






# Regulatory expectations of Non-Executive Directors and their relationship with the CRO

Monday 25<sup>th</sup> April 2016

Peter Oakes

Copyright Peter Oakes 1

## Peter Oakes

- Executive and non-executive director and advisory committee member to regulated and unregulated companies, including Fintech, RegTech, MiFID and Funds
- Peter is the founder of Fintech Ireland, Fintech UK (RegTech Ireland & Regtech UK). These groups supports 'fintech' & 'regtech' initiatives in Ireland & the UK
- Board Director & Chief Risk Officer for Bank of America Merchant Services Europe based in London)
- Appointed as the Central Bank's first Director of Enforcement and AML/CTF Supervision in October 2010. In this role Peter was a member of the Senior Leadership, Operations, Policy and Supervisory Risk committees
- He is a solicitor admitted in Ireland, the United Kingdom and Australia. Over the past 25 years Peter has worked as a regulator (Ireland, UK & Australia) and in the investment management and funds industries (UK & Ireland). Peter has established a number of successful consultancy and training firms in Ireland. He has advised Central Banks, Regulators and their senior management on a wide range of supervisory and enforcement issues

©Peter Oakes  
[www.peteroakes.com](http://www.peteroakes.com) / [www.fintechireland.com](http://www.fintechireland.com) / [hello@fintechireland.com](mailto:hello@fintechireland.com) / ph +353 1 639 2971

2



## Director & Consulting Services


- Contact Peter to discuss non-executive director & consulting services for regulated financial entities, fintech & other innovative companies

 <https://ie.linkedin.com/in/peteroakes>

 [peter@peteroakes.com](mailto:peter@peteroakes.com)

 [+353 87 2731434](tel:+353872731434)

Copyright Peter Oakes 3



## Cyber Security – Regulatory Expectations overview

- Will focus on Irish and UK cyber security governance initiatives
  - and of course there are other regulators that are focussing on this area, e.g. EBA, IOSCO, ASIC, SEC and pretty much every EU regulator*
- The role of the Board
- The accountability of the Non-Executive Director (NED)
- The relationship between the Chief Risk Officer, the Board and the NED

Copyright Peter Oakes 4

## Looking back to 2002

- Lord Young of Graffham (former trade secretary to Margaret Thatcher), when President of the Institute of Directors:

hit out at what he called *corporate governance "box tickers"* who had built up the role of non-executive to a level where they were supposed to supervise the work of executive directors

boards will end up being *stuffed with people who know nothing* about the company

<http://www.independent.ie/business/have-you-heard-the-one-about-the-nonexecutive-director-26053112.html>

Copyright Peter Oakes

5

## The old view of the non-executive director?

- *What's the difference between a non-executive director and a shopping trolley? There's only so much food and drink you can cram into a shopping trolley.*




- *Why is a non-exec a bit like a bidet? It's there to add a bit of class to the place, but nobody really knows what it does.*



Copyright Peter Oakes

6




## Central Bank of Ireland - PRISM

- Central Bank of Ireland:
 

*We intend to supervise all financial firms in a way which makes it **materially less likely that they will, collectively or individually, fail in a way which endangers financial stability or consumers.** We see **systematic risk-based supervision** as offering the best route to that goal.*

Think of this in terms of cyber security & cyber risk

Copyright Peter Oakes 7



## Where might cyber security sit within PRISM?

Credit Risk	Market Risk	Operational Risk	Insurance Risk	Capital Risk	Liquidity Risk	Governance Risk	Strategic Business Model Risk	Environmental Risk	Conduct Risk
Inherent Credit Risk	Inherent Market Risk	Inherent Operational Risk	Inherent Insurance Risk	Excess Margin/ Capital		Board & Committee Quality		Sector Specific Risks	Inherent Risk of Products
Quality of Controls in Credit Risk	Quality of Controls in Market Risk	Financial Crimes Controls	Quality of Controls in Insurance Risk	Group Relations/ Structural		Management Quality		Macro Economic Risks	Conduct Risk Controls
Concentration of Credit Risk	Concentration of Market Risk	Quality of Controls in Operational Risk	Reinsurance Risk Concentration			Internal Audit Quality			
						Culture & Compensation			
						Supervisory & Structural Complexity			
						Risk Management Quality			


