Cyber Risk @ Barclays

RSMF Annual Conference 2014

BARCLAYS

Agenda

Quick overview of Barclays operations

Cyber Risk Management

Vulnerability & Threat Management

Summary of Approach

Q & A

We’re an old bank

1690

John Freame and Thomas Gould start trading as goldsmith bankers in Lombard Street, London

1864

Barclays builds a new banking house in Lombard Street, London

1966

Barclaycard, the UK’s first credit card, is launched

1967

Barclays unveils Barclaycash, the world’s first cash machine, at the Enfield branch, London

1986

Barclays is the first British bank to list its shares on both the Tokyo and New York stock exchanges

2008

Barclays purchases Lehman Brothers’ North America investment banking and capital markets businesses

2012

Pingit launched in the UK, allowing customers to transfer money via their mobile phone

2013

Barclays launches its Purpose and Values

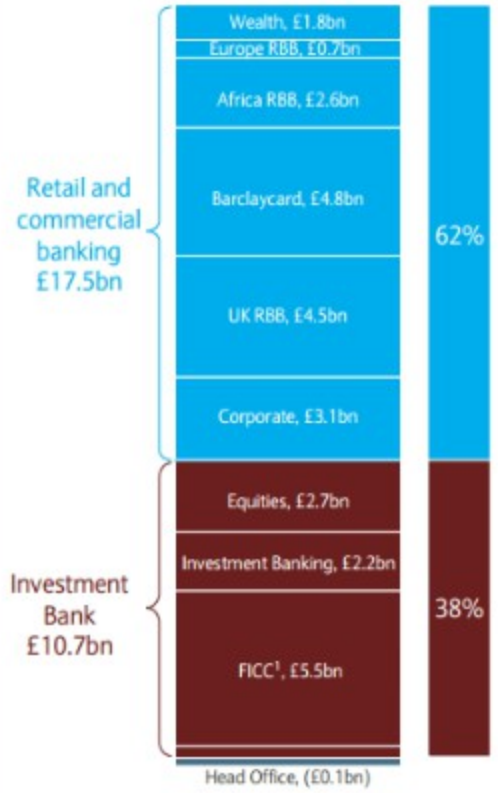
BARCLAYS

We're a big bank

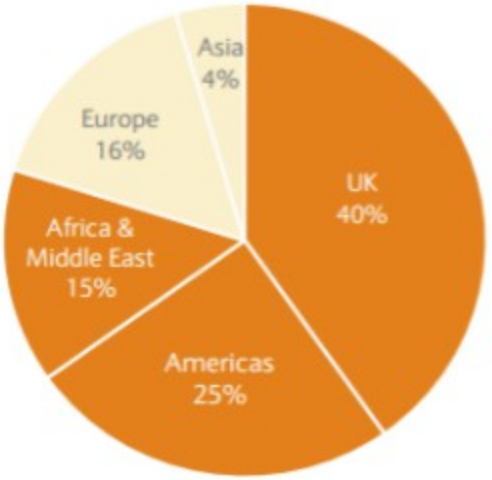
Global presence

- **Operating in over 50 countries, serving clients based in over 130**
- **Employ 140,000 people worldwide**
- **Six trading hubs: New York, London, Singapore, Tokyo, Johannesburg**

