

# ***Cyber Security***

*Digital world risk that cannot be ignored*

May  
2016



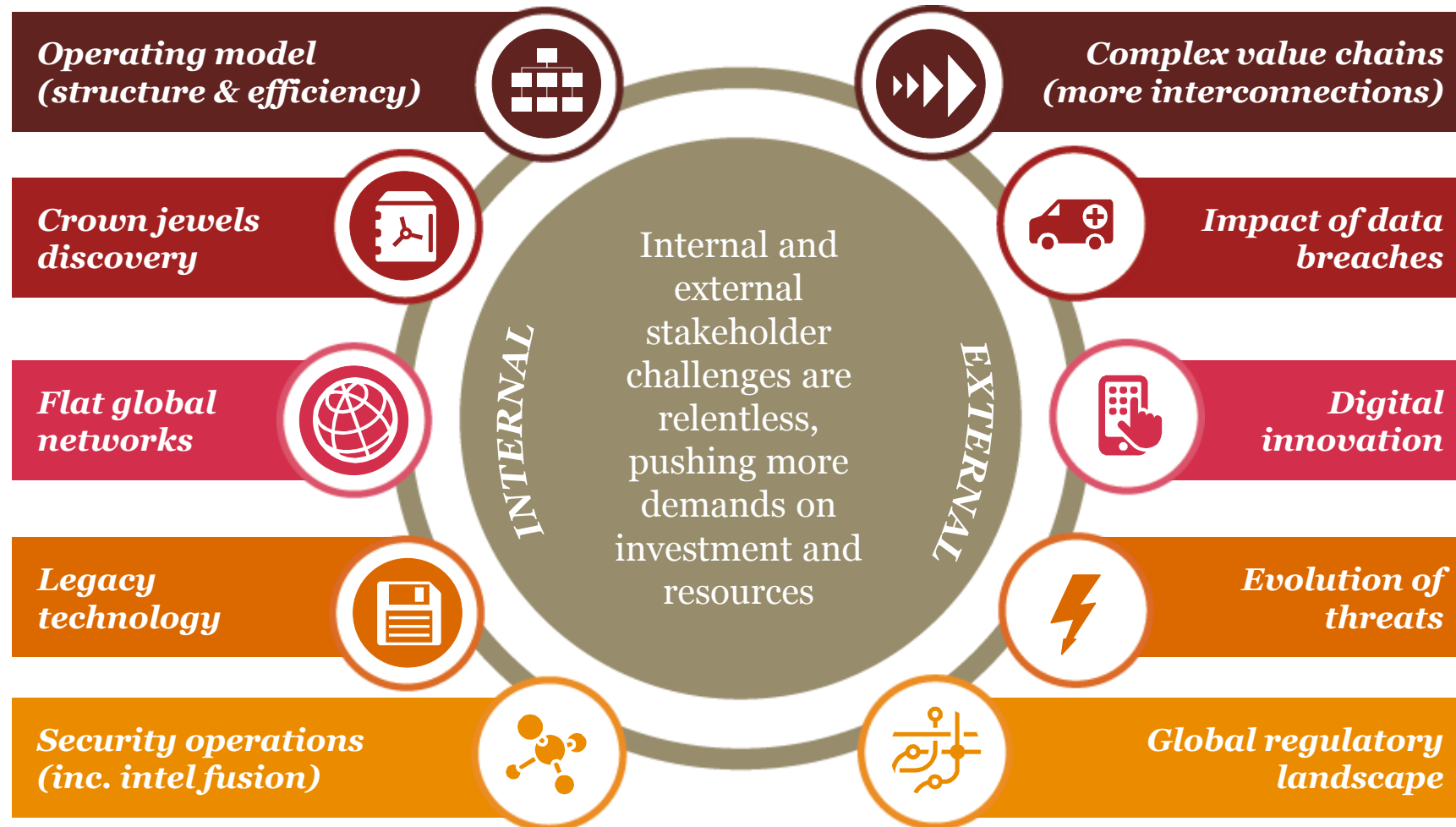
***Matt Hawley***

## Cyber security context

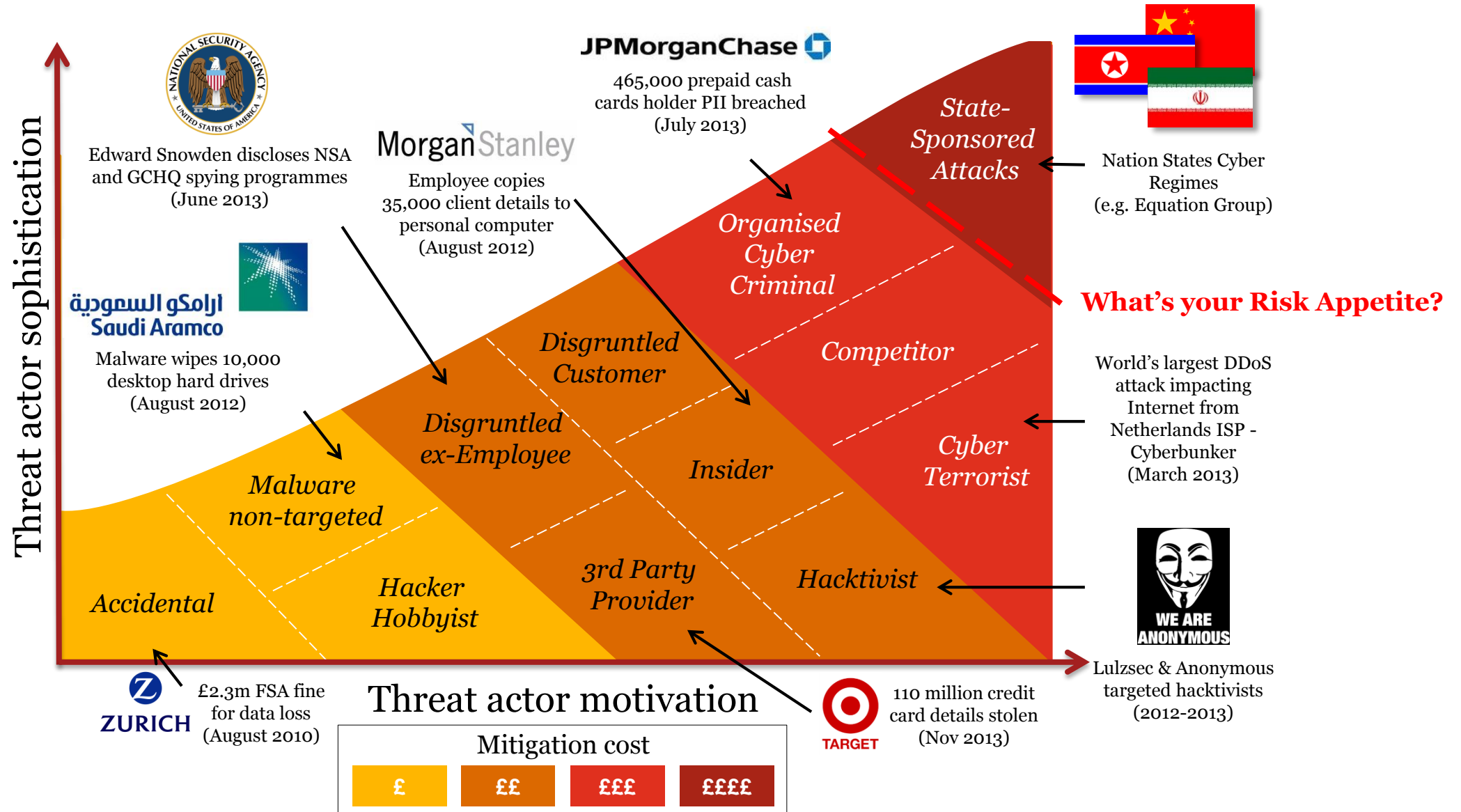


# Cyber security context for Financial Services

Increasing balance between internal and external challenges, threats and demands





















# Threats are rapidly increasing and evolving



# What are the threats in Financial Services and how easy are they to mitigate?

Some threats require industry collaboration to effectively mitigate, and some require government intervention

