



Society of Actuaries in Ireland

Enterprise Risk Management Forum

10th May 2016

Agenda

- ERM Committee objectives 2016 (Eric Brown)
- A regulatory perspective on consumer risk (Helena Mitchell – Central Bank of Ireland)
- The cyber threat landscape (Detective Inspector Michael Gubbins, Computer Crime Investigation Unit)
- Current hot topics (Tom Donlon)

Disclaimer:

The material, content and views in the following presentation are those of the presenter(s).



Society of Actuaries in Ireland

ERM Committee Objectives 2016

10th May 2016



SAI ERM Committee - Objectives 2016

Group	Objectives
Risk	Consider Emerging risks and hot topics
Communications	Develop a communication strategy and increase awareness of ERM amongst members
Learning	Organise learning opportunities and promote awareness of risk management courses
Research	Promote research activities
Regulation	Influence consultations and consider need for ERM ASPs or IANs
Relationships	Develop links with risk management associations and other parties



ERM committee members

- Tom Donlon (chair)
- Brian Morrissey
- Richard McMahon
- Alex Breeze
- Eamonn Mernagh
- Danielle O'Sullivan
- Colm Fitzgerald
- Eric Brown
- Don Browne
- Jean Rea
- Eamonn Phelan
- Billy Galavan

“The Cyber Threat Landscape”

Society of Actuaries

Risk Management Seminar

Chartered Accountants House,

Pearse Street,

Tuesday 10th May 2016

Detective Inspector Michael Gubbins

Computer Crime Investigation Unit

- Garda Bureau of Fraud Investigation
- National Unit
 - Forensic Examinations
 - Cybercrime Investigation
 - International Liaison



Connected Life



7,27 bn
current world population

90 bn
Google
searches so far this year

2 mln 
blog posts written today


Tweets sent today
423 mln



3,01 bn
Internet users worldwide



monthly active users
1,4 bn



7 bn
mobile devices worldwide



By **2020**
total connected devices
12 bn
mobile connected devices



70%
Internet penetration in Europe

51%
of employees connect to unsecured wireless networks with their smartphones




115 bn
Emails sent today

2014 in Numbers

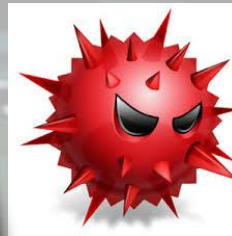


19%
Android users
encountered a
mobile threat

15,577,912
malicious mobile
apps worldwide



123,054,503
unique malicious
objects detected



12,100
mobile banking
Trojans



38%
of user computers
subjected to at least
one web attack

over **307** new
cyber threats every
minute, **5**
more than
every second



annually

Cybercrime costs
\$445 billion
or ~ **1%**
of global
income



1,432,660,467



attacks launched
from online resources

Current Cybercrime Activity

- CEO Fraud (Invoice re-direct)
- DDOS - DD4BC, Armada Collective & Lizard

Squad

- PABX/IRSF Fraud
- Ransomware
- Phishing
- DDoS - Operation Icarus

Email 1

On 2 Jul 2015, at 19:03, Sean Murphy
<Sean.Murphy@abc123.com> wrote:>> >> I
need to sort out a financial obligation urgently.
What details do i need to give you to make a
wire transfer?>> >> Sean.>> >> Sent from my
iPhone

E-mail Header for E-mail 5

Delivered-To: Jack.Ryan@abc123.com

Received: by 10.194.19.195 with SMTP id h3csp829294wje; Thu, 2 Jul 2015 14:12:24 -0700 (PDT)

X-Received: by 10.194.93.198 with SMTP id cw6mr64571537wjb.113.1435871544283; Thu, 02 Jul 2015 14:12:24 -0700 (PDT)

Return-Seanh: Sean.Murphy@abc123.com

Received: from emkei.cz (emkei.cz. [46.167.245.71]) by mx.google.com with ESMTMP id q14si10912314wju.110.2015.07.02.14.12.24 for <Jack.Ryan@abc123.com>; Thu, 02 Jul 2015 14:12:24 -0700 (PDT)

Received-SPF: softfail (google.com: domain of transitioning Sean.Murphy@abc123.com does not designate 46.167.245.71 as permitted sender) client-ip=46.167.245.71;

Authentication-Results: mx.google.com; spf=softfail (google.com: domain of transitioning Sean.Murphy@abc123.com does not designate 46.167.245.71 as permitted sender) smtp.mail=Sean.Murphy@abc123.com

Received: by emkei.cz (Postfix, from userid 33) id C190FD56B5; Thu, 2 Jul 2015 23:12:20 +0200 (CEST)

To: Jack.Ryan@abc123.com

Subject: Re: RequestFrom: "Sean Murphy" Sean.Murphy@abc123.com

X-Priority: 3 (Normal)

Importance: Normal

Errors-To: Sean.Murphy@abc123.com

Reply-To: Sean Murphy replytome-8@myway.com

Content-Type: text/plain; charset=utf-8

Message-Id: 20150702211220.C190FD56B5@emkei.cz

Date: Thu, 2 Jul 2015 23:12:20 +0200 (CEST)

Okay let me have a confirmation copy when it is done. I will brief you more later.

Here are the details:

Account name: ACME Ltd
Bank name: VOLKSBANK IM MK
Account Number:2004xxxx
Bank Code: 44xxxxxx

IBAN: DE 10 44xx xxxx 0020 04xxxx
BIC: xxxxxxxxx
Reason: Marketing
Amount: 8,914.90 Euros

Sean.

Sent from my iPhone

Fake E-Mails – <https://emkei.cz/>

The screenshot shows a web browser window with the URL <https://emkei.cz/>. The page features a navigation menu with 'File', 'Edit', 'View', 'Favorites', 'Tools', and 'Help'. A 'Select Language' dropdown is visible. The main content area displays the 'EMKEI'S MAILER' logo in a stylized green font. Below the logo, a description reads: 'Free online fake mailer with attachments, encryption, HTML editor and advanced settings...'. The form includes fields for 'From Name' (Brian Honan), 'From E-mail' (brian.honan@gmail.com), 'To' (michael.p.gubbins@garda.ie), 'Subject' (Spoofed email), and 'Attachment' (Browse...). There are also fields for 'Reply-To' (test@gmail.com), 'Errors-To', 'CC', and 'Bcc'. The 'Priority' is set to 'Normal' (radio button selected), and the 'X-Mailer' is set to '- none -'. At the bottom, there are fields for 'Confirm delivery' and 'Confirm reading'. On the left side, there are social media sharing buttons for Flattr, Bitcoin, and Litecoin, along with a QR code and a 'Like' button. On the right side, a white box contains the text: 'Please support emkei.cz by clicking advertisement on miniGambler.com if you are interested in. Thank you in advance for supporting the existence of this site.'