Group adjusted income of £28.2bn…

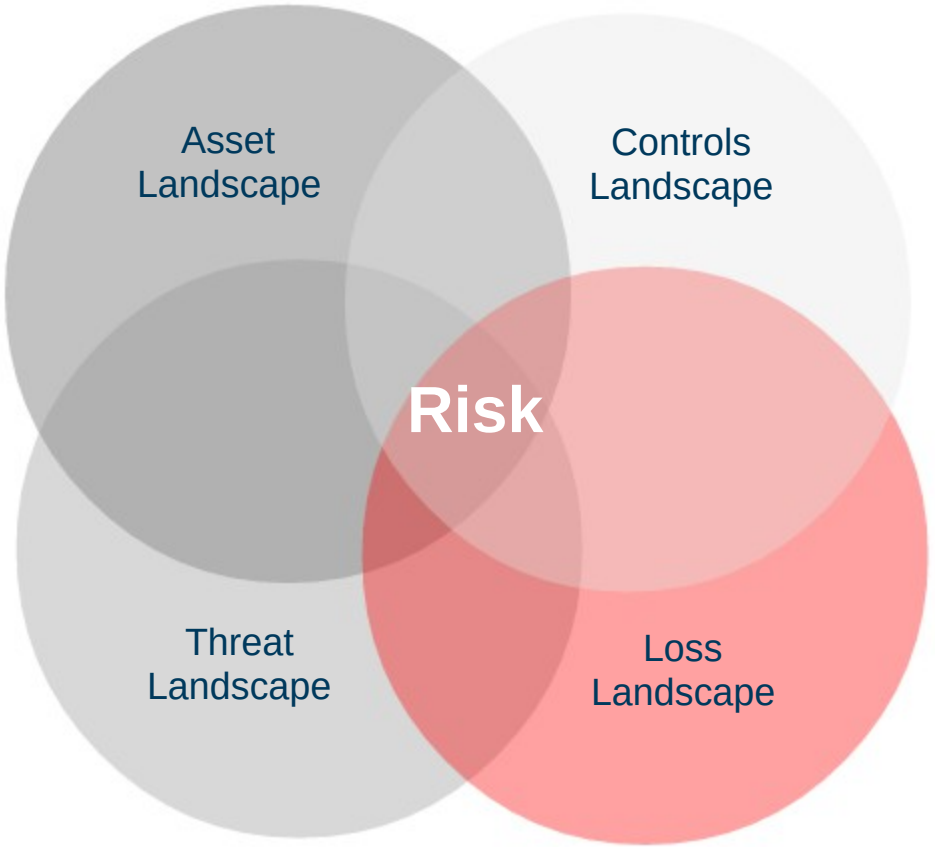


…with 80% of income from three markets



BARCLAYS

Landscape of Risk



BARCLAYS

ERMF: Cyber Key Risk Governance

ERMF Elements

Direct and Set Risk Appetite

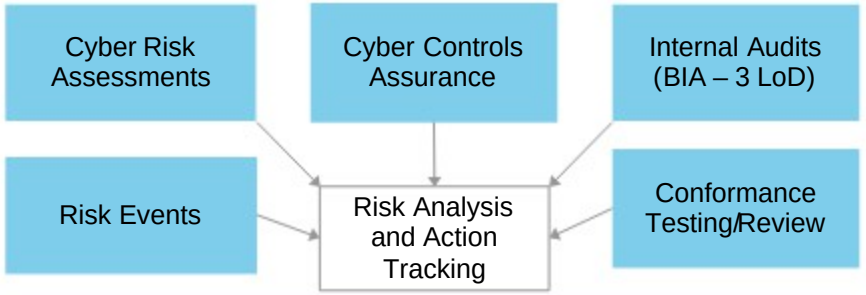
- Cyber Risk Control Framework
- Cyber Risk Policy
- Standards: Threat and Vulnerability Management, Threat Simulations, Investigations

Set and Monitor Controls

- Key Risk Indicators
- Cyber Risk Management Processes and Tools
- Key Metrics

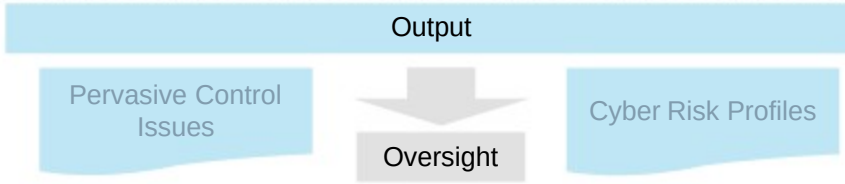
- Cyber is a Group Key Risk
- Managed through Cyber Control Risk Framework
- Cyber Risk focuses on “attacks”
- Risk Appetite to be set at Business Unit and Group level

Evaluate



- The status of risk is assessed by reviewing multiple sources of risk data (both self assessment and independent review)

