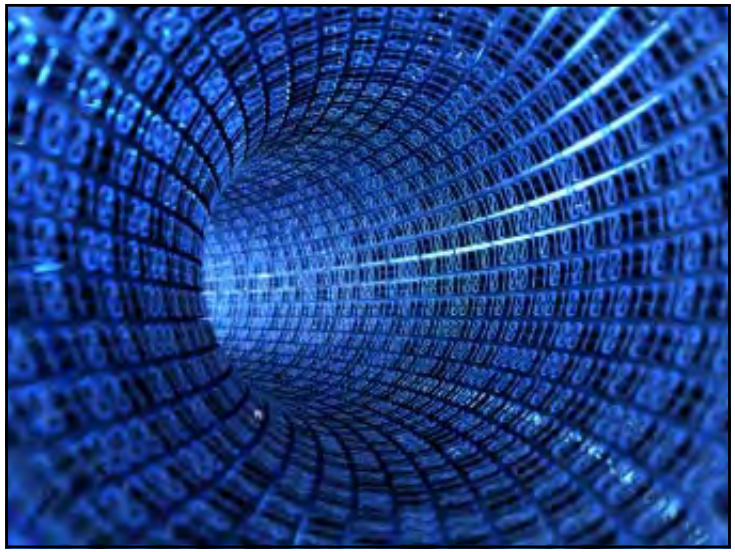
CURRENT & FUTURE CYBER RISKS TO IRISH CREDIT UNIONS

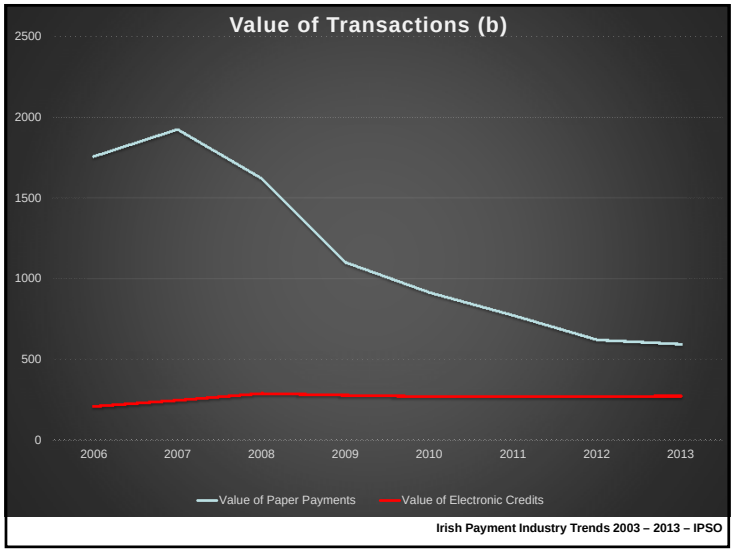
BH Consulting

Who Am I?

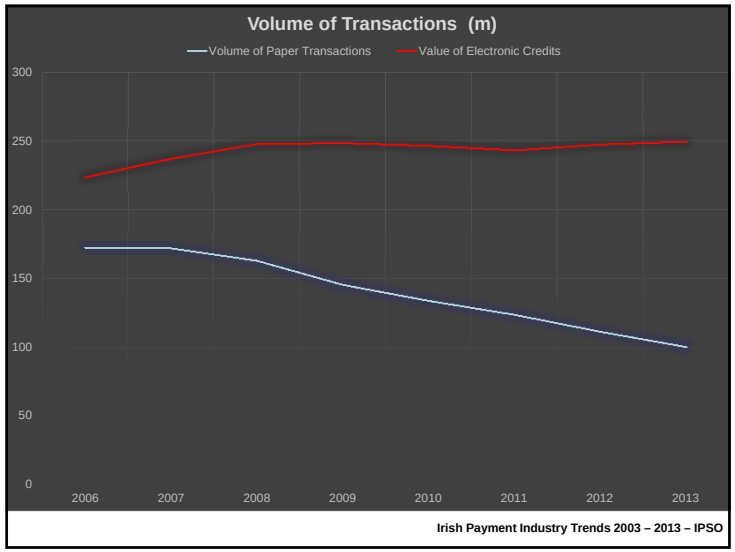
- CEO of BH Consulting – Independent Information Security Firm
- Founder & Head of IRISSCERT – Ireland's first Computer Emergency Response Team
- Special Advisor on Internet Security Europol's CyberCrime Centre (EC3)
- Adjunct Lecturer at University College Dublin
- Expert Advisor to European Network & Information Security Agency (ENISA)
- Regularly comments on media stories –
  - BBC, Forbes, Bloomberg, FT, Guardian, Sunday Times

