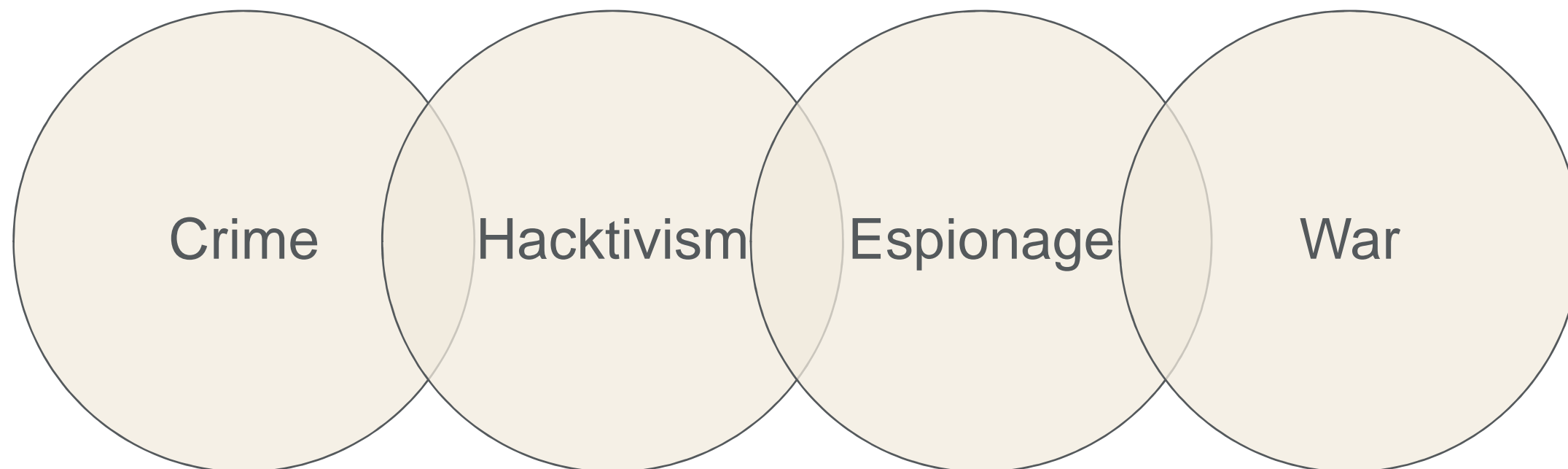
Industrial Control Systems

- Physical damage
- Loss of productivity
- Operational disruption
- Compromise of sensitive information

Consequences:

- Losses of Market and Financial Value
- Loss of Competitiveness
- Damage to Facilities, Reputation
- Exposure to Regulation, Investigation, Litigation

Four Forms of Cyber Attacks



Crime

- Unauthorized computer penetration for immediate financial gain through fraud or blackmail

Hacktivism

- Use of cyber attacks as a form of politically or ideologically motivated protest

Espionage

- Unauthorized computer penetration to acquire sensitive or valuable information to gain competitive advantage

War

- Use of cyber attacks to cause damage through severe disruption or damage of computer controlled systems

Recent Cyber Attacks Against the Energy Sector

- **March 2015:** The US Department of Homeland Security warned of an increase in sabotage attacks against US energy companies located in the Middle East.
- **Jan 2015:** US Energy Based Think Tank attacked with focus on energy policy materials and connection to sources of energy company sponsors
- **December 2014:** US Nuclear energy technology company breached. Attack focused on technology related to development of new systems. Attack also breached several other company systems and caused partial denial of service.
- **August 2014:** Various US Utilities attacked in probing incident where purposes was apparently to attempt to determine level of control in advance of denial of service attack.
- **June 2014:** Oil Service Company attacked by state sponsored actor with focus on market intelligence on deployment of company resources and cost of equipment.
- **April 2014:** Wide spread attacks across oil sector related in increased political tensions from Russian-Ukraine crisis in relation to sanctions response. Attacks focused on company assets and personnel deployed in region.