DD4BC

Hello,

To introduce ourselves first:

<http://www.coindesk.com/bitcoin-extortion-dd4bc-new-zealand-ddos-attacks>

<http://bitcoinbountyhunter.com/bitalo.html>

<http://cointelegraph.com/news/113499/notorious-hacker-group-involved-in-excoin-theft-owner-accuses-ccedk-of-withholding-info>

Or just google “DD4BC” and you will find more info.

So, it’s your turn!

All your servers are going under DDoS attack unless you pay 30 Bitcoin.

Pay to [1XFz3YBkSRNsNoQBasHrBZ6mgTEb5tAHL](https://blockchain.info/address/1XFz3YBkSRNsNoQBasHrBZ6mgTEb5tAHL)

Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps.

Right now we are running small demonstrative attack on one of your IPs:

123.123.123.123

Don't worry, it will not be hard and will stop in 1 hour. It's just to prove that we are serious.

We are aware that you probably don't have 30 BTC at the moment, so we will wait 24 hours.

Find the best exchanger for you on howtobuybitcoins.info or localbitcoins.com

You can pay directly through exchanger to our BTC address, you don't even need to have BTC wallet.

Current price of 1 BTC is about 230 USD, so we are cheap, at the moment. But if you ignore us, price will increase.

IMPORTANT: You don't even have to reply. Just pay 30 BTC to [1XFz3YBkSRNsNoQBasHrBZ6mgTEb5tAHL](https://blockchain.info/address/1XFz3YBkSRNsNoQBasHrBZ6mgTEb5tAHL) – we will know it's you and you will never hear from us again.

We say it because for big companies it's usually the problem as they don't want that there is proof that they cooperated.

If you need to contact us, feel free to use some free email service.

Or contact us via Bitmessage: BM-NC1jRewNdHxX3jHrufjxDsRWXGdNisY5

International Action Against DD4BC Cybercriminal Group – Dec 2016

“Distributed Denial of Service (DDoS) attacks remain a considerable threat in the European Union and beyond. This type of extortion attack has become a well-established criminal enterprise and has affected thousands of victims globally, with the number of unreported incidents believed to be much higher. The absence of reporting by private companies and individuals poses particular difficulties in law enforcement’s efforts to prosecute these cyber threats.”

From: LZ Security [sec@lqsec.com]
Sent: 28 April 2016
To:
Subject: DDoS Attack Imminent - Important information

PLEASE FORWARD THIS EMAIL TO SOMEONE IN YOUR COMPANY WHO IS ALLOWED TO MAKE IMPORTANT DECISIONS!

We are the Lizard Squad and we have chosen your website/network as target for our next DDoS attack.

Please perform a google search for "Lizard Squad DDoS" to have a look at some of our previous "work". All of your servers will be subject to a DDoS attack starting at Tuesday the 3rd of May.

What does this mean?

This means that your website and other connected services will be unavailable for everyone, during the downtime you will not be able to generate any sales. Please also note that this will severely damage your reputation amongst your users / customers as well as strongly hurt your google rankings (worst case = your website will get de-indexed).

How do I stop this?

We are willing to refrain from attacking your servers for a small fee. The current fee is 5 Bitcoins (BTC). The fee will increase by 5 Bitcoins for each day that has passed without payment. Please send the bitcoin to the following Bitcoin address: 18QXdP9LUATBTisHJeA2jYRXJfQ1xoYET6. Once you have paid we will automatically get informed that it was your payment. Please note that you have to make payment before Tuesday the 3rd of May or the attack WILL start!

How do I get Bitcoins?

You can easily buy bitcoins via several websites or even offline from a Bitcoin-ATM. We suggest you to start with <http://scanmail.trustwave.com/?c=6600&d=jPmi16G3vRp9LiFnJJWzG7yCiPYaLh-E4xvcxGUyvg&s=342&u=http%3a%2f%2flocalbitcoins%2ecom> or do a google search.

What if I don't pay?

If you decide not to pay, we will start the attack at the indicated date and uphold it until you do, there's no counter measure to this, you will only end up wasting more money trying to find a solution. We will completely destroy your reputation amongst google and your customers and make sure your website will remain offline until you pay.


This is not a hoax, do not reply to this email, don't try to reason or negotiate, we will not read any replies. Once you have paid we won't start the attack and you will never hear from us again!

Please note that Bitcoin is anonymous and no one will find out that you have complied.

International Revenue Share Fraud




- Fraudster Strikes Revenue Sharing Deal with Local Carrier in High Cost Destination




- Fraudster Gains Illegal Access to VoIP Service Provider's Network



- Fraudster "Pumps" Call Traffic through Compromised Network to High Cost Destination



- Fraudster Collects A Profit Percentage from Local Carrier



- Hacked VoIP Service Provider Gets Stuck with the Bill

Howto_Restore_FILES.HTM x

file:///C:/Users/User/Desktop/Howto_Restore_FILES.HTM

NOT YOUR LANGUAGE? USE [Google Translate](#)

***What happened to your files?**
All of your files were protected by a strong encryption with RSA-4096
More information about the encryption RSA-4096 can be found here: [http://en.wikipedia.org/wiki/RSA_\(cryptosystem\)](http://en.wikipedia.org/wiki/RSA_(cryptosystem))

What does this mean?
This means that the structure and data within your files have been irrevocably changed, you will not be able to work with them, read them or see them, it is the same thing as losing them forever, but with our help, you can restore them.

How did this happen?
Especially for you, on our server was generated the secret keypair RSA-4096 - public and private.
All your files were encrypted with the public key, which has been transferred to your computer via the Internet.
Decrypting of YOUR FILES is only possible with the help of the private key and decrypt program, which is on our Secret Server!!!

What do I do?
Alas, if you do not take the necessary measures for the specified time then the conditions for obtaining the private key will be changed.
If you really need your data, then we suggest you do not waste valuable time searching for other solutions because they do not exist.

For more specific instructions, please visit your personal home page, there are a few different addresses pointing to your page below:

1. <http://idjsnfnkwjefnsdf.likinrealm.com/>
2. <http://krfdnhfnsai3d.abeleros.com/>
3. <http://idjsnfnkwjefnsdf.likinrealm.com/>
4. <https://4nauizsaaopuj3qj.onion.to>
5. <https://4nauizsaaopuj3qj.tor2web.org/>
6. [https://4nauizsaaopuj3qj.onion.cab/!](https://4nauizsaaopuj3qj.onion.cab/)

If for some reasons the addresses are not available, follow these steps:

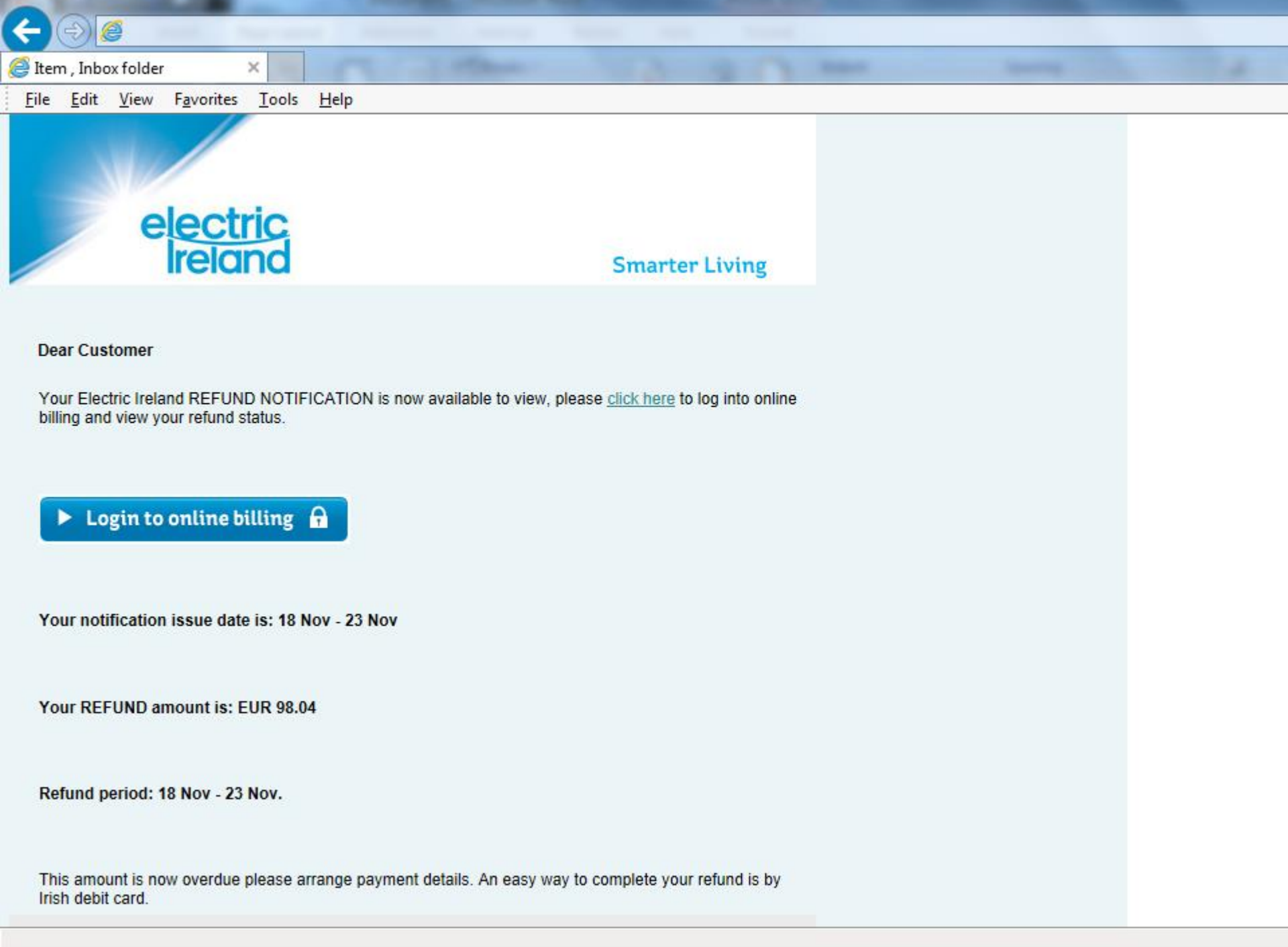
1. Download and install tor-browser: <http://www.torproject.org/projects/torbrowser.html.en>
2. After a successful installation, run the browser and wait for initialization.
3. Type in the tor-browser address bar: 4nauizsaaopuj3qj.onion/
4. Follow the instructions on the site.

!!! IMPORTANT INFORMATION:

Your Personal PAGES:
<http://idjsnfnkwjefnsdf.likinrealm.com/>
<http://krfdnhfnsai3d.abeleros.com/>
<http://idjsnfnkwjefnsdf.likinrealm.com/>
<https://4nauizsaaopuj3qj.onion.to/>

Your Personal TOR-Browser page : 4nauizsaaopuj3qj.onion/

Your personal ID (if you open the site directly):



Smarter Living

Dear Customer

Your Electric Ireland REFUND NOTIFICATION is now available to view, please [click here](#) to log into online billing and view your refund status.

▶ Login to online billing 

Your notification issue date is: 18 Nov - 23 Nov

Your REFUND amount is: EUR 98.04

Refund period: 18 Nov - 23 Nov.

This amount is now overdue please arrange payment details. An easy way to complete your refund is by Irish debit card.

Log Out



Check out our rewards club where we reward our customers just for choosing us. It's our little way of saying thank you!

Your Account

Refunds

Account Details

View Bill

View Transactions

Pay Gas Bill

View Next Bill Date

Paperless Billing

Online Direct Debit

Refunds

Please use the form below to complete your refund.

Please select your bank

Continue

Please select your bank

Allied Irish Banks

Ulster Bank

Bank of Ireland

Permanent TSB

Other

will need to provide the necessary
please select "Other"

Refunds

Please use the form below to complete your refund.

Total amount to be refunded: €61.74

Bank of Ireland 

Full Name :

(exactly as it appears on the card in upper case: E.G. MR ALAN SMITH)

Address :

Credit/Debit Card Number:

Card Verification Number:

3-Digit Card Security Code

Card Expiration Date:

 -

(mm / yyyy)

Date of birth:

 - -

(mm / dd / yy)

First 4 digits of your current account number:

(first 4 digits of your Current Bank Account number)

Street or area you lived when you were 10:

Mother's Maiden Name:

Verified by Visa / MasterCard Secure Password

:

(if you don't have one type NONE)

Submit

In the Media

Security

Irish government websites hit by widening DDoS attacks

First they came for the forums. Then the lottery. Now...

22 Jan 2016 at 16:20, John Leyden



A number of Irish government-related and public sector websites were knocked offline by an apparent DDoS attack on Friday morning.

The **latest assaults** follow apparently similar web attacks on the popular boards.ie discussion boards (**bang**) and the Irish National Lottery earlier (**wallop**) this week.

At the time of first of the assaults against boards.ie, an individual using a pseudonym got in touch to suggest follow-up assaults against a wider range of Irish sites would follow, ostensibly motivated by a desire to highlight security weaknesses.

This is the beginning of a national cybersecurity audit. There is a team of security folks testing a lot of Irish websites.

They have indicated that news outlets and financial institutions will be next. Their goal is to highlight poor security practices within Ireland and to raise the bar on a national level.

More like this

Cybercrime

Ddos



Most read



Sainsbury's Dank web pages stuck on crappy

Major Data Breaches in 2015



February

Anthem
BlueCross BlueShield
Records of about 80 million people have been stolen.

March

PREMERA
BLUE CROSS
Health records of about 11 million people have been compromised.

April

AdultFriendFinder
Database of almost 4 million records of dating site users has been hacked and leaked.

May

IRS
Data of 300,000 US taxpayers has been compromised in course of Internal Revenue Service hack.

June

Office of Personnel Management
Data of 21.5 million government employees has been stolen.