Background





Irish Payment Industry Trends 2003 – 2013 – IPSO



Irish Payment Industry Trends 2003 – 2013 – IPSO

The likelihood of a "**high-impact event"** to the global financial system has increased over the last six months

Over 60% of risk managers at financial services frim believe there is an increased probability for a "high-impact event" in the next **12 months**

Regulatory Drivers

- Central Bank of Ireland
- European Central Bank (ECB)
- European Banking Authority (EBA)
  - Payment Services Directive (PSD2)
- Payment Card Industry – Data Security Standard
- Irish National Cybersecurity Strategy
- EU General Data Protection Regulation
- EU Network & Information Security Directive

Central Bank of Ireland

*"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"*

And that:

*"an ethos of **effective corporate governance**, coupled with appropriate **I.T. and cyber-security risk management**, can be the foundation of successful protection against cyber-crime. The board should develop a **culture of security and resilience** throughout the firm and ensure that the firm has the necessary **plans in place to deal with both internal and external cybersecurity breaches**".*

"Review of the management of operational risk around cyber-security within the Investment Firm and Fund Services Industry" - September 2015.

Central Bank of Ireland

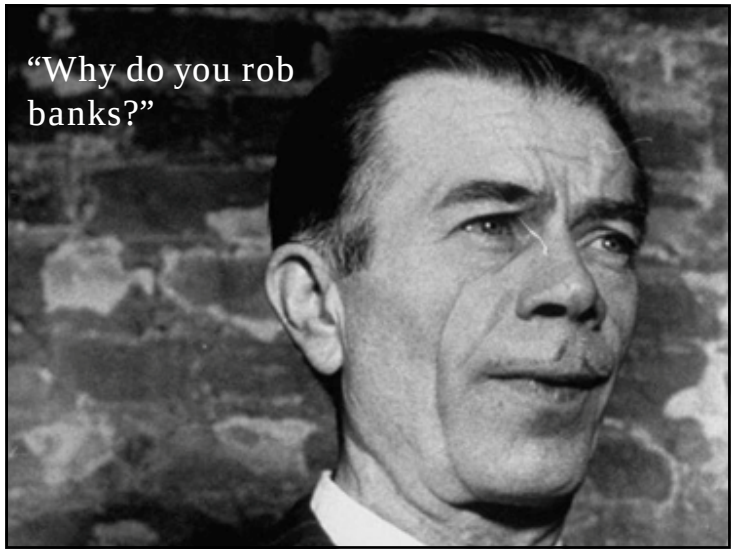
"We do acknowledge that an effective cybersecurity programme should be reflective of the size, business model, nature and sensitivity of the firm's critical assets. That being said, there are a number of common themes that are pertinent to most or all firms:

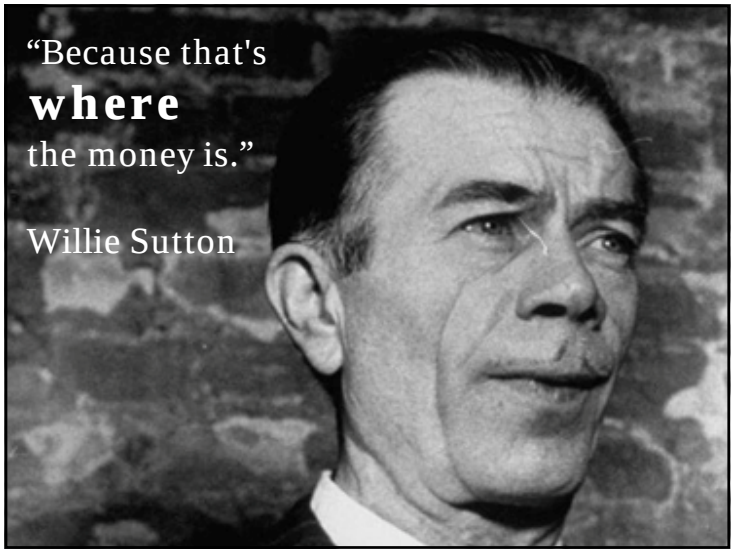
- **The Board should have a good understanding of the main risks:**
- **Perform risk assessments and intrusion tests:**
- **Prepare for the successful attacks**:
- **Manage vendor risk:**
- **Gather information and follow best practices:**
- **Educate staff:**
- **Robust IT policies, procedures and technical controls are put in place:**
- **Consider buying cyber-insurance:**

Deputy Governor Central Bank of Ireland, Cyril Roux, to the Society of Actuaries in Ireland Risk Management Conference in September 2015.

