Intelligence-Led Cyber Strategy

Protecting Money, Data and Time

Robin Barnwell
Head: Security Strategy Enablement
Standard Bank Group

Some History….

What not to do…

Compliance-Led Information Security

In 2015…..

- Very **traditional** security function
- Strategy is **ISO27001** alignment and **closing audit findings**
- **Focus on volume** of controls vs effectiveness of controls
- Heavily invested in **traditional prevention** controls (eg LAM, Firewalls)
- Sold through fear, uncertainty and doubt (**FUD**)
- **Not a priority** for the organization / no business value
- Security is an **opt-in** service / bolted onto products and services
- Robust risk management processes but **little risk mitigation**
- Belief that **complying to frameworks** gave us good Cyber Security

Information Security Forum

PCI DSS COMPLIANT

INFORMATION SECURITY MANAGEMENT SYSTEMS ISO ISO/IEC 27001:2013

Nothing we were doing could stop a Cyber attack

Problem statement

- **Blind compliance** to frameworks doesn't work against Cyber threats
- Cyber threat landscape **changes daily** – frameworks do not
- Spending too much time fixing the **wrong problems**
- Lots of technology, but **ineffective** prevent and detect capabilities
- Missing key capabilities for **cyber incident response**
- **Incidents increasing** in frequency and severity
- **Complex** environment across the Group (multiple legal entities, 3rd parties)
- Multiple **exposure** points, multiple attack vectors

Think about cyber prioritisation differently

Cyber Risk Approach

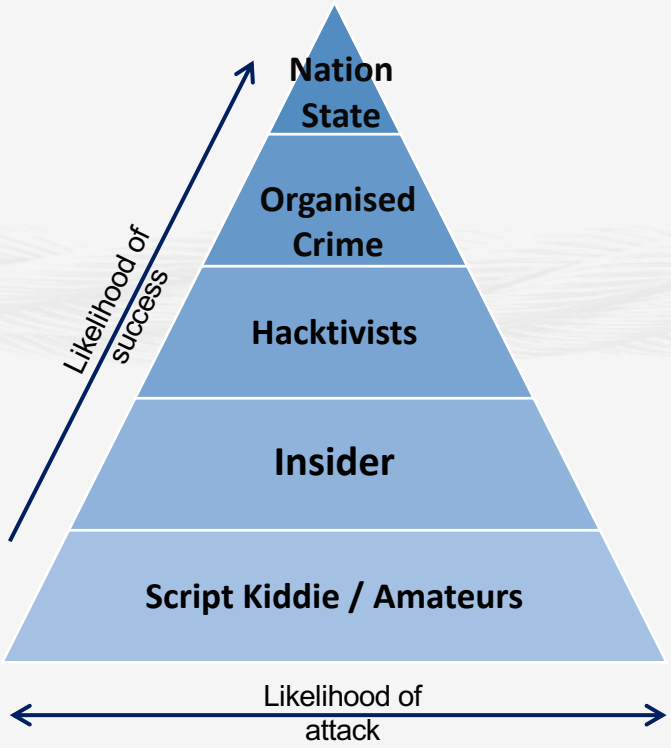
Learning from attack trends and incidents

Cyber Risk is complicated….. or is it???

Assets → **Vulnerabilities** → **Threats** → **Impact**

- Explosion in Assets
- **Cloud, BYOD, IOT, 3rd Party, Mobile**, etc, etc, etc

- Around **19,000 new** technical vulnerabilities reported in 2018*
- **Up 27%** on 2017*
- Vulnerabilities in core security products, **hardware / firmware**
- Increase in **Zero Days**
- **People** and process gaps



Financial Loss *(Money)*

Steal Information *(Data)*

Disrupt Services *(Time)*

**Tenable Vulnerability Intelligence Report*

Cyber Risk Management Process

Assets

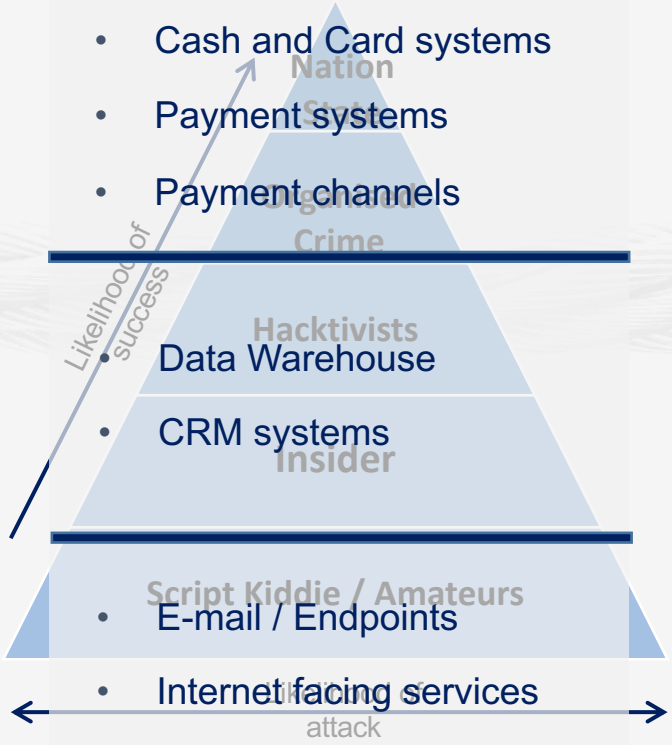
- Explosion in Assets
- **Cloud, BYOD, IOT, 3rd Party, Mobile**, etc, etc, etc

Vulnerabilities

- Financial Malware
- Malware attacks on cash/payment systems
- Around **19,000 new** technical vulnerabilities reported in 2018*
- **Up 27%** on 2017*
- Vulnerabilities in core security