Central Bank publishes findings of Cyber Security / Operational Risk Thematic Inspection

23 September 2015

[View industry letter](#)

In February, the Central Bank as part of its on-going supervisory engagement, published a series of aligned thematic inspections for 2015. This included a thematic inspection in relation to **Cyber Security / Operational Risk** which was concluded recently. The results have been communicated to the boards and senior management of investment firms, funds and service providers and stock-brokers.


Copyright Peter Oakes 8



## Data Security & Cyber Security

### - Financial Crime

- FCA refers regulated firms to [examples of good and poor practice in data security](#) at Chapter 5 in Part 1 and Chapters 6 and 10 in Part 2 of our Financial Crime: A Guide for Firms
- “Outsourcing to a 3rd party [does not mean you have outsourced your obligations](#) to look after customer data. [Must] carry out due diligence on 3<sup>rd</sup> party suppliers [before hiring them](#), try to establish what their vetting procedures are, and ensure that they respect your firm’s security arrangements”
- If you are a senior manager or board director of a FCA regulated entity take note




Financial Conduct Authority

**Financial crime: a guide for firms**  
Part 1: A firm’s guide to preventing financial crime

April 2015


Copyright Peter Oakes 9



## Is it really a matter for the Board? YES!

- See Central Bank letter on operational risk & cyber security dated 22 September 2015

“It is the responsibility of the board to ensure that a firm is properly governed”



Bank Creditors in Ireland  
Central Bank of Ireland  
Dublin

22 September 2015

Review of the management of operational risk around cyber-security within the Investment Firm and Fund Services Industry

Dear Chair,


The Central Bank of Ireland (the ‘Central Bank’) recently undertook a thematic review to assess the management of cyber security and related operational risks across Investment Firms, Fund Service Providers and Stockbrokers. The objective of the review was to examine firms’ control environments (including policies and procedures) designed to detect and prevent cyber security breaches as well as board oversight of cyber security.

Cyber security is steadily emerging as an increasingly recognised risk in all firms. This is primarily due to the increasing reliance by firms in all sectors on information technology (IT), the evolving sophistication of cyber-crimes and the growing frequency in the type and number of cyber related breaches, attempts, attacks and intrusions. Valuable assets including confidential data, cash and intellectual property should therefore be protected by appropriate security, processes and policies.

Firms should be aware that cyber security risk is a real and live threat and a successful attack could have a significant negative impact on daily operations. Firms need to recognise that a successful cyber-attack can also have far-reaching financial and reputational implications; therefore appropriate levels of security are required to be in place.

It is the board’s responsibility to ensure that a firm is properly governed and has the necessary processes and systems to protect the firm and all of its assets. The review found that in a number of firms IT security, including cyber security, is deemed to be the sole responsibility of the IT department with limited involvement, if any, from other business areas or from the board itself.

Copyright Peter Oakes 10



## Why would a non-executive director care? (1/4)

Section 189 MiFID Regulations (SI 60/2007)


189. (1) Where an offence is committed under these Regulations by a body corporate and is proved to have been committed with the consent, connivance or approval of or to have been attributable to the willful neglect on the part of any person, being –

- (a) director, manager, secretary or other officer of the body corporate, or
- (b) a person who was purporting to act in any such capacity,

that person as well as the body corporate is guilty of an offence and is liable to be proceeded against and punished as if that person were guilty of the first-mentioned offence.

(2) A person may be charged with having committed an offence under these Regulations even if the body corporate concerned is not charged with having committed an offence under these Regulations in relation to the same matter.