Major Issues/Concerns

- DDoS Extortion
- Ransomware
- CEO Fraud





BBC Sign in | News | Sport | Weather | Shop | Earth | Travel | More | Search

NEWS

Home | Video | World | UK | Business | Tech | Science | Magazine | Entertainment & Arts | Health | World News TV | More

Business | Market Data | Markets | Economy | Companies | Entrepreneurship | Technology of Business | More

European Central Bank website hacked

24 July 2014 | Business

A hacker demanded money for stolen data, but the bank said no internal systems were hacked.

Top Stories

Ninety given French problem trial drug
4 hours ago

Switzerland defends migrant assets law
7 hours ago

UK's Peake on historic spacewalk
5 hours ago

Features & Analysis

Belgian bank Crelan loses €70 million to BEC scammers

Belgian bank Crelan has become a victim of fraudsters. According to a statement (in Dutch) published last week, the bank has lost over 70 million euros (around $75,8 million).

Garda probe as hackers fool the Central Bank into transferring money to bogus online account

Central Bank has confirmed that up to €32,000 is still missing

Hackers steal £650 million in world's biggest bank raid

Investigators uncover what is thought to be the biggest ever cybercrime with more than £650 million going missing from banks around the world

DDoS Strikes Take EU Banks Offline

Experts Say Outages Not Linked to U.S. Attacks

ATM Fraud Allowed Thieves To Steal $45 Million In Hours

Qatar National Bank: Database leak gives data on al-Jazeera journalists and British 'spies'

By Jason Murdock
April 26, 2016 11:46 BST | Updated 4 hr ago

Spelling mistake prevented hackers taking $1bn in bank heist

New York Fed reveals spelling of 'foundation' as 'fandation' prompted bank to seek clarification and stop transfer, but hackers still got away with about $80m

The hackers breached Bangladesh Bank's systems and stole its credentials for payment transfers, two senior officials said. Photograph: Alamy Stock Photo

Spelling mistake prevented hackers taking $1bn in bank heist

New York Fed reveals spelling of 'foundation' as 'fandation' prompted bank to seek clarification and stop transfer, but hackers still got away with about $80m

Billion dollar Bangladesh hack: SWIFT software hacked, no firewalls, $10 switches

The Bangladesh Bank's internal network security was sorely lacking.

Bangladesh Bank hackers compromised SWIFT software, warning issued

How To Defend

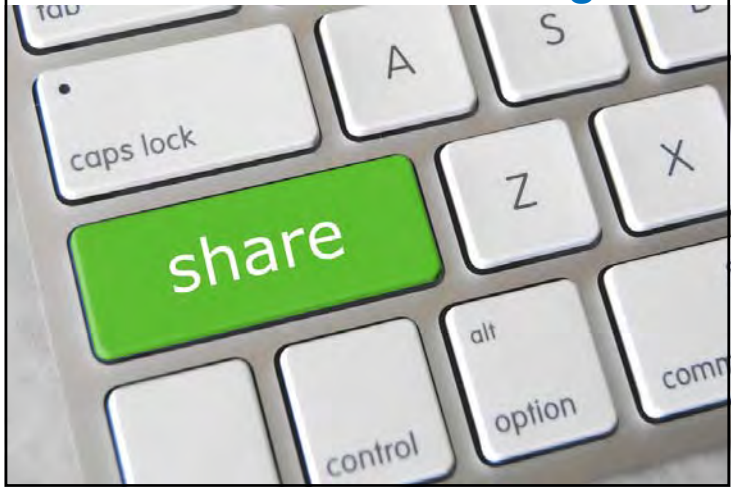
Identify & Value Key Assets

Establish Policies

Security Awareness Training

Monitor & Respond

Information Sharing



@BrianHonan
Brian.honan@bhconsulting.ie
www.bhconsulting.ie