Respond



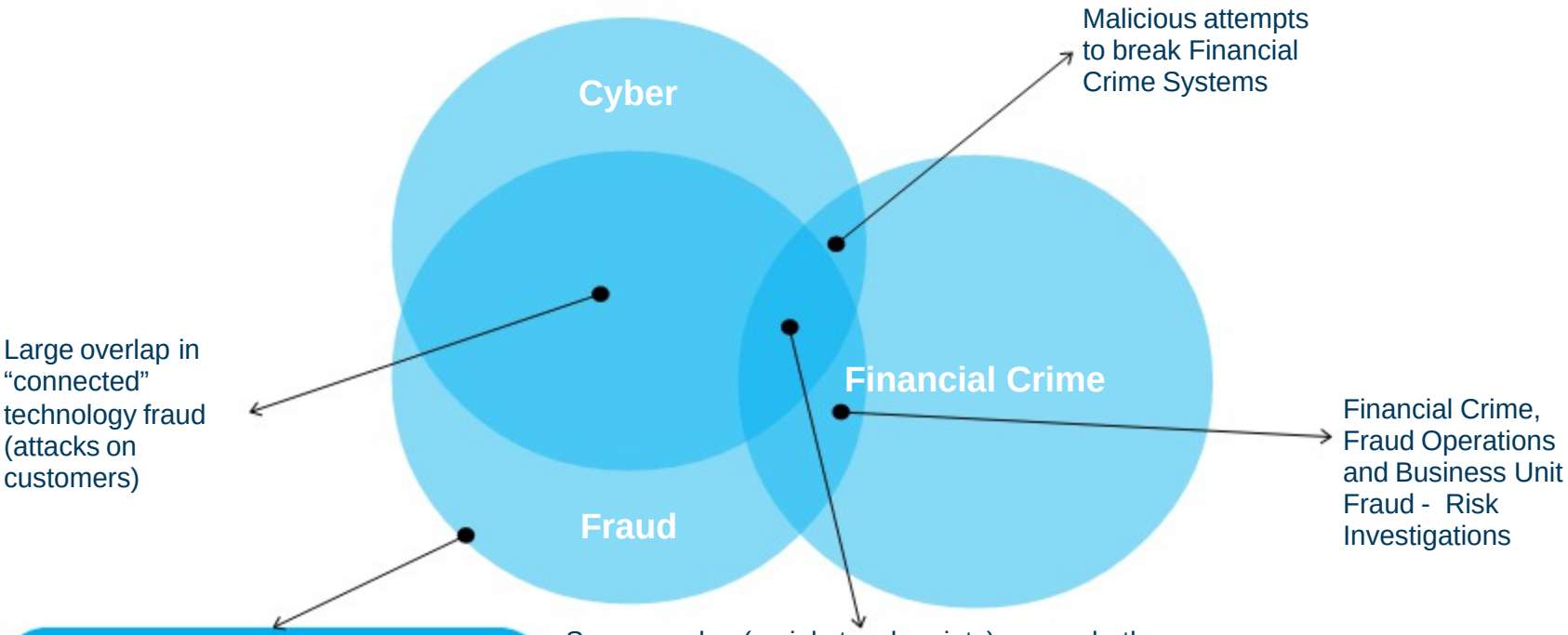
- This data is analysed to identify risk themes which drive improvement actions within Cyber Risk

Monitor

- Group-level oversight of the profile and direction of Cyber Risk performed by the Cyber Key Risk Forum

BARCLAYS

Cyber – Connection with Fraud & Financial Crime



BARCLAYS

Cyber Risk vs. Technology Risk (2nd Line of Defence)