Key cyber threat scenario	 Direct Compromise of internet accessible systems	 Denial of service attacks on Internet accessible systems	 Breach of physical and/or logical boundary (e.g. branch / supplier)	 Leak of sensitive information by trusted insider	 Compromise of endpoint security through malware infection	 Online fraud directly targeting customers	 Financial system risk, market manipulation, insider trading	 Reliance on upstream service providers for Internet services	 Large scale cyber terrorism and cyber warfare
Typical threat actors	Hackers, hacktivists, chancers	Hackers, hacktivists	Organised criminals, nation states	Employees, third party delivery partners	Organised criminals, nation states	Organised criminals	Insiders, competitors	Nation states, organised criminals	Nation states
Primary Motivations	Fun, political agenda	Fun, political agenda	Financial gain, espionage	Revenge, accidental, whistleblowing	Financial gain, espionage	Financial gain, identity theft	Financial gain	Various	Geo-political agenda
Ability to mitigate	High	High	Medium	Medium	Medium	Medium	Low	Negligible	Negligible
Recent example	 In August 2015, Carphone Warehouse suffered a security breach of their website, resulting in the encrypted card details of up to 90,000 customers being accessed.	 In July 2015, RBS was hit by a DDoS attack meaning the customers could not access online banking facilities for around an hour.	 In 2014, a fraudster was tried for remotely controlling a computer in a Barclays branch to carry out a number of fraudulent transactions.	 A HSBC insider handed sensitive files about high net worth individuals to French authorities, triggering a number of tax evasion investigations	 Sony was the victim a targeted email phishing campaign resulting in the compromise of sensitive information and significant reputational damage	 In October 2015, 14 fraudsters were arrested over involvement in a £60 million fraud targeting bank customers leading to significant reputational damage	 In 2014, it was alleged that Goldman Sachs intercepted and acted upon trade requests from other brokers to gain a competitive advantage	 In 2014, the 'heartbleed' vulnerability was made public and showed that many websites were vulnerable as the result of an insecure cryptography standard	 Stuxnet malware is believed to have been developed by the US and Israeli as a cyber weapon to sabotage Iran's nuclear program

# ***What's the impact of a cyber attack?***

Consider the impacts of fraud and espionage

## **Direct Costs**

### ***Investigation & Remediation***

*£ms in 3<sup>rd</sup> party specialist fees*

### ***Regulatory Sanction***

*4% of global revenue for GDPR breaches*

### ***Customer Redress***

*Anthem spent ~\$100m on customer redress campaign*

## **Indirect Costs**

### ***Increased Cyber Insurance Premium***

*3x increase for hacked organisations*

### ***Customer Fraud***

*Banks underwrite £ms/week of losses*

### ***Class Action Law Suit***

*47k staff sue Sony for stolen data*

## **Intangible Costs**

### ***Damage to Brand***

*Harder to attract new customers*

### ***Heads Roll***

*Target CEO and CTO lose their jobs*

### ***Competitive Disadvantage***

*Google close Chinese ops after IP thefts*

# Cyber Security Confidence Areas

To understand the current state of your cyber security programme, we review cyber programme using the Cyber Governance Health Check six cyber confidences as the foundation. The confidences cover the key areas we believe are necessary to proactively manage and protect a business to ensure it is fit for the cyber and digital world in which we operate





## *What does this mean for Financial Services Industry- Example AWM?*

*The Board must be “cyber confident”*

*Visibility of risk*

*Ownership of risk*



*Cyber risk must be managed across the whole value chain*

*Financial Advisors*

*Fund Managers*

*Custodian*

*Administrators*

*Crown Jewels?*

- *Investor personal data*
- *Investment strategies*

*Cyber Threats?*

- *Data sold on black market*
- *Fraudulent transactions*

*Vulnerabilities?*

- *Poor investor ID&V*
- *Lack of data encryption*



*Maintain the trust of your customers and the regulator*



---

## *How are we helping our clients?*

### **Client Trigger**

### **Our Service**

### **Outcome**

*I've been breached!*

***Breach Aid***  
*Respond, investigate & remediate*

***Damage  
Limitation***

*Am I secure?*

***Security Assurance***  
*Assess, test & exercise*

***Confidence***

*How to best protect  
myself?*

***Security Transformation***  
*Plan, design & build*

***Return on  
Investment***

**Matt Hawley**

matthew.hawley@uk.pwc.com

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers LLP, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2015 PricewaterhouseCoopers LLP. All rights reserved. In this document, “PwC” refers to PricewaterhouseCoopers LLP (a limited liability partnership in the United Kingdom) which is a member firm of PricewaterhouseCoopers International Limited, each member firm of which is a separate legal entity.