TRUMP
HOTEL COLLECTION
Debit and credit cards of hundreds of customers have been compromised.

]HackingTeam[
400GB of data was leaked online.

ASHLEY MADISON.COM
Personal information from 37 million of the site's members was leaked online.

bitdefender
Data of 400 million customers was put at risk.

November

TalkTalk
Personal data of 156,959 customers was stolen.

October

Experian
Personal data of 15 million T-Mobile customers was stolen.

September

Excellus
Data of 10.5 million people has been compromised.

August

Carphone Warehouse
Personal and financial details of 2.4 million people were stolen.

July

MALWARE: COMMON SOURCES OF INFECTION



EMAIL: Opening suspicious or unsolicited attachments or clicking on links from spam/phishing emails and unknown senders



WEBSITES: Clicking on links to unknown websites or just by visiting them (i.e. websites featuring adult content)



POP-UP WINDOWS: Clicking on them to download software or to view compromised advertisements



OPEN WI-FI: Cybercriminals use these networks to harvest your personal data and access your electronic systems



SOFTWARE: Downloading pirated or free software (games, screen savers, etc.) or downloading files via peer-to-peer networks



REMOVABLE STORAGE DEVICES: Malware can spread by copying itself to any removable device connected to a computer system



Cybercriminals will use social engineering and phishing techniques to trick you into performing any of the described actions and obtain your personal information

Predictions for 2016

- Online extortion
- Next generation mobile payment apps
- Ransomware
- Destructive data breach attacks
- Data Protection Officers, Chief Risk Officer & Chief Information Security Officer

EU NIS Directive

- Improve cybersecurity capabilities in Member States
- Improve Member States' cooperation on cybersecurity
- Require operators of essential services in the energy, transport, banking and healthcare sectorsto take appropriate security measures and report incidents to the national authorities

Criminal Justice (Offences Relating To Information Systems) Bill 2016

Provisions of the Bill

Section 1 provides the necessary interpretation provisions and includes a definition of “information system”.

Section 2 provides that it is an offence to intentionally access an information system without lawful authority.

Section 3 makes it an offence to intentionally interfere with an information system so as to hinder or interrupt its functioning.

Section 4 provides that it is an offence to intentionally interfere with data on an information system.

Section 5 makes it an offence to intentionally intercept the transmission of data to, from or within an information system.

Criminal Justice (Offences Relating To Information Systems) Bill 2016

Section 6 provides that it is an offence to intentionally produce, sell, procure for use, import, distribute, or otherwise make available, a device, computer programme, password, code or data for the purpose of the commission of an offence under sections 2, 3, 4 or 5.

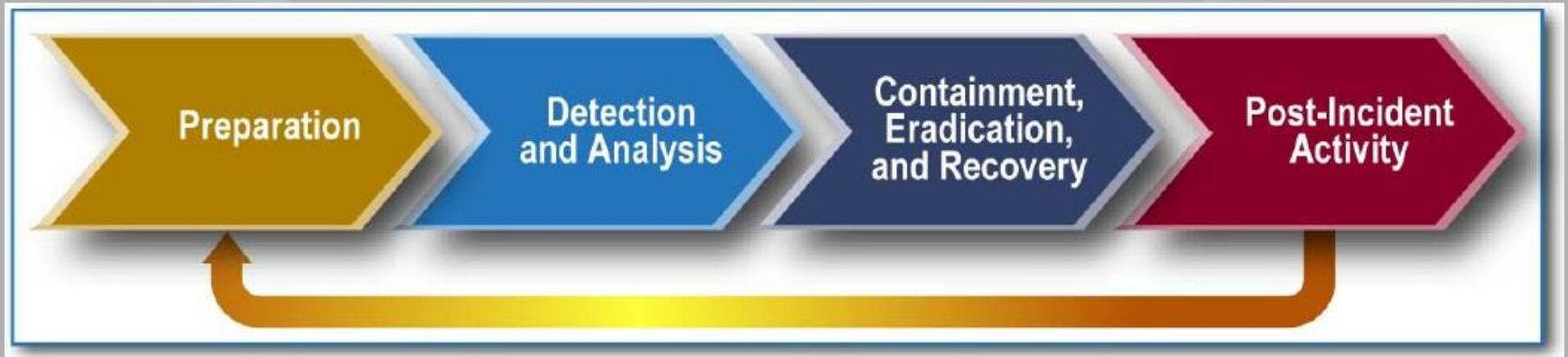
Section 7 provides for a search warrant to be issued to the Garda Síochána by the District Court in relation to the investigation of the suspected commission of offences under the Act. It also sets out the process involved, how the search warrant will operate and provides for related matters.

Section 8 sets out the penalties in respect of offences under the Act.

Section 9 clarifies that where an offence under the Act is committed by a body corporate, liability shall rest with the person acting on behalf of the body corporate as well as with the body corporate itself.

Section 10 establishes legal jurisdiction with regard to the commission of offences under sections 2 to 6 of the Act.

Incident Response



What do we want from you?

- People
- Time
- Statements
- Exhibits



< CCIU will not interrogate your system >

Europol

- J-CAT
 - Malware
 - Botnets
 - Intrusion
 - crime facilitation
 - bulletproof hosting
 - counter-anti-virus services
 - infrastructure leasing and rental
 - money laundering (inc VC)
 - online fraud
 - online payment systems
 - Carding
 - social engineering
- Europol Malware Analysis System (EMAS)
- Cross matching
- Joint Action Day (Airport Action Day)



“Security-by-design and privacy-by-design should be the guiding principles when developing smart devices and when collecting and processing data. This includes the need to only collect the minimum amount of data necessary, automatically protect personal data by using proactive security measures and means to make individuals less identifiable.”

F



H

 **EUROPOL**

EC3
European Cybercrime
Centre

**The Internet Organised Crime
Threat Assessment (IOCTA)**

DDoS

HSBC online banking crashes after cyber attack

The bank says it is defending itself against the hackers, as disruption leaves customers locked out of their accounts

101 0 90 191 Email



Another payday, another banking glitch for HSBC Photo: GEOFF PUGH

By Julia Bradshaw
9:00PM GMT 29 Jan 2016
Follow 969 followers

HSBC is apologising to angry customers after its online banking service crashed after coming under cyber attack.

 **HSBC UK** 
@HSBC_UK 

We are working hard to restore services, and normal service is now being resumed. We apologise for any inconvenience. 2/2
11:22 AM - 29 Jan 2016
57 22

SET YOUR POCKETS FREE

✗ GO FROM THIS..



✓ TO THIS



Start slimming your wallet with...



Proactive Prevention

Barclays hacks its own systems | Barclays - Google Chrome
https://www.home.barclays/news/2015/10/barclays-hacks-its-own-systems-to-stay-ahead-of-the-cyber-crimin.html

BARCL L 166.90p ↓ -2.10 Contact Us UK online banking


BARCLAYS Search by keyword Search

News About us Investor Relations Citizenship Careers Products and services

Barclays hacks its own systems to stay ahead of the cyber criminals

08 Oct 2015

[f](#)
[in](#)
[t](#)
[✉](#)



Barclays is hacking its own computer systems to stop cyber-attacks and protect customers.