Copyright Peter Oakes 11



## Why would a non-executive director care? (2/4)

- Cannot locate an offence in the MiFID Regulations that appears to categorically state that a breach of cyber security is a breach of MiFID [but consider PSD Regs]
- However note that a breach of Regulation 160 of MiFID (safeguarding clients' rights) would be a **prescribed contravention**


Copyright Peter Oakes 12



## Why would a non-executive director care? (3/4)

- Under Part IIIC of the Central Bank Act 1942 the *Irish Central Bank can take administrative sanction procedures against both the regulated financial service providers and persons concerned in their management* (where that person participated in the prescribed contravention, e.g. a director, manager etc)
- Fitness & Probity Standards  
A director could also be *brought to task under these standards*


Copyright Peter Oakes 13



## Why would a non-executive director care? (4/4)

- Section 111 of the Criminal Justice (Money Laundering & Terrorist Financing) Act 2010  
the Irish and UK AML/CFT regimes are fairly similar  
note FCA Financial Crime issue above
- Section 29 Data Protection Acts (1988 & 2003)


Copyright Peter Oakes 14



## Section 29 Data Protection Acts (Ireland)

- (1) Where an offence under this Act has been committed by a body corporate and is proved to have been committed with the consent or connivance of or to be attributable to any neglect on the part of a person, being a director, manager, secretary or other office of that body corporate, or a person who was purporting to act in any such capacity, that person, as well as the body corporate, shall be guilty of that offence and be liable to be proceeded against and punished accordingly
- (2) So consider *if breaches of safeguarding and the duty of care* in the Acts would expose a director to criminal liability

Copyright Peter Oakes 15




## PSD 2 (1/3)

- 68 instances of the word ‘security’ appearing in PSD 2
- Article 5(1)(f) – “a description of the procedure in place to monitor, handle and follow up a *security incident and security related customer complaints*, including an incidents reporting mechanism which takes account of the notification obligations of the payment institution laid down in Article 96”

Copyright Peter Oakes 16






## PSD 2 (2/3) – Article 94

### fintech - Data Protection

- 1. Member States shall permit processing of personal data by payment systems and payment service providers when *necessary to safeguard the prevention, investigation and detection of payment fraud*. The provision of information to individuals about the processing of personal data and the processing of such personal data and any other processing of personal data for the purposes of this Directive shall be carried out in accordance with Directive 95/46/EC, the national rules which transpose Directive 95/46/EC and with Regulation (EC) No 45/2001.
- 2. Payment service providers *shall only access, process and retain personal data necessary for the provision of their payment services, with the explicit consent of the payment service user*.

