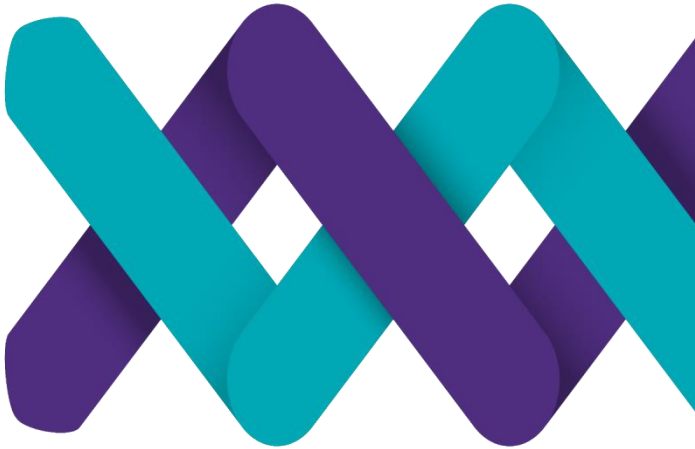
Grant Thornton

An instinct for growth™

Cyber security and cyber resilience

Protecting yourself and your business



THE PROFILE OF A CYBER CRIMINAL

8.1 MILLION AMERICANS WERE HIT BY IDENTITY THEFT IN 2010

EVERYONE IS A TARGET

BY 2011 THIS NUMBER HAD INCREASED 13 PERCENT TO **11.6 MILLION**

EVERY DAY OVER **1.5 MILLION** WORLDWIDE ARE VICTIM TO CYBERCRIME

65% GLOBAL INTERNET USERS HAVE BEEN VICTIMS OF CYBERCRIME

73% OF AMERICANS HAVE BEEN VICTIMS OF CYBERCRIME (WORLD'S 3RD HIGHEST AVG)

ONLY .0019% OF CYBERCRIMES WERE CONVICTED IN THE US IN 2010

THESE CRIMINALS TEND TO WORK FROM FOREIGN COUNTRIES MAKING THEM DIFFICULT TO IDENTIFY AND HARDER TO CONVICT IF CAUGHT.

WHO ARE THEY?

AGELESS SOCIETY

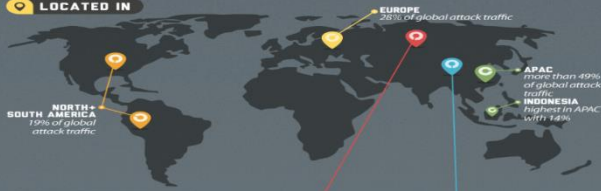
GENDER

WORK IN PACKS

CYBER CRIMINALS WORK IN GROUPS AS PART OF LARGER ORGANIZATIONS

- 25% ACTIVE CYBER CRIMINAL GROUPS HAVE OPERATED FOR 6 MONTHS OR LESS
- 50% CYBER CRIMINAL GROUPS HAVE 6 OR MORE MEMBERS

LOCATED IN



HIGHLY ORGANIZED

FULL-FLEDGED BUSINESSES WITH EXECS, MIDDLE MANAGERS AND WORKERS

UNDERGROUND CHAT ROOMS, WEB PORTALS + MARKETPLACES FOR HIRING HACKERS, BUYING MALWARE + OTHER ILLEGAL INFORMATION ARE SUPPORTING THESE "BUSINESSES"

INVITATION-ONLY, HELP-WANTED PORTALS SPECIFICALLY FOR CYBER CRIMINALS EXIST POST ORIGINATING FROM RUSSIA

HOSTING PROVIDERS ARE KEY TO SUCCESS OF CYBERCRIMINALS WHO NEED SERVERS TO STORE ILLEGAL CODE, MALWARE + STOLEN DATA. MOST OF THESE PROVIDERS ARE IN RUSSIA AND CHINA

WE CAN'T STOP THEM FROM ATTEMPTING THEIR CRIMES

BUT WE CAN STOP THEM FROM GETTING OUR IDENTITIES AND AND PRECIOUS INFORMATION ONLINE

FIGHT BACK

ALWAYS	CAUTION	NEVER
IF BUYING MERCHANDISE OR MAKING A PAYMENT ONLINE, ENSURE IT IS A REPUTABLE, SECURE SOURCE.	BE WARY OF PROVIDING CREDIT CARD INFORMATION THROUGH EMAIL.	NEVER PROVIDE UNKNOWN PROSPECTIVE EMPLOYERS WITH YOUR SOCIAL SECURITY NUMBER.
TRACK YOUR ONLINE CREDIT TRANSACTIONS OFTEN FOR FRAUDULENT ACTIVITY.	BE CAUTIOUS WHEN DEALING WITH INDIVIDUALS FROM OUTSIDE YOUR COUNTRY.	NEVER GIVE YOUR CREDIT CARD # OVER THE PHONE UNLESS YOU MADE THE CALL TO A KNOWN BUSINESS.
SHRED, DON'T THROW AWAY ANY BANK OR CREDIT CARD STATEMENTS.	BE CAUTIOUS WHEN MONEY IS REQUIRED UP FRONT FOR ANY JOB LEAD.	NEVER OPEN OR RESPOND TO SPAM EMAILS.