Troels Oerting, Chief Information Security Officer, has set up a team to attack our systems to find flaws and fix them before thieves, vandals or terrorists can exploit them.

"We emulate how criminals will try to get into the bank," said Troels. "Then the red unit will do the

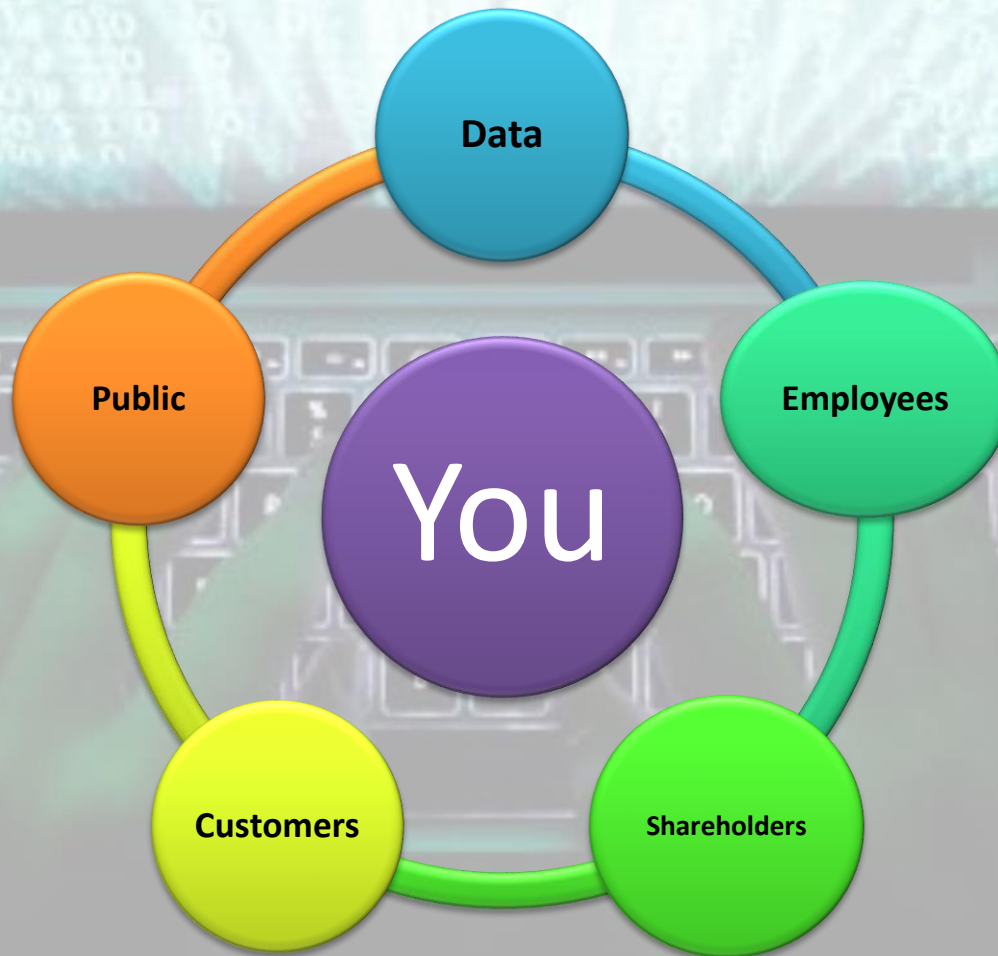
Latest News

CITIZENSHIP
Choose Barclays to help verify your identity online
14 Apr 2016, 10:00 BST

TRANSFORMING BARCLAYS
Further Non-Core disposal
07 Apr 2016, 08:00 BST

CONTRIBUTING TO GROWTH
Barclays publishes lending data across UK postcodes
01 Apr 2016, 10:00 BST

Responsibilities





T H A N K
Y O U

Contact Details

*Detective Inspector Michael Gubbins
Computer Crime Investigation Unit,
Garda Bureau of Fraud Investigation,
Harcourt Street,
Dublin 2*