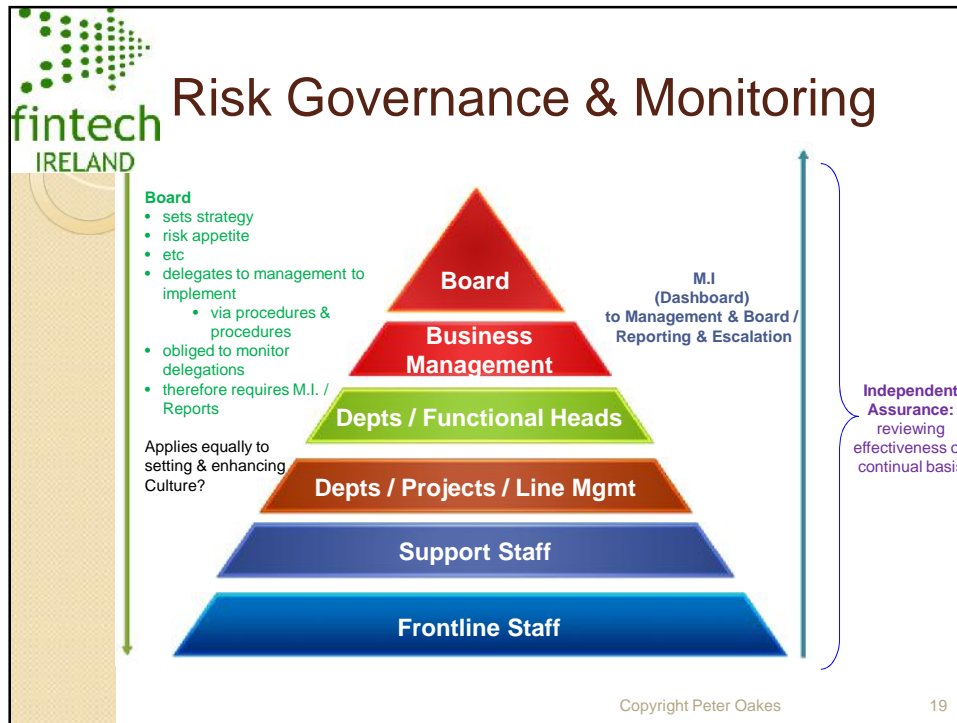
Copyright Peter Oakes 17



## PSD 2 (3/3) - Article 95(1)

- Member States shall ensure that payment service providers *establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks*, relating to the payment services they provide.
- As part of that framework, *payment service providers shall establish and maintain effective incident management procedures, including for the detection and classification of major operational and security incidents*.

Copyright Peter Oakes 18




**fintech IRELAND**

## Board & Chief Risk Officer

- Should the CRO have an **automatic seat on the Board**?
- Does he/she sit on Audit, Risk & Compliance etc Committees?
- What about the CIO / CISO?
  - should he/she be on the Board?
  - who on the Board has the relevant information and security risk experience to ensure that these 'business critical' areas are covered by the Board
  - it's a problem in fintech and innovation!*
- Article 95(2) & Article 96 should drive a closer relationship between the Board & the CRO, the CIO and the CISO
- Article 95(2): Member States shall ensure that payment service providers *provide to the competent authority on an annual basis, or at shorter intervals as determined by the competent authority, an updated and comprehensive assessment of the operational and security risks relating to the payment services* they provide and on the adequacy of the mitigation measures and control mechanisms implemented in response to those risks.


Copyright Peter Oakes 20



## Accountability of the CRO & other C-suite officers?

- See above for directors, managers and persons concerned in the management
- Note the new UK Senior Mangers Regime  
BoE says – “*aimed at supporting a change in culture at all levels in firms through a clear identification and allocation of responsibilities to individuals responsible for running them*”
- What about this concept in the USA of supervisory liability  
recent case in the USA of a compliance officer being held accountable  
*BBH did not have an adequate supervisory system* to prevent the distribution of unregistered securities. BBH's former Global AML Compliance Officer Harold Crawford was also fined \$25,000 and suspended for one month
- However plenty of cases where UK FCA/FSA has taken enforcement action against compliance officers

Copyright Peter Oakes 21



## Some 'recent' comments by US SEC

- SEC - *The Role of Chief Compliance Officers Must be Supported*  
June 2015 by Commissioner Luis A. Aguilar
- Could we apply these instances of CCO liability to the role of the CRO?
- In which case the NED & the CRO have a symbiotic relationship  
its in their mutual interest to forge a trusting relationship

Copyright Peter Oakes 22

## Question is, what type of symbiotic relationship is it?

### Obligate vs Facultative

- Most parasites are **OBLIGATE** - that is they must live parasitically and die when their host dies
- Obligate parasites also have very few specialised structures for feeding or locomotion
- Some fungi are **FACULTATIVE** parasites since they can continue to feed saprophytically once their host has died
- Fewer facultative parasites have evolved as they must form complicated systems to detect, take in and digest food. Due to natural selection they would be at a disadvantage to obligate parasites.

Copyright Peter Oakes

23

## What keeps the CRO awake at night?



Copyright Peter Oakes

24



# Thank you

Contact Peter Oakes

 <https://ie.linkedin.com/in/peteroakes>

 [hello@fintechireland.com](mailto:hello@fintechireland.com)

 [+353 87 2731434](tel:+353872731434)



Copyright Peter Oakes 25