Grant Thornton | An instinct for growth™

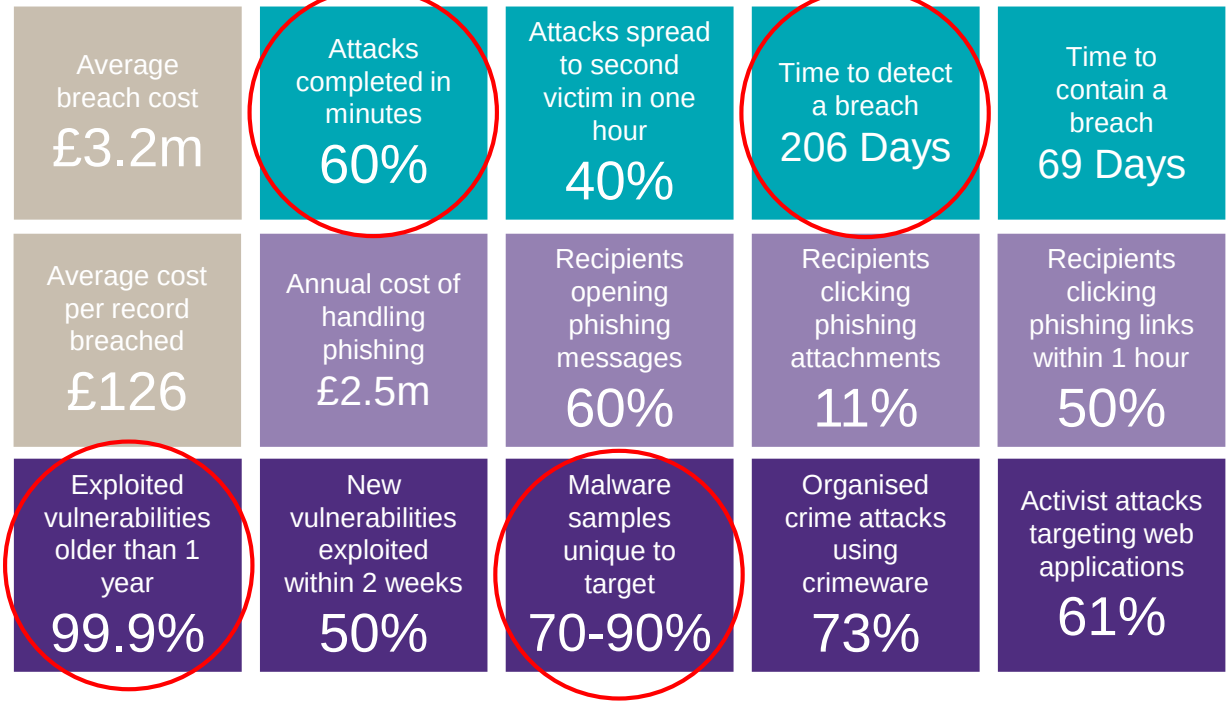
Definition of key terms

Cyber resilience:
‘Cyber resilience is a Financial Market Infrastructure’s ability to anticipate, withstand, contain and rapidly recover from a cyber attack’ **FCA**