Tel: +353 1 6663708

Email: michael.p.gubbins@garda.ie



Society of Actuaries in Ireland

ERM Forum Hot Topics

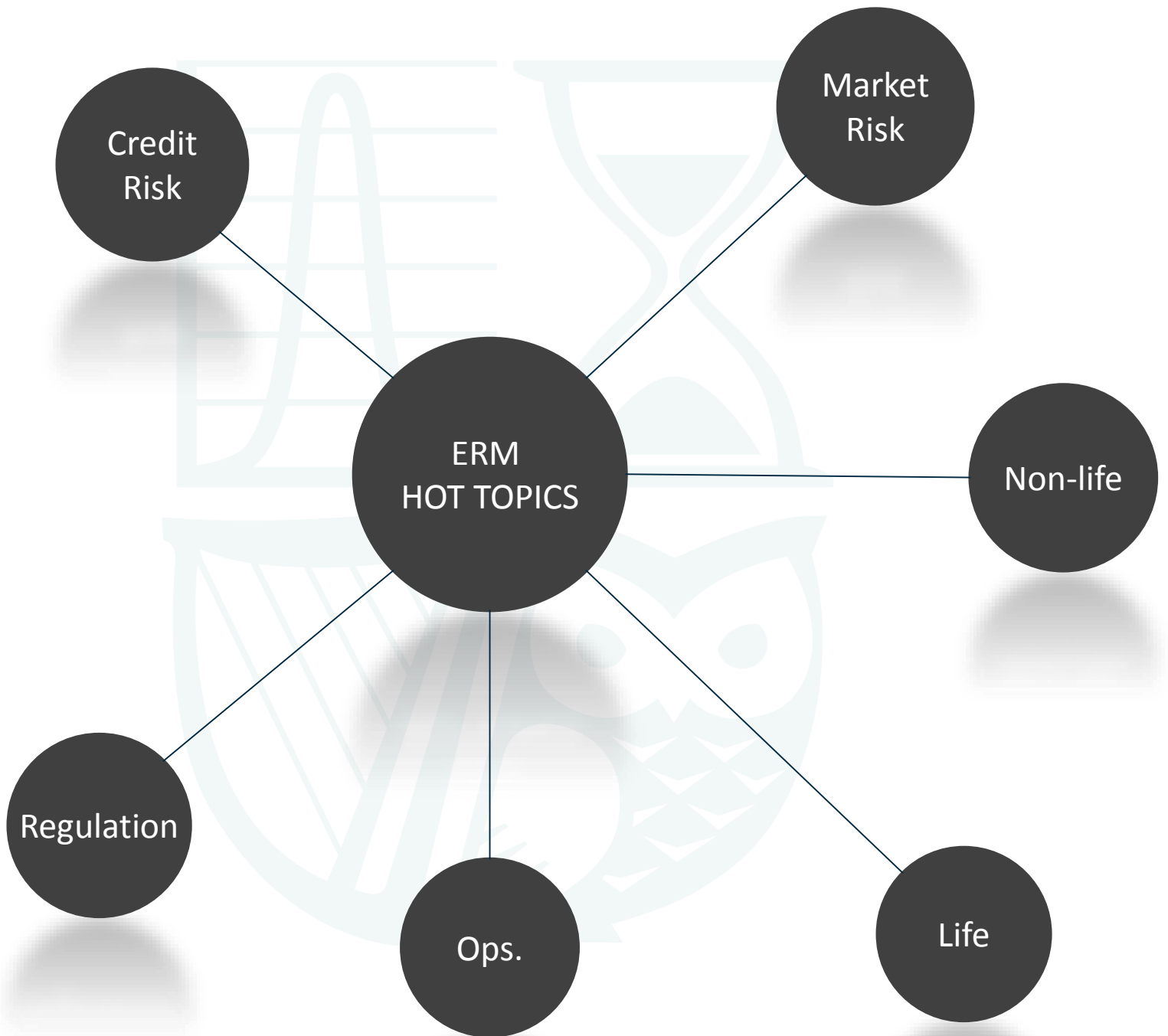
10 May 2016

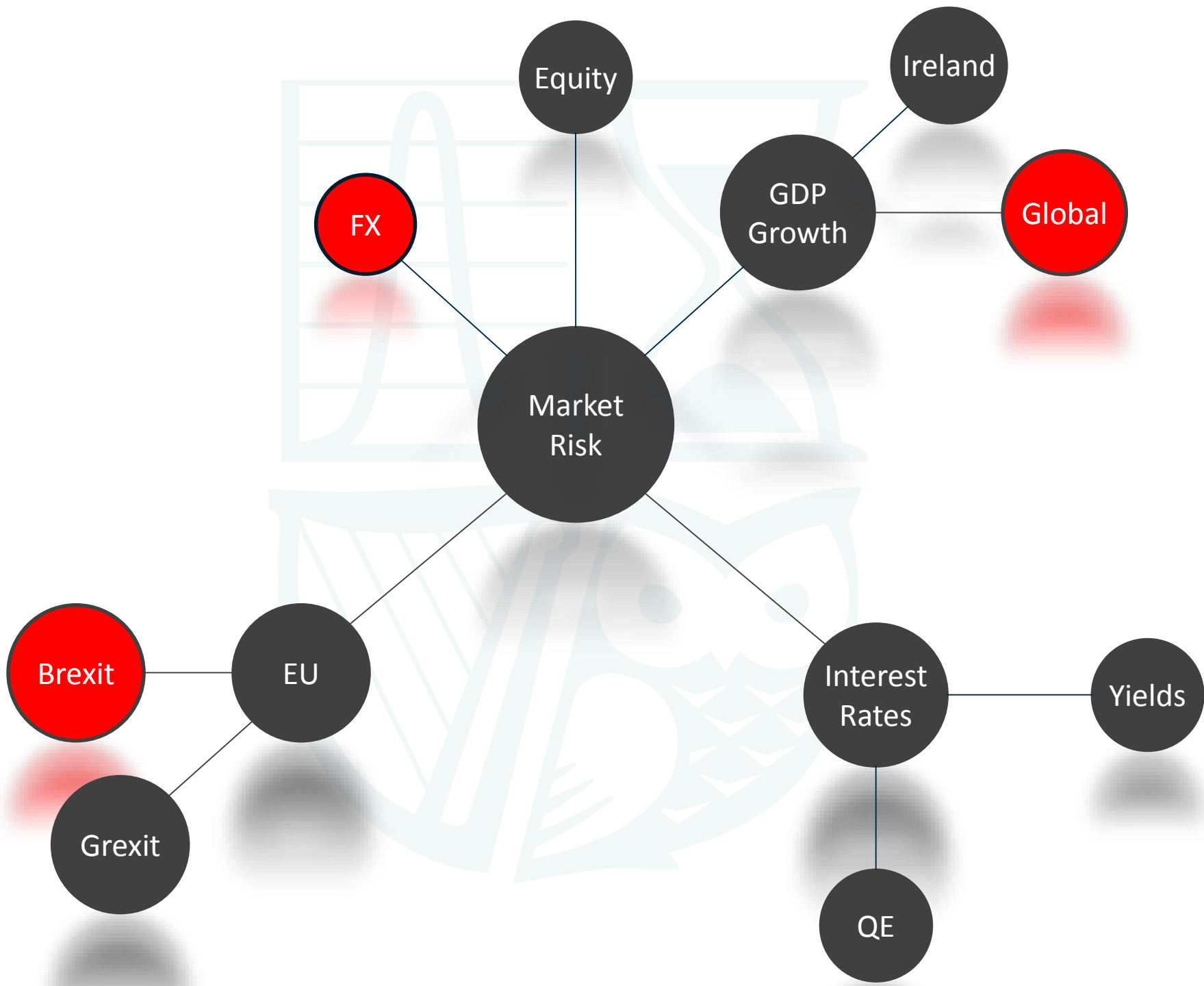