Recent Cyber Attacks Against the Energy Sector

- **July 2013:** The Department of Energy confirmed that a cyber attack occurred that resulted in the unauthorized disclosure of federal employee Personally Identifiable Information.
- **May, 2013:** The US Department of Homeland Security warned of an increase in sabotage attacks against US energy companies located in the Middle East.
- **December 2012:** 50Hertz, a German power utility was hit with a cyber attack that nearly broke down its power grid and crippled its communications capability.
- **August 2012:** The computer network of Saudi Aramco was struck by a self-replicating virus that erased data on three-quarters of Aramco's corporate PCs - documents, spreadsheets, e-mails, files - replacing all of it with an image of a burning American flag.
- **August 2012:** RasGas, one of Qatar's largest producers of natural gas, had its internal corporate networks attacked with an unknown virus in August of 2012. While the virus did not interfere with natural gas production, it seriously disrupted RasGas' office systems.
- **July 2012:** Hackers affiliated with Anonymous obtained emails and passwords of Exxon, BP, Shell, Rosneft, and Gazprom employees, leaking them online. Canadian security agencies warned other energy companies, including Imperial Oil, that they could be targeted by Anonymous because of their development of oil sands.

Cybersecurity Framework

The Framework Core Structure

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Managing Risk Requires Strategic and Technological Solutions

- Solutions include Executive Cybersecurity Risk Profile, Legal Review, and Board Level Recommendations
- Nine issues for senior executives in energy industry
 - Role of CEO and senior management
 - Direction by legal counsel: attorney/client privilege
 - SEC disclosure, public policy concerns, and standards development
 - Enterprise wide risk management strategy and governance framework
 - Executive and employee training and awareness
 - Crisis Management and communications
 - Application of insurance coverage to cyber events
 - Technology solutions for mitigating cyber risk on corporate and control networks
 - Mitigating material risk through Cybersecurity by Design: procurement and acquisition; secure development processes; culture

Key Considerations for Managing Risk

- Identify high-value information targets
 - What are the "crown jewels" of the company?
 - What must absolutely be protected from a cyber breach?
- Design protection strategy with assumption that hackers will get in to your system
 - Focus on relevant risk of the company
 - Focus on risk threshold of the company
- Formulate a Cyber Threat Detection and Response Plan
 - Develop a scenario matrix by devising possible scenarios for cyber attacks with probability of occurrence and impact on the business
 - Develop a breach response plan and pressure test it

Key Considerations for Managing Risk (cont'd)

- Disclosure Considerations
 - Securities and Exchange Commission has issued guidance on obligations for disclosure of cyber security risks and incidents
 - Not a rule, regulation or official statement - but failure to disclose can lead to filing delays and potential exposure to plaintiff bar
 - When disclosing, use "materiality" standard
- Cyber security and the human factor
 - Employees can be substantial cause of cyber security issues - usually inadvertent conduct or act
 - 30% of companies face a cyber security breach due to an employee's activities through social networking
 - Provide constant training to employees to prevent this and complement with technical security controls (e.g., antivirus, antispyware, web-filtering)

Questions for Planning for a Breach

- How will you know when you've been breached or hacked?
- How do your practices compare to the industry best practices?
- What are the biggest weaknesses to your IT system? What would cause the biggest damage to your IT system?
- Has an audit been performed on your IT system?
- What was your worst cyber security breach?
- Are you investing enough into your IT system to make it harder to hack?

Questions for Dealing with a Breach

- How did you learn about the breach? Internally? By outside agency?
- What was stolen? What was affected? What has been compromised?
- Did your response plan work?
- Who have you notified about the breach? Has your legal team prepared the proper notifications?
- Who was the hacker? Motivation?
- What were the weaknesses in your IT system and how to prevent this?

Thank you




Karl V. Hopkins
Dentons
Partner
+1 202 408-9225
karl.hopkins@dentons.com



KCS

Strategic Intelligence & Corporate Security

A background image depicting a digital data stream or code rain, similar to the Matrix movie. The characters are in shades of blue and green, falling from the top of the frame. The overall effect is a sense of depth and digital immersion.