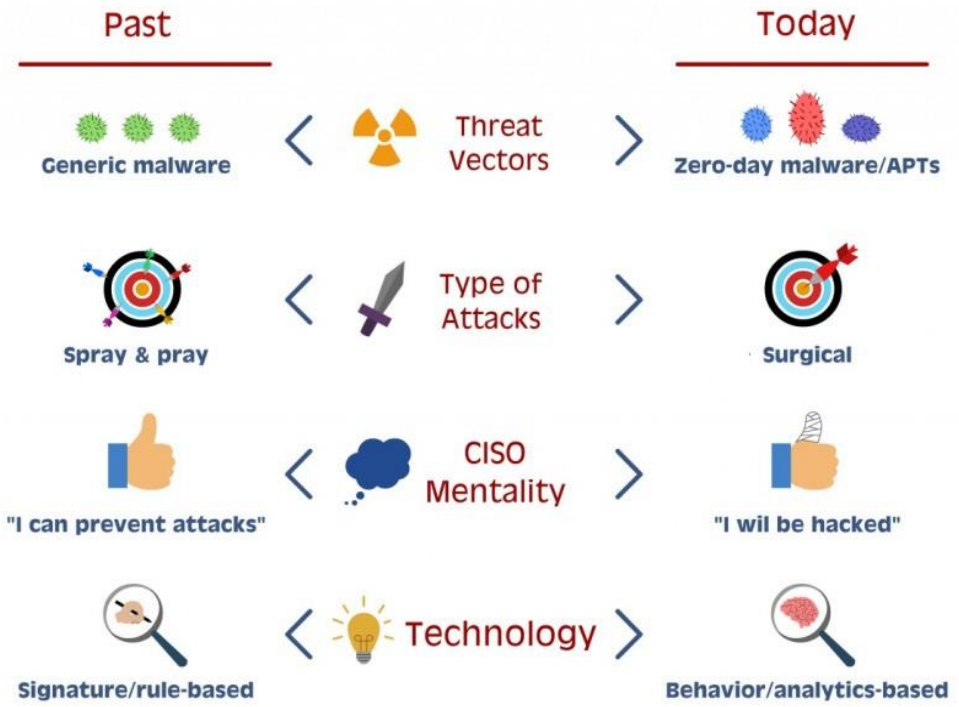
Cybersecurity / Cyberspace security:
‘Preservation of confidentiality, integrity and availability of information in the cyberspace.’ **ISO/IEC 27032:2012 Information Technology**

Cyberspace:
‘Complex environment resulting from the interaction of people, software and services on the internet by means of technology devices and networks connected to it, which does not exist in any physical form.’ **ISO/IEC 27032:2012 Information Technology**