Agenda

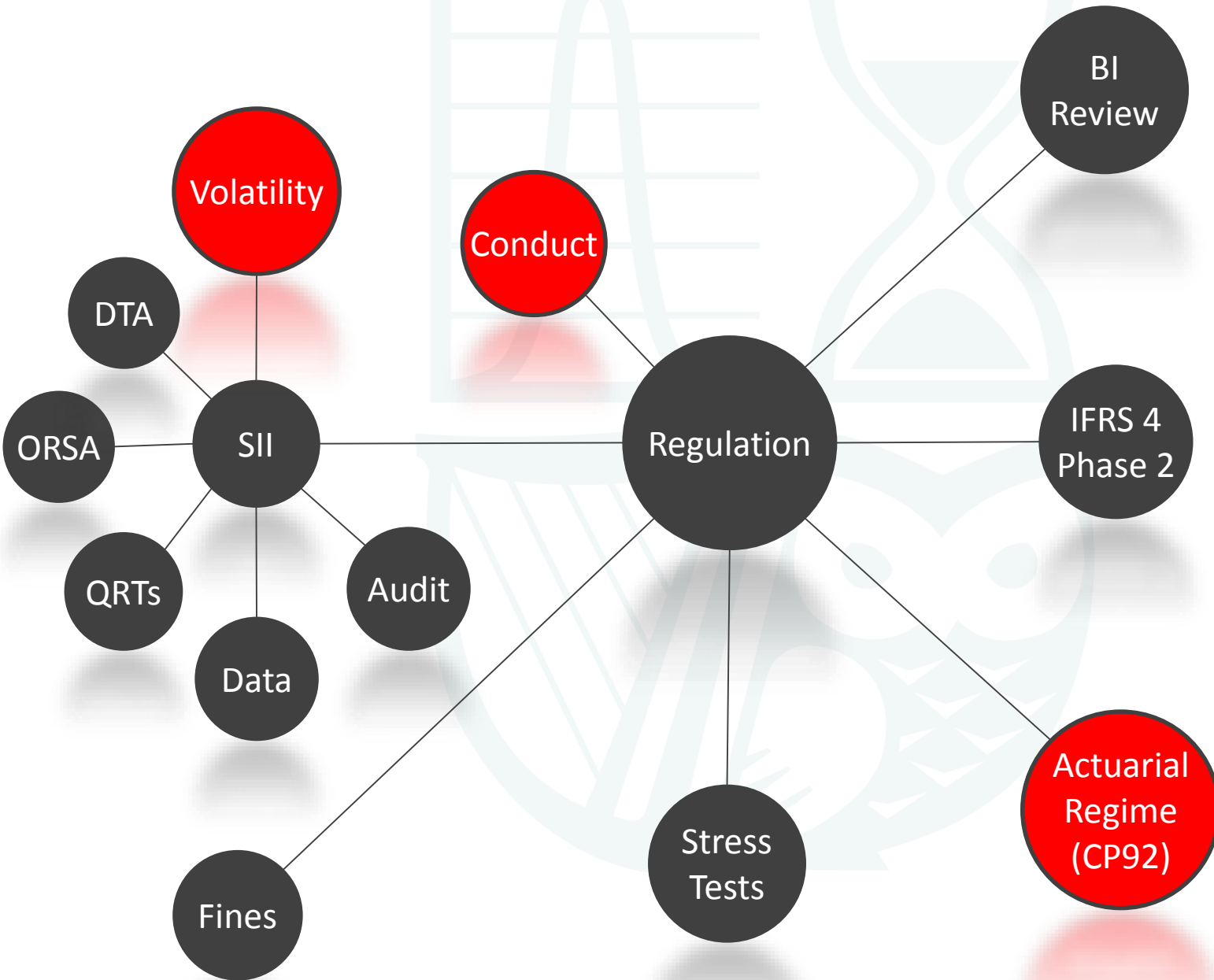
- Current Hot Topics in ERM
- Updated from September 2015
- Interactive Q&A

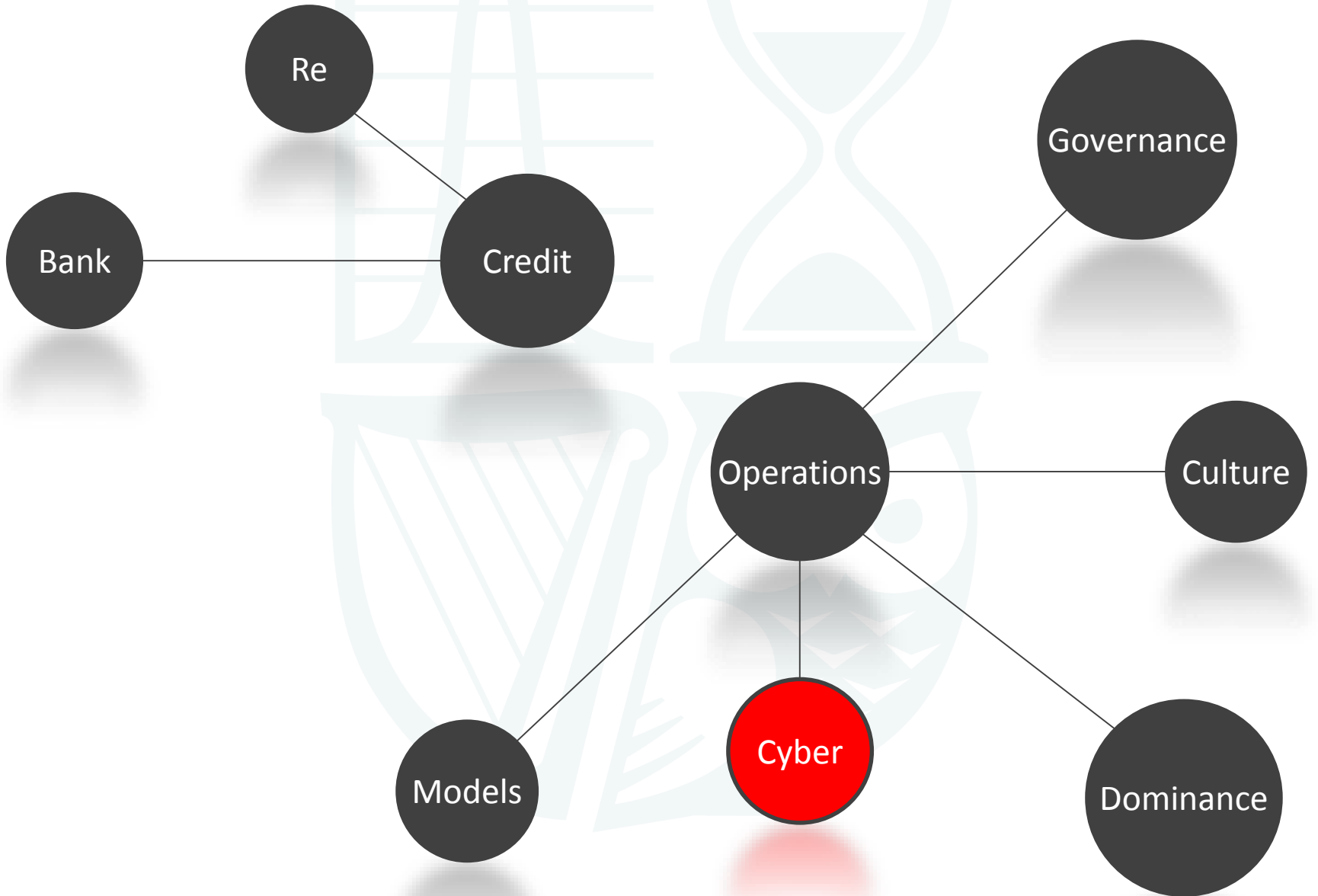
Disclaimer:

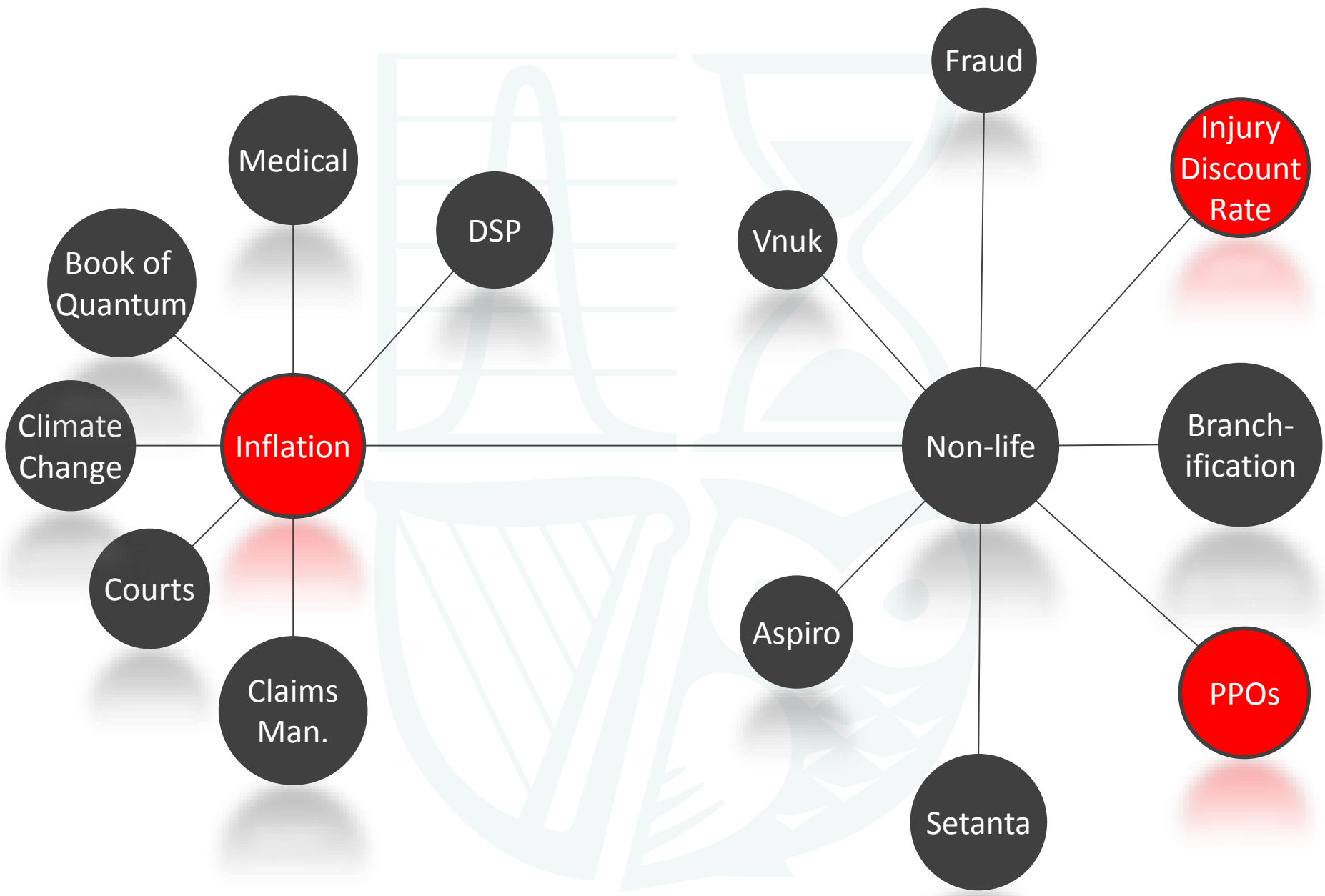
***The material, content and views in the following presentation
are the personal views of the presenter.***

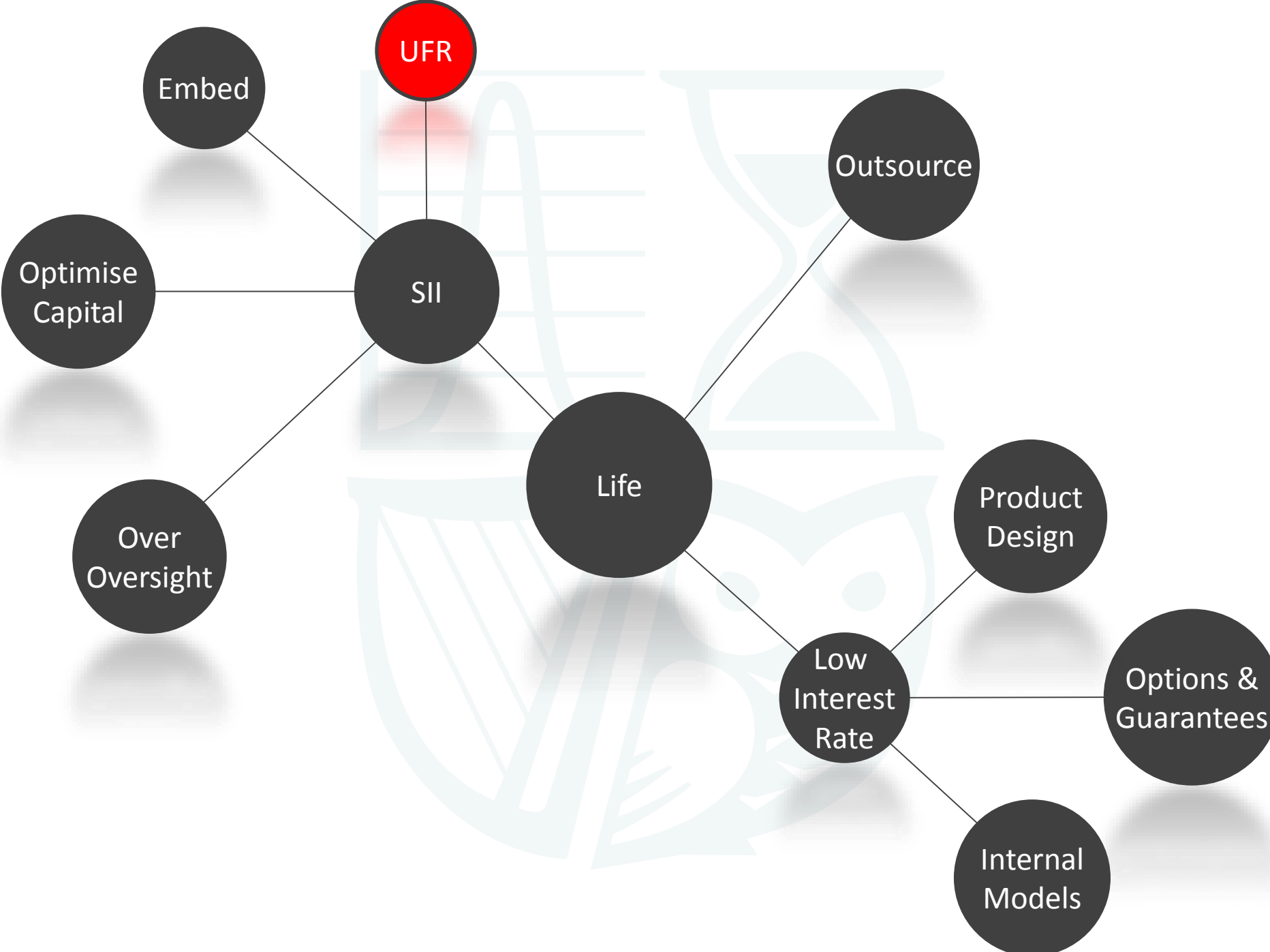












Hot Topics Across All Disciplines?

Brexit

Investment Yields

SII Balance Sheet Volatility

“Branchification”

Over-oversight

Profitability

Disclaimer:

The material, content and views in the following presentation are those of the presenter(s).