Social Engineering: How they know who you are



KCS

Strategic Intelligence & Corporate Security

Hackers For Hire



Social Engineering



Pietr Hadere

HR Manager at Self-employed

London, Greater London, United Kingdom | Legal Services

Previous HBJ Gateley, MFI

Send Pietr InMail



uk.linkedin.com/pub/pietr-hadere/86/402/432

Background



Summary

I am an experienced head-hunter and former Human Resources manager currently freelancing for a number of high-profile industry and business clients. Having started as an administrative assistant I rapidly progressed to my senior role, being ultimately responsible for a team of five in-house HR professionals, and managing the daily running of the office, including both front-of-house and backroom concerns. I managed staff profiles, organised diaries/schedules for both company Directors and the firm's employees in general, and took the lead in the recruitment process for potential new employees.

My HR experience began in 1998 when I spent six years working for MFI. Towards the close of this period I was given additional duties in the Public Relations department, and this was an avenue which I pursued over the better part of the next decade in London firms elsewhere. I have since set out on my own as a professional head-hunter for blue-chip, City and high-profile industry contacts. I have built up an extensive client list for which I source ideal employees, having an innate understanding of qualities required to excel in a role and knowledge of how best to confluence individuals and industries.

My core competencies include excellent organisation/time management, 'people skills' and an in-depth knowledge of the working processes of a corporate environment.





KCS

Strategic Intelligence & Corporate Security



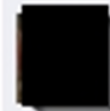
[Redacted] UK Ltd
30 November 2012 · 🌐



Like · Comment · Share

[Redacted] **[Redacted]** more hair on your face than headxx

30 November 2012 at 18:39 · Like · 🔄 1



Write a comment...



KCS

Strategic Intelligence & Corporate Security

Friends who also work at [Redacted] UK Ltd

[Redacted Profile Picture]

[Redacted Name]

Buckinghamshire New University

[Add Friend](#)

[Redacted Profile Picture]

[Redacted Name]

ICT Operations Team Coordinator at [Redacted] UK Ltd

[Add Friend](#)

[Redacted Profile Picture]

[Redacted Name]

[Redacted]

[Add Friend](#)

[Redacted Profile Picture]

[Redacted Name]

[Redacted]

[Add Friend](#)

[Redacted Profile Picture]

[Redacted Name]

Works at [Redacted] UK Ltd

[Add Friend](#)

[Profile Picture]

[Redacted Name]

[Redacted]

[Add Friend](#)

[Redacted Profile Picture]

[Redacted Name]

[Redacted]

[Add Friend](#)

[Redacted Profile Picture]

[Redacted Name]

Works at [Redacted] UK Ltd

[Add Friend](#)

[Redacted Profile Picture]

[Redacted Name]

ICT Operations Team Leader at [Redacted]

[Add Friend](#)

[Redacted Profile Picture]

[Redacted Name]

[Redacted]

[Add Friend](#)



KCS

Strategic Intelligence & Corporate Security

Timeline **About**

DO YOU KNOW [REDACTED]

If you know [REDACTED] send her a message.

ABOUT

- ICT Operations Team Leader [REDACTED] and ICT Operations Team Leader at [REDACTED] Ltd
- Studied BTEC National Diploma in IT at Crawley College
Past: Steyning Grammar School
- Lives in Horsham
- From Partridge Green, West Sussex, United Kingdom



KCS

Strategic Intelligence & Corporate Security

TV Programmes

Likes



BBC Eurovision
TV Programme



I'M A CELEBRIT...
TV Programme



The Million Poun...
TV Programme



BI
TV



Foo Fighters ✓
Musician/Band



The SSE Hydro ✓
Concert venue



Matchbox Audio
Record Label



Ten Years Late
Musician/Band



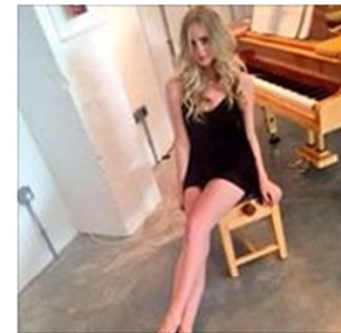
The Script ✓
Musician/Band



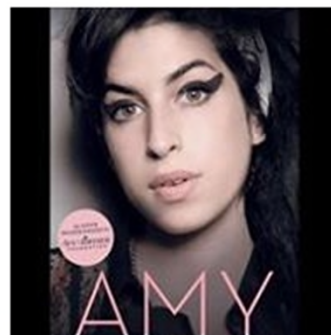
Snow Patrol ✓
Musician/Band



Contemporary R&B
Musical Genre



Diana Vickers ✓
Musician/Band



Amy Winehouse ✓
Musician/Band





KCS

Strategic Intelligence & Corporate Security

[Redacted Name]
United Kingdom | Information Technology and Services
Current
[Redacted]
Send [Redacted] nMail [Redacted]

