COMMERCIAL BANKING

CYBER THREATS
CYBER-ENABLED FRAUD
AWARENESS AND GUIDANCE

Tim Wiseman

Commercial Banking, Data Services

5th June 2017

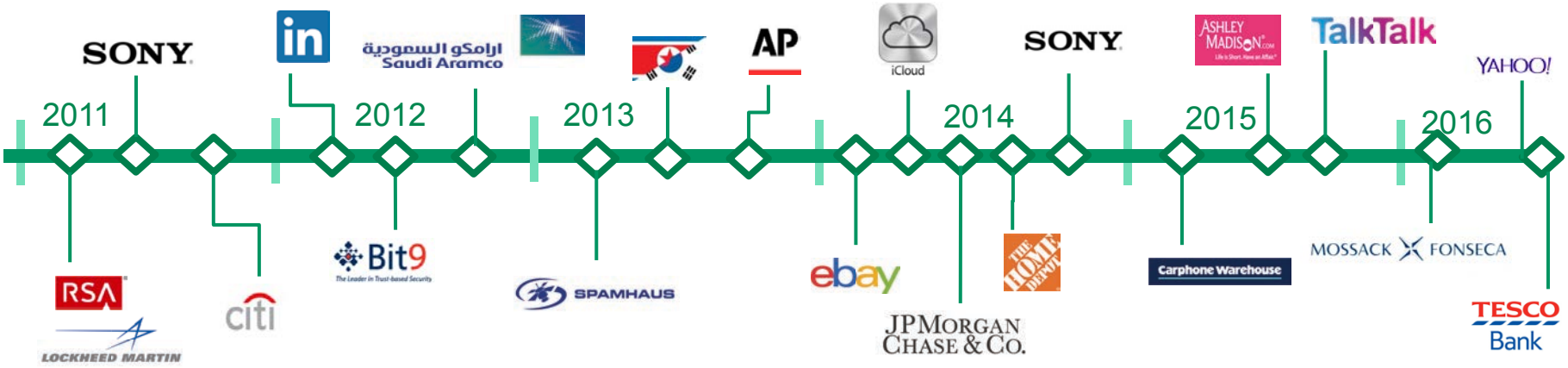
LLOYDS BANK

OVERVIEW

- A definition of Cyber, a background on the threat (who? what? how?) some examples, some thoughts around how to manage the risk.
- Cyber-enabled Fraud threats to your business, advice and guidance on prevention.
- The Cyber Security Landscape.
- Questions and Answers: please hold for the end.

BLACK SWAN EVENT?

"Event or occurrence that deviates beyond what is normally expected of a situation and that would be extremely difficult to predict."



"Cyber security breaches have a direct impact on the organisations affected, including lost staff time dealing with the breach and disruption to other work. As a result businesses incur financial losses with the average direct costs of a breach estimated at £36,000 for large businesses and £3,100 for micro/small businesses. The most costly single breach identified in the Cyber Security Breaches Survey was £3,000,000."

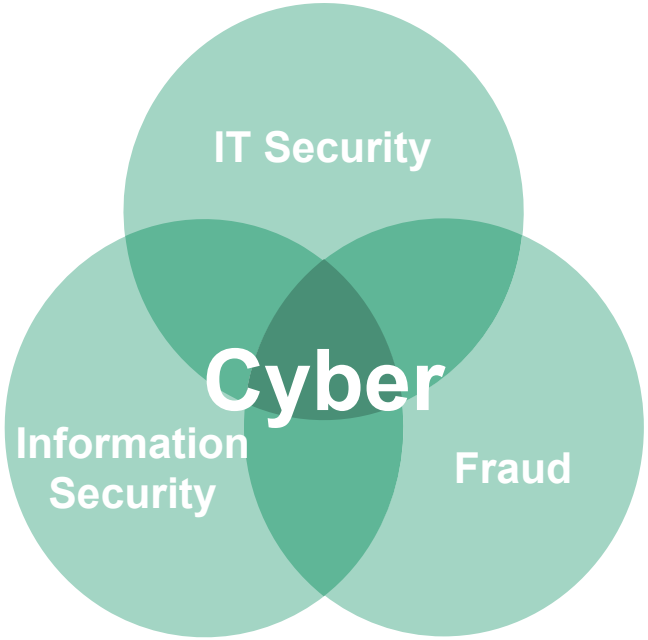
HM Government's Cyber Security Regulation and Incentives Review – December 2016

65% of large firms detected a cyber breach or attack in the past year."