Sub-Risks

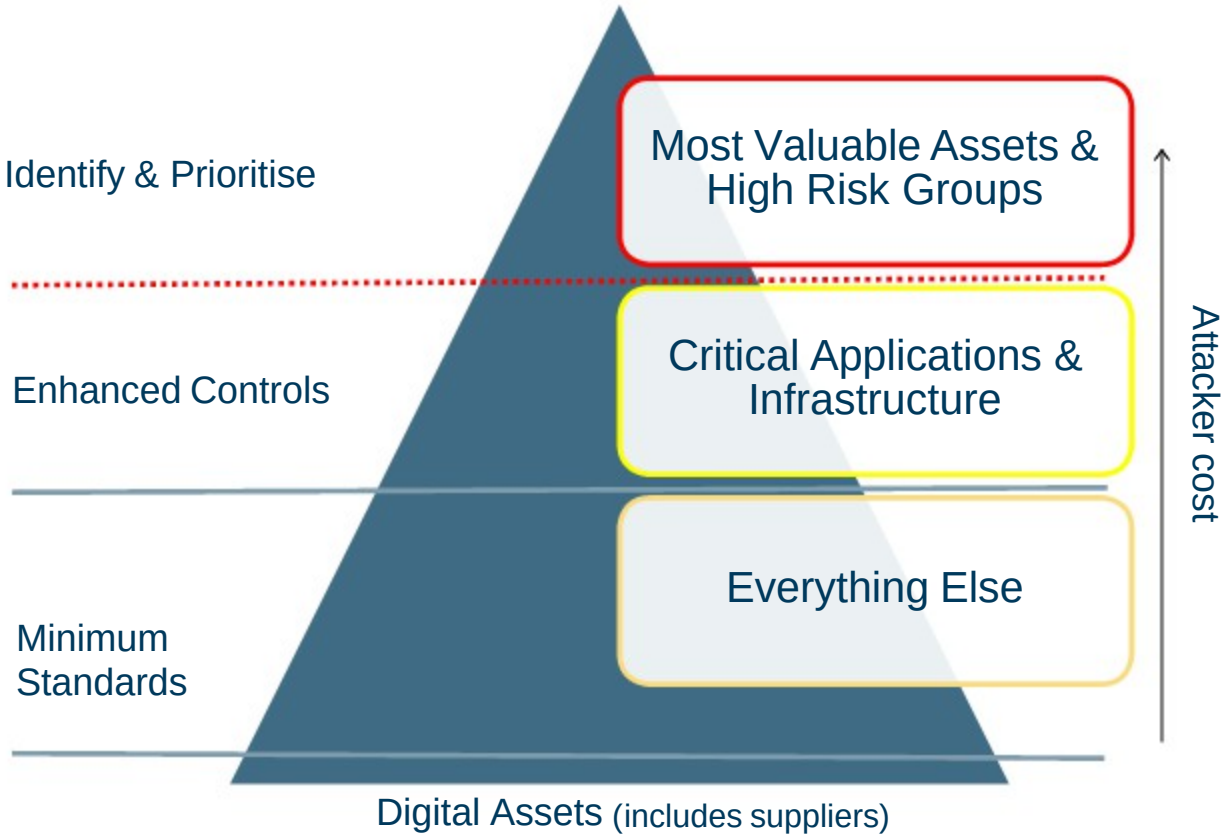
- Attacks on our Customers
- Attacks on Us and our Partners
- Attacks against Service Availability
- Attacks against Critical Banking Infrastructure we depend on

Sub-Risks

- IT Operations: Non-availability of IT systems
- IT Change: Inadequate design, testing and implementation of new and changed IT solutions
- IT System Security: Inadequate IT system security. The risk of unauthorised access to IT systems, resulting from inadequate IT systems security