101 connections

uk.linkedin.com/pub/[Redacted]/56/358/a66

Background

Experience

IT Operations Team Leader
[Redacted]
[Redacted] 2002 – Present (12 years 9 months)

1 recommendation

Tom McGeown
Senior Systems Administrator at Trimble Networks

Having worked closely with [Redacted] for many years I can recommend her without hesitation. She is an excellent leader, manager and organiser who pays attention to details whilst driving herself and her team towards the larger objective. Jodie is... View ↓



KCS

Strategic Intelligence & Corporate Security

Information divulged / obtained

- Sports teams
- Friends & G/F or B/F
- Family members
- Previous companies
- Ages (DoB)
- Interests / Hobbies
- Common Combinations

90% of Passwords

- Sports teams
- Friends & G/F or B/F
- Family members
- Previous companies
- Ages (DoB)
- Interests / Hobbies
- Common Combinations



KCS

Strategic Intelligence & Corporate Security

Demonstration



KCS

Strategic Intelligence & Corporate Security

Prepare and prevent, don't repair and repent.

(Anonymous)

Energy Charter Treaty: provides you with a unique tool to minimise your political risk

Michelle Bradfield
Partner
Dentons
April 2015

Investment Treaties

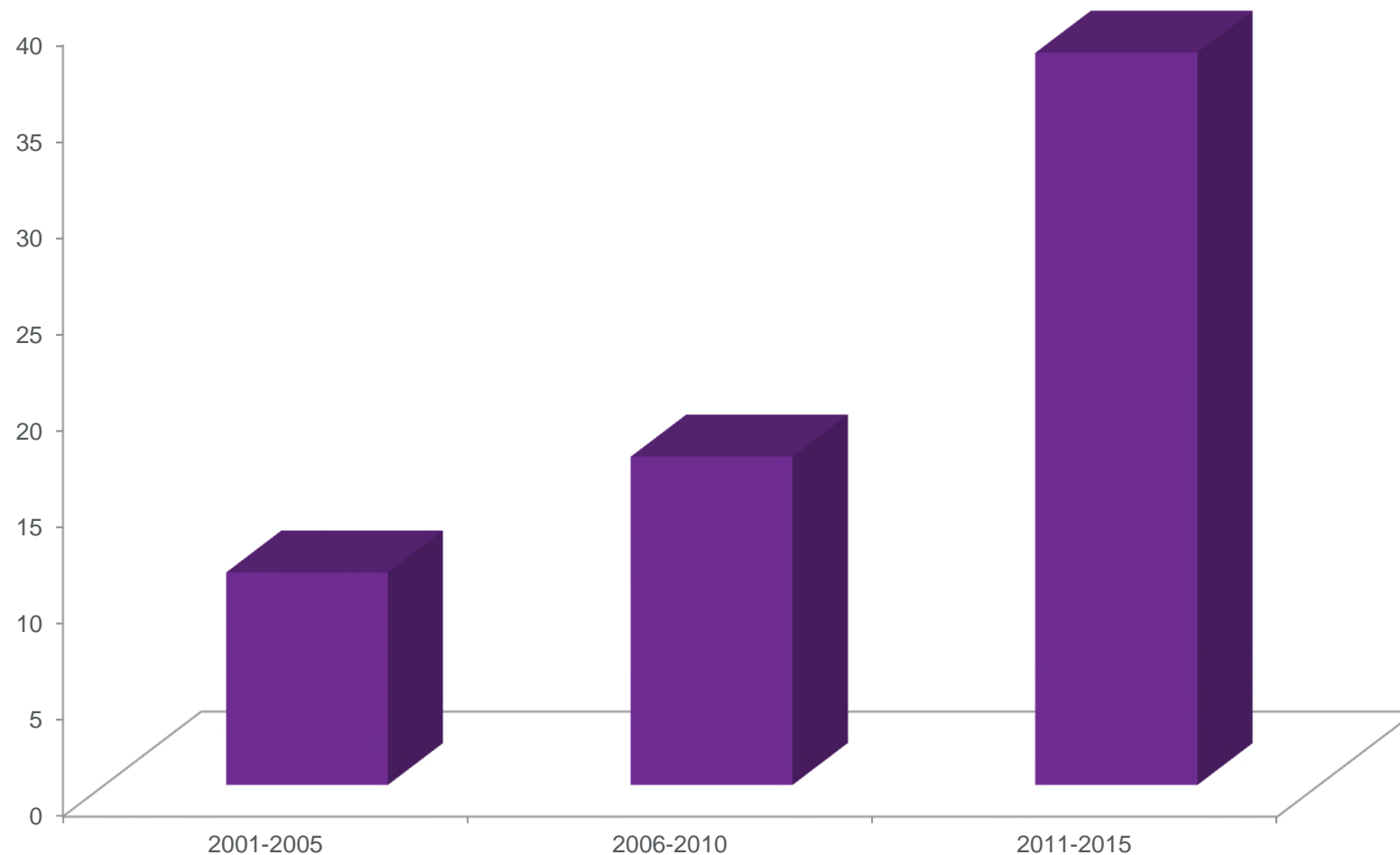
- Political risk is pervasive and exists when investing into any country.
- Cost-effective way of protecting your business and minimising this risk. They have many benefits over political risk insurance.
- Signed between countries and provide protections to companies from government interference in the investment.
- Protect against outright seizure and many forms of indirect or regulatory interference.
- No need for a direct relationship or contract with the host State.
- There are in excess of 3,500 bilateral investment treaties and many multilateral investment treaties, including the Energy Charter Treaty.