Dept. of Culture, Media & Sport – 2016

WHAT IS CYBER?

- Cyber attacks affect people, processes and technology
- Cyber risks are business problems
- Cyber is typically concerned with **external threats** and encompasses a variety of factors. Key factors are:
  - Actors
  - Motivations
  - Attacks



Confidentiality | **Integrity** | **Availability** | **Market Manipulation** | **Supplier** | **Customer**

WHAT ARE THE TYPES OF ATTACK?

Attacks can be broken down into categories based on their effects

Confidentiality

Enables the unauthorized use or disclosure of information, that should only be accessible to approved individuals.

Integrity

Compromises the accuracy and completeness of information and processing methods, and allows unauthorised modifications to be made to data.

Availability

Denies access to systems and data to authorised users when they require it.

Attempting to artificially control the market through various means e.g. spreading misleading information about a company.

Market Manipulation

Indirectly attacking a company's network by targeting the vulnerabilities in a suppliers systems and tunnelling in via this route.

Supplier

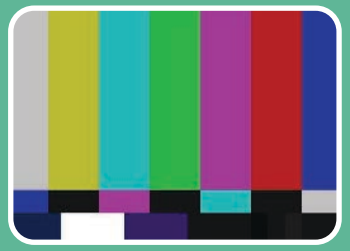
Attacking a customer's systems such that when they try to connect to another system it sees they are infected and blocks them.

Customer

HOW CYBER RISK DIFFERS

In the event of a fire, flood or other physical event:

- Passive adversary
- Target perceived as victim
- Impacts well understood
- Risks bounded to the physical location



In the event of a technical failure:

- Passive adversary
- Impacts usually well understood / root cause secondary concern
- Risks often bounded

In the event of a cyber attack:

- Active adversary
- Target may be seen as negligent
- Impact is not well understood and may dramatically shift
- Cyber may behave more akin to a pandemic outbreak
- Increased customer concern due to potential additional impacts e.g. monetary losses / data theft
- Loss of confidentiality: could lead to large fines under new EU GDPR (up to 4% of global turnover)
- Cyber is not bounded by physical locations

HOW DO ATTACKS HAPPEN?

Most attacks start with hackers using LinkedIn and Facebook as a research tool

Cyber Campaigns	• Planned, in progress or executed attacks by individuals or organisations of Cyber criminals. e.g. Anonymous, 3xp1r3 Cyber Army, & Iran Security Team.
Spear Phishing	• E-mail spoofing fraud attempt that targets a specific person, pretending to be from a known individual or business but is actually a malicious attacker. Capitalises on the human element of systems.
Zero Day Vulnerabilities	• A zero day vulnerability refers to a hole in software that is unknown to the vendor. This security hole is then exploited by hackers before the vendor becomes aware and hurries to fix it—this exploit is called a zero day attack.
Malware	• Malicious software, generally concealing its presence, that contains references to a company's domain name or IP addresses.
Hacking Tools	• Basic free easily available software such as Nmap probe servers for open and vulnerable ports or Wireshark which lets hackers sniff traffic over networks.
Commoditisation of Hacking	• Hacking tools can be purchased easily online through sites on the dark web such as Silk Road, sometimes called the eBay of hacking services.