BARCLAYS

Asset Landscape vs. Control Landscape

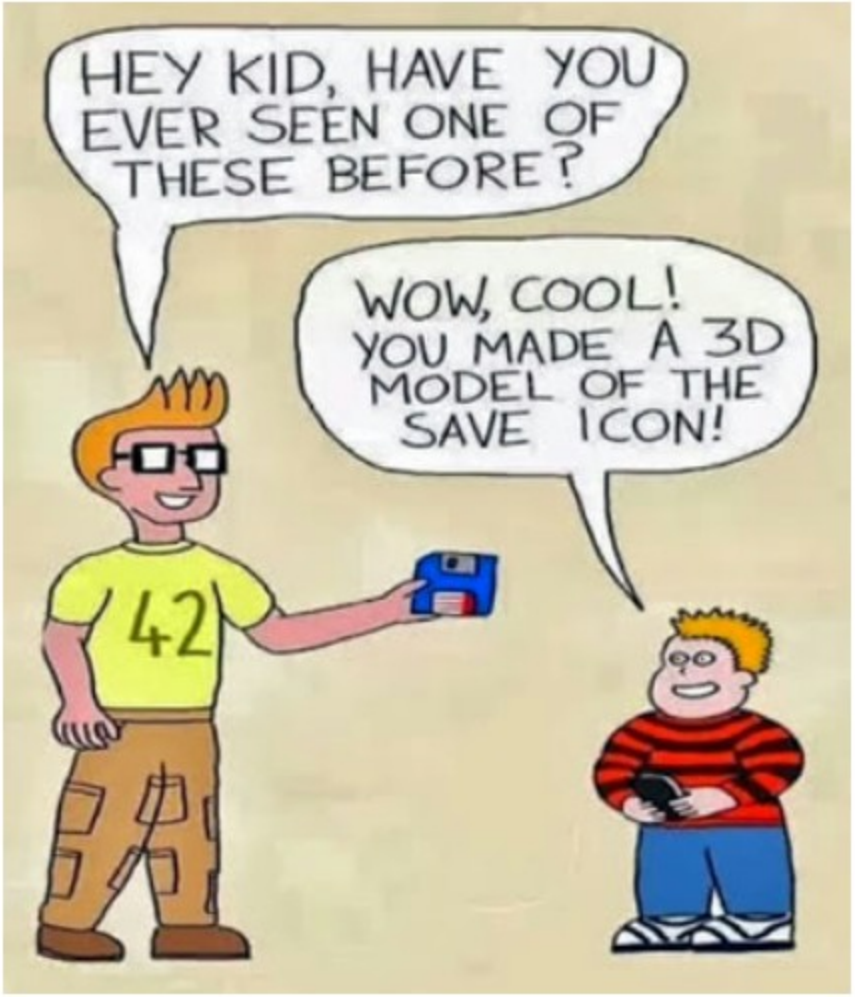


BARCLAYS

Megatrends

- **Minimum Viable Product:** shrinking time to market disrupting software development lifecycle, operations and security assurance
- **User experience:** Customer Journey (vs. Threat Actor Journey)
- **Digital insights**: data sources, volume, signal vs. noise, data scientists
- **BYOD, Mobile, Cloud:** 3 tech and workplace forces reshaping how we think about risk and control
- **3rd party risk:** supply chain risks; e.g. Target breach
- **CyberInsurance:** XLS vs. signals intelligence
- **Cyber Skills...**

Cyber Skills



BARCLAYS

Traditional InfoSec

- Extensive system hardening
- Heavy perimeter defences & detection
- Technology aligned penetration tests
- Segregated physical and infosec ops
- Practitioners apply their own risk appetite
- Threat intelligence == "nice to have“
- Secops BS (Big Screens)
- Fix all the things: harried defenders, “Just say No”
- Striving for Perfection vs. Purposeful Survivability?

Vulnerability Management

- Breadth vs. Depth: at scale vs. Channel specific
- Goals: complete? Patch what's important? Compliance?
- Vulnerability Identification
  - false positives vs. false negatives
  - Static vs. dynamic checks
  - Infrastructure, commercial apps, in-house apps, endpoints, “other”

Vulnerability Management

- Vulnerability Analysis (aka what to patch?)
  - CVSS...
  - Economic impact?
  - Critical/High vs. Medium/Low?
  - Attack chains: how many low risk vulns does a high risk make?
  - Exploitability index?
  - Proof of concept code availability?
  - Present in criminal kits?
  - For sale on the underground exploit market?
  - Trust relationships: explicit and implied
  - Operational risk of patching

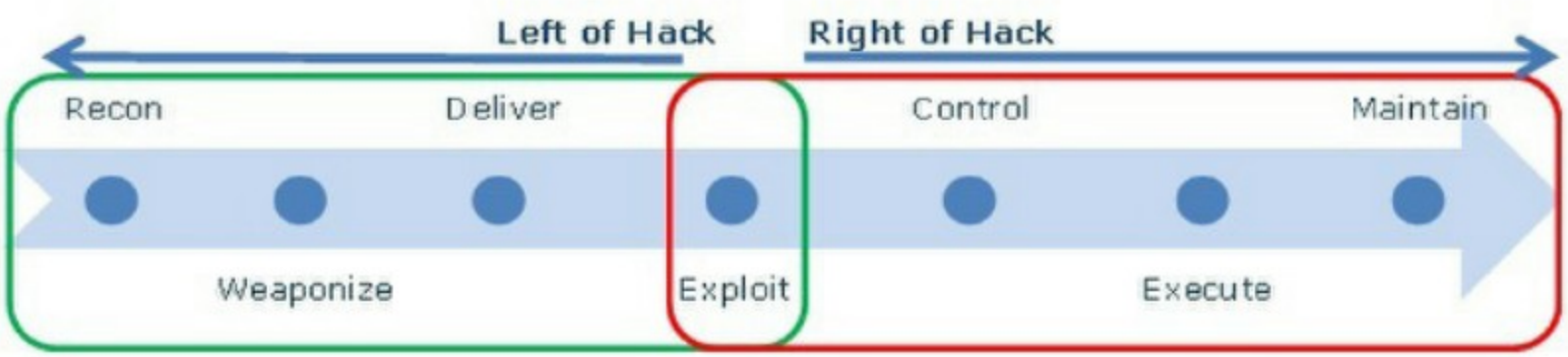
Innovation: Protecting the upside

- What is the business risk appetite? Markets differ, competition varies, winner takes all?
- Minimum Viable Product: Learning through failing (closed?)
- How to handle new technology with fresh, shiny and unknown attack surface?
- Trade off between security assurance activities and speed to market
- What is the right balance between investment in upfront protective and detective controls?
- Instrument services heavily, build a baseline and detect anomalies in real time?
- Piggy back Continuous Deployment to “hot patch” as part of Incident Response strategy (OODA loop)
- What about non-traditional tech....wearables?