Overview of the Energy Charter Treaty

- The ECT is a treaty designed to promote energy security by protecting foreign investments in the energy sector.
- The substantive investment protections include a prohibition on expropriation without compensation and the requirement to accord "fair and equitable treatment", "protection and security", "national" and "most favoured national" treatment.
- Disputes are settled by independent tribunals under the established rules of international arbitration.
- The ECT entered into force in 1998 and has been signed by 52 states (including EU States, Japan, Australia, Turkey, Uzbekistan and the European Union).

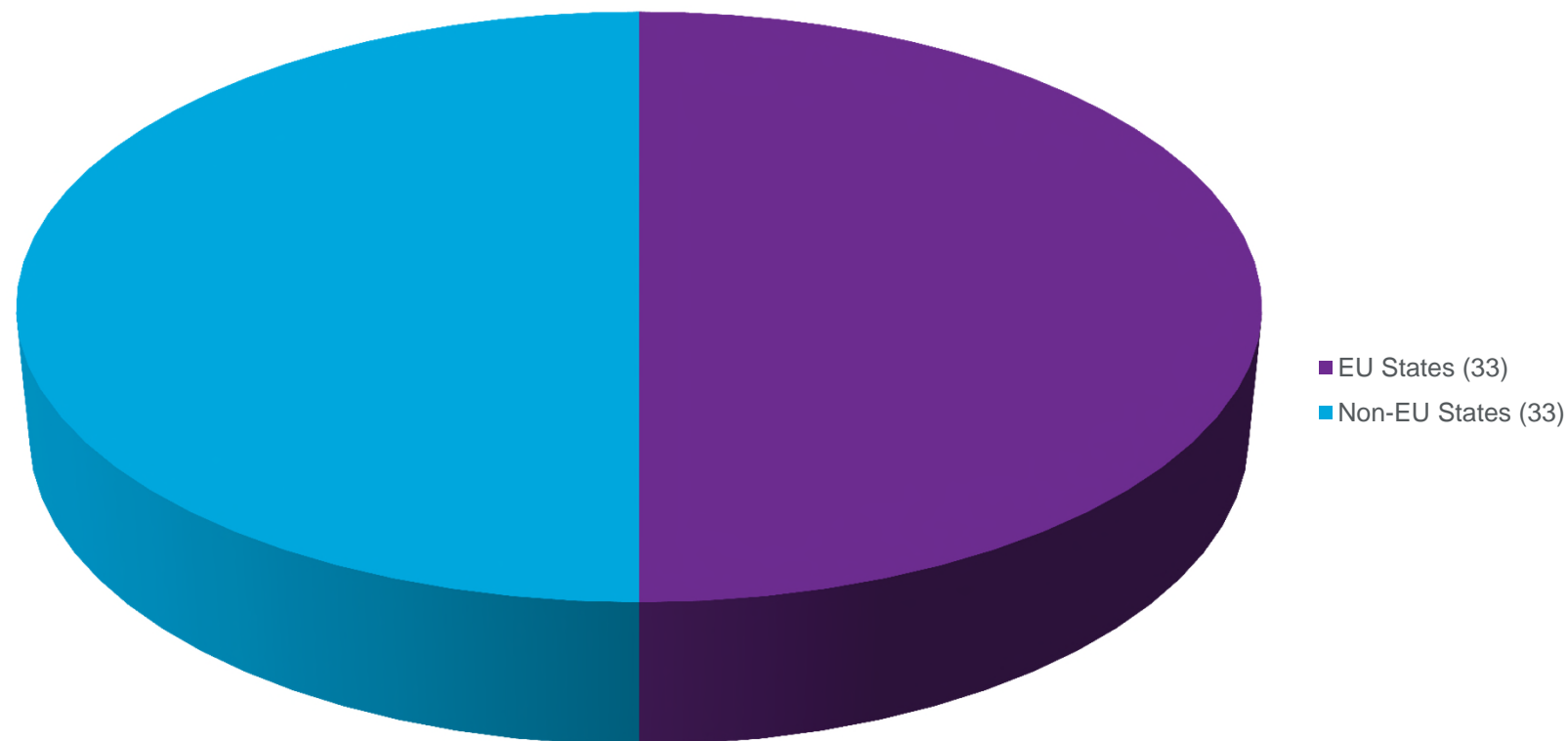
Do companies really use the ECT?

- There have been at least 66 claims against States.



How many countries have been sued under the ECT?

- 25 States have appeared as respondents, with the most common being Spain (15) and the Czech Republic (7).
- Germany (2), Croatia (1), Italy (1), Latvia (1) and Poland (1) have also been respondents.



Legislation change regarding the Solar industry...

- Numerous claims have been made against Spain, the Czech Republic and Italy which relate to a change in policy in the renewable energy sector.
- From 2010, each of these States have taken steps to scale back feed-in tariffs and other subsidies that had been put in place to attract foreign investment into their renewable energy sector.