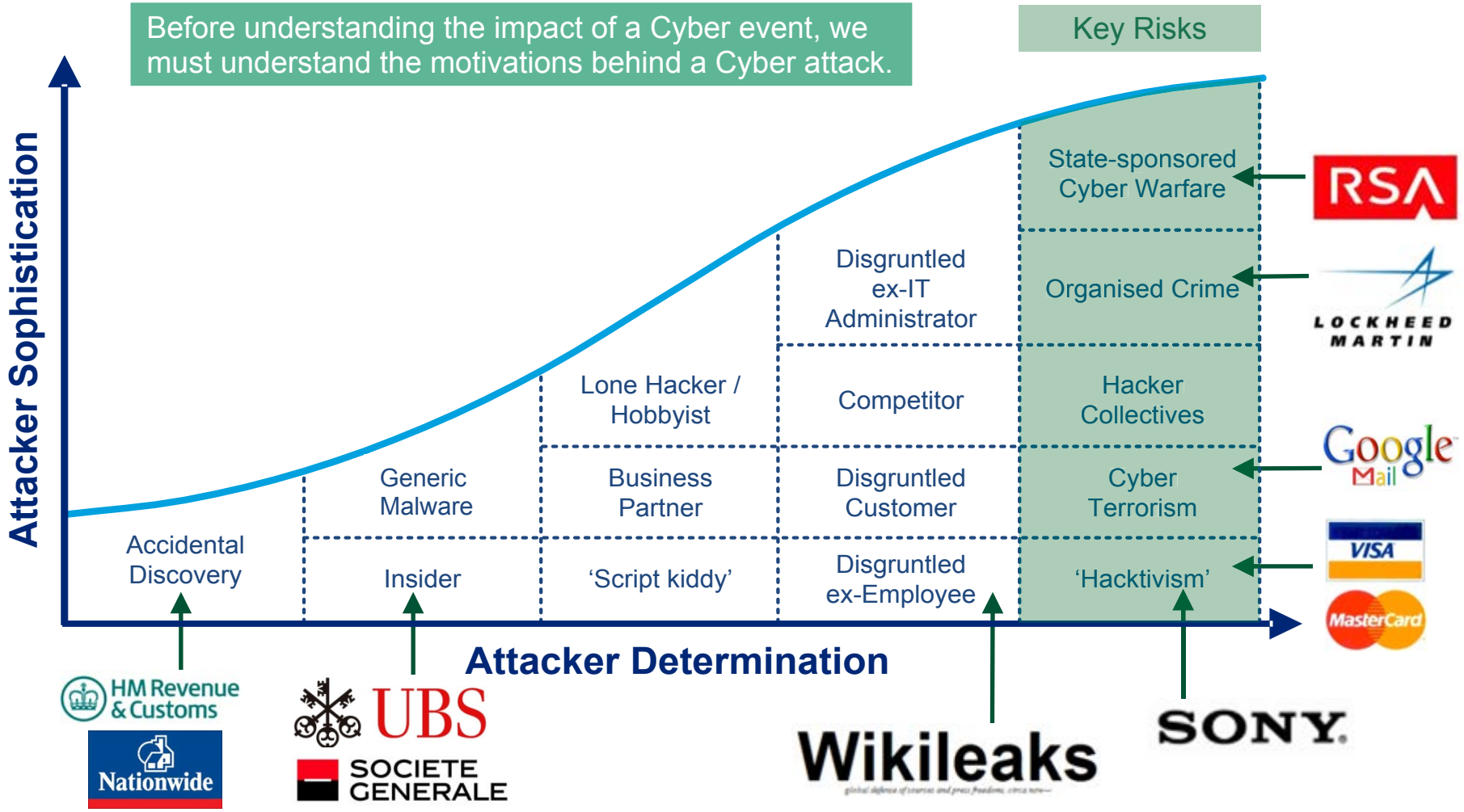
WHO ARE THE ATTACKERS?

Threat Actor	Capability	Primary Objective
Organised Criminal Groups (OCG)	High	Russian-speaking crime groups remain a primary threat. These OCGs seek to extract financial and personally identifiable information for **financial gain.** e.g. JP Morgan Chase, US Data Breaches
Nation States/ State Sponsored	Very High	The main motivation is for political and espionage gains and to commit network **disruption** and **capture valuable data** such as intellectual property. *e.g. Sony Hack, Syrian Electronic Army DDOS attacks on US Banks, People's Republic of China espionage for sensitive IP of companies and customers.*
Hacktivists	Medium	Ideologically motivated by a range of issues and aim to cause maximum **damage** and **embarrassment,** they have captured media attention and favoured techniques include Denial Of Service**.** *e.g. Anonymous, Lizard Squad*
Emerging Cyber Activism affiliated to Terrorism	Low	Emerging activity from Hacktivist Groups, claiming to be terrorist affiliated. No confirmed attribution to IS – current focus of Terrorist groups still remains on **acquiring weapons**, and any cyber defacement is linked to ideological propaganda and media attention.