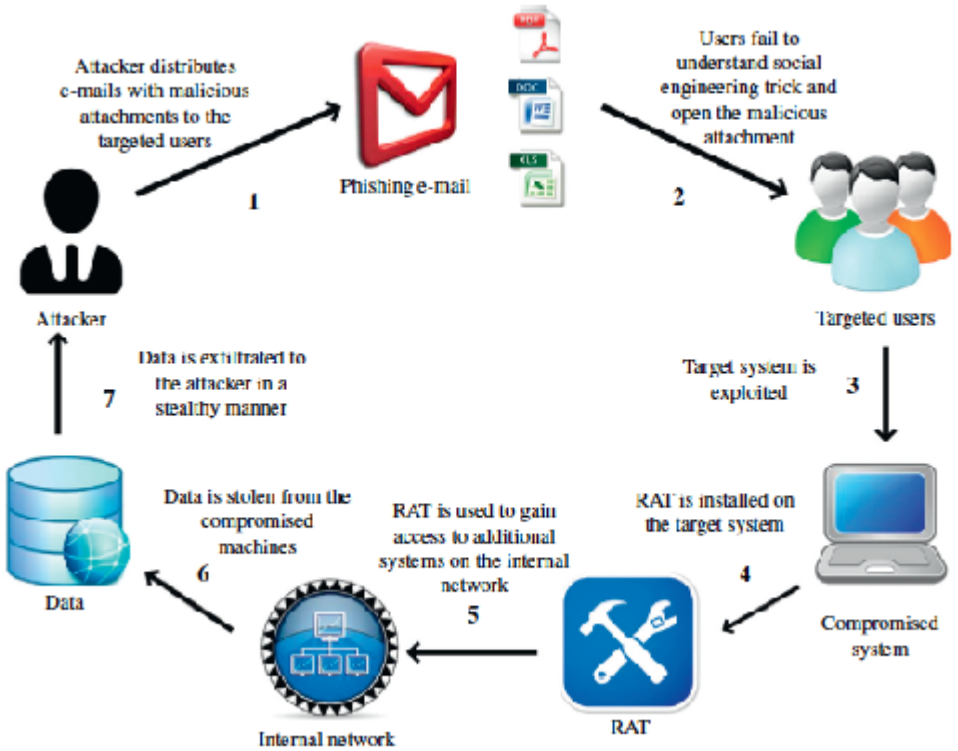
Cyber attacks – Some numbers



Attitude towards cyber is changing



Attack pattern shown in the video



Cyber and the regulatory landscape

FCA guidance on reporting a cyber incident

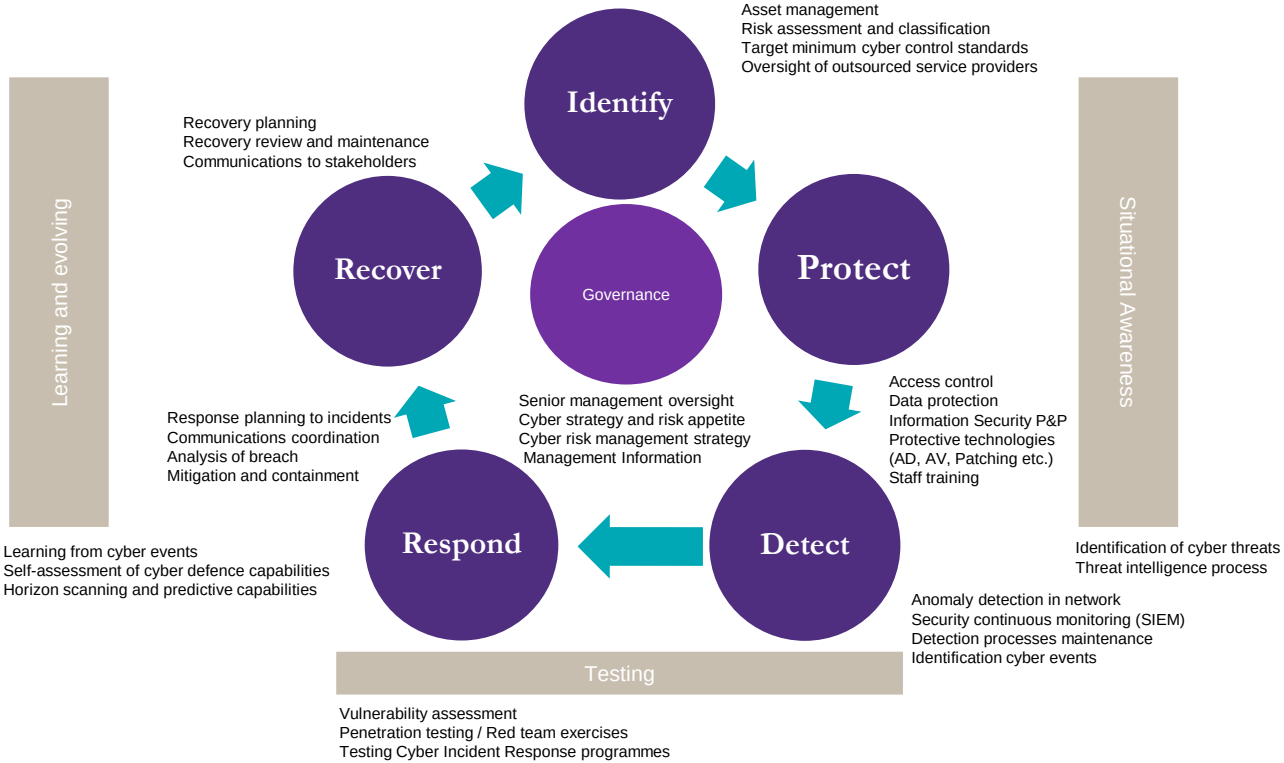
Under Principle 11 of the FCA Handbook, you must report material cyber incidents.

An incident **may be material** if it:

- results in **significant loss of data,** or the availability or control of your IT systems
- **affects a large number** of customers
- results in **unauthorised access** to, or malicious software present on, your information and communication systems

- Significant FCA focus via last year's self assessment questionnaire and recent visits to regulated firms with an aim to understand the Financial Service industry's level of resilience to cyber attacks and to inform future supervisory work in this area.
- The FCA expects forms of all sizes to have already established – and continue to develop – a security culture which is 'driven from the top down', including an active Board to the commitment of every employee.
- Material breaches are required to be reported to the FCA (in accordance with Principle 11 of the FCA Handbook). Complying with this requirement and sharing this information via the Cyber Information Sharing Partnership Platform is crucial for 'identifying and tackling patterns of attacks.'
- GDPR requires firms to report material data breaches within 72 hours after detection to the Information Commissioner's Office.
- Significant cybersecurity regulation passed by the NY DFS in 2017 now requires executives of their firms' resilience to cyber attacks.

The evolving regulatory landscape



How can we help…

Perform **Cyber health check** to help you with a high level assessment of your cyber security strengths and weaknesses, prioritise relevant risk areas and benchmark against peer organisations.

Cyber resilience review/audit to help you understand the effectiveness of your controls over cyber risk.

Vulnerability and penetration testing in which we test the state of specific internal and external cyber defences.

Phishing training in which we test your staff susceptibility to click on links or documents