Threat Management: Protect, Detect, Respond

- What does Success look like? (Link to Risk Appetite)
- What are you protecting? (Link to “Most Valuable” to us)
- What is “Most Valuable” to your intruders? (Critical Infrastructure, Access to 3rd party connections?)
- What signals are you assessing and what are your triggers? (outbound C2 polling? Netflow? DNS? 3rd party data dumps? SQL errors in application logs? Traffic mix? IP blacklists matched against channel activity?)
- What actionable insights are you getting from your existing data sources?
- How do you learn from prior events?

“Left a bit”: Cyber Kill Chain – Lockheed Martin



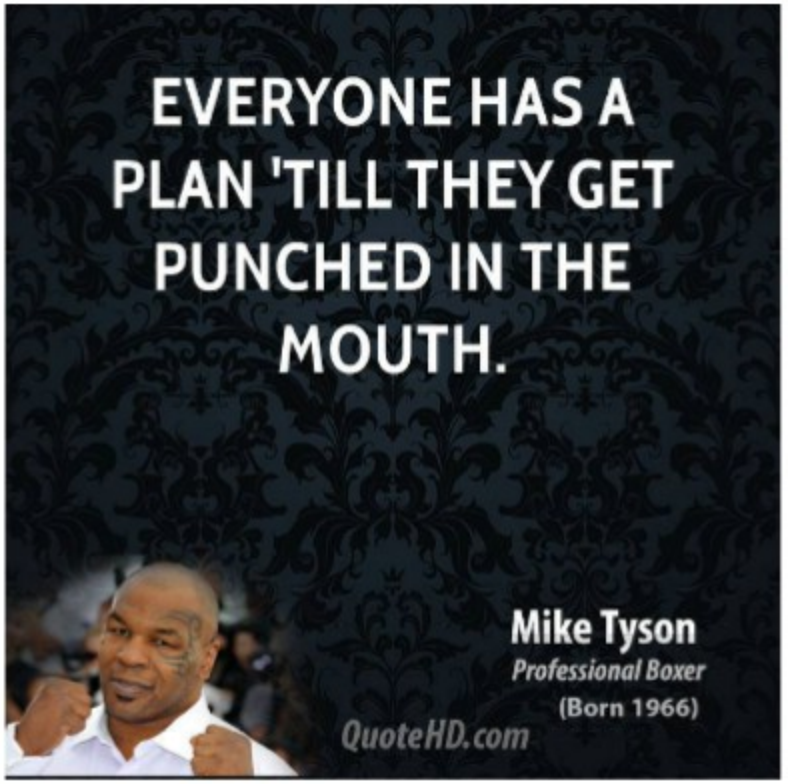
BARCLAYS

Threat Simulations

- Red Teaming vs. Penetration tests
- Broad in scope, yet specific business focused goals ("crown jewels")
- Ask your CIO: "what keeps you awake at night”
- Characterise the threat and act it out
- Drive improvements in protect, detect, response
  - breach simulations: assume you’re vulnerable (who isn’t?)
  - tabletop vs hands on
- Simulations make reality plastic; passports, Denial of Service
- Process hacking

Incident Response

- Situational Advantage vs. Attacker Dilemma
- Containment?
  - Speed (time to respond vs. contain)
- Persistence mechanism identification
  - Baseline
- How long to hover over the Kill switch?



BARCLAYS

Check and Challenge

Are we capturing the right data to measure our Key Risk Indicators?

Deep dives on Risk “Events”

Are our policies aligning incentives and driving responsible risk tasking within appetite?

Are we effectively increasing the costs of our attackers whilst managing our own?

Do we have the right capabilities in the right places?

Cyber Risk Approach - Summary

- **Threat Centric**: understand our foes, their goals and attack patterns (kill chain analysis)
- **Agile controls:** instrument broadly & use lean data science, Threat Intel and Risk Appetite to drive focused approach to control scope & design
- Run broad scope, goal oriented **Threat Simulations** to drive continuous improvements in Protection, Detection & Response
- **Protect the upside**: design controls with our Digital Office agenda front and centre

Q & A

craig.balding@barclays.com

BARCLAYS