WHY DO THREAT ACTORS ATTACK?

Threat actors; their capabilities and determination.

Before understanding the impact of a Cyber event, we must understand the motivations behind a Cyber attack.



AVAILABILITY ATTACK

Ransomware (Cryptolocker)

What is Ransomware?

Ransomware is a type of malware that encrypts a user's data or system and refuses to decrypt it until that user pays a ransom.

How are users infected?

Victims often receive emails purporting to be from someone else with a file attached that when opened runs malicious code, installing the software onto the victims computer.

What does it do?

The attack usually places a time limit on when the ransom must be paid otherwise the encryption key will be deleted and the data lost forever.

How popular is it?

Security vendor McAfee released data showing that in 2013 it had found over 250,000 unique samples of ransomware. Ransomware is one of the most common tools of Cyber criminals, recently seen in February 2016 attack on Hollywood Presbyterian Medical Centre.

AVAILABILITY ATTACK

Distributed Denial of Service (DDoS)

What is a DoS attack?

A Denial of Service attack traditionally attacks a network by flooding it with useless traffic and is designed to prevent legitimate access and service, however there are also many other emerging methods with the same results.

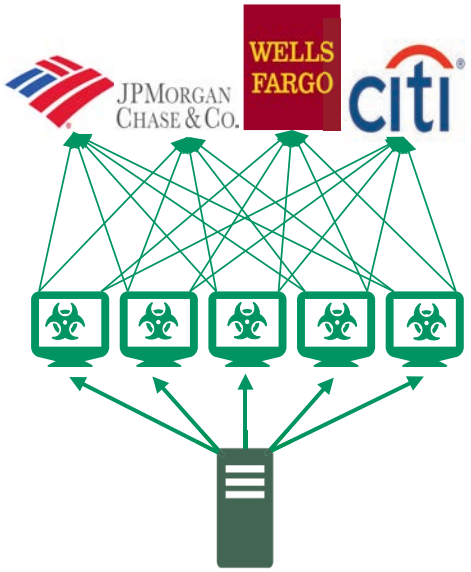
What is a DDoS?

DDoS is when multiple compromised systems, often infected with a Trojan, are used to target a single system to deny legitimate users service.

What is a Botnet?

An infected computer is known as a bot and when these are linked together for a DDoS attack they are collectively called a botnet, or sometimes a zombie army.

In 2012 a group of major American banks had their websites taken down after being hit by one of the largest DDoS attacks in history.



SUPPLIER ATTACK

Target – Third Party Vulnerability

What?

Hackers managed to gather 40 million card details and 70 million personal records of customers. This included names, phone numbers, email and mailing addresses.

How?

Initial intrusion into its systems traced back to network credentials stolen from a third party vendor. The attackers then pushed malware through the system onto point of sale devices.

Why?

Either to use or sell the personal details for monetary gain.

TARGET®

KEY CONSIDERATIONS WHEN MANAGING RISK

IT Services	Business Protection	Governance	Total Failure Planning	Third Party Security	Customer Security
					
What services do critical business processes rely on? How many people need access to these services? What is the time criticality of key services?	How can we confirm the integrity of the data our processes rely on? What alternate systems and processes can be put in place for minimal operation?	What prep do our senior managers need? Do we have a comms. plan ready for a critical incident?	Which records are critical for business reconstruction? Do we run regular test exercises for a critical incident?	What systems and/or data do we and should we share? How do we entrust our sensitive recovery records?	What critical reliance does the customer have on us? Do we know our key customers? Do we have alternative channels to reach key customers in the event of a critical incident?