- 7 claims have been initiated against the Czech Republic; 14 against Spain; 1 against Italy and many more are in the pipeline...
- The Claimants have alleged that the reversal of the States' various incentives has amounted to a breach of the following provisions: expropriation without compensation; fair and equitable treatment and full protection and security.

Other Recent Claims

- ***Yukos v Russia (2014)***: Russia was found to have breached the ECT through an unlawful expropriation via a "*calculated effort to destroy Yukos*" through tax collection, intimidation and harassment of staff, a rigged auction of Yukos' main production asset and bankruptcy proceedings. The Tribunal ordered Russia to pay US\$51.6b in damages.
- ***JKX v Ukraine (ongoing)***: JKX Oil & Gas is seeking US\$180m for the losses it has suffered from Ukraine's failure to treat its investments in a "fair and equitable" manner. The measures complained of include: (1) increasing royalties on gas from 28% to 55%, (2) requiring that gas be purchased solely from a State-owned company; and (3) imposing restrictions on foreign cash transactions and the repatriation of dividends.
- ***ALPIQ v Romania (ongoing)***: Swiss electric power production and distribution utility has filed a expropriation complaint against the Romanian State-controlled entity in respect of the termination of supply contracts.

Risk management for energy lawyers: key issues for 2015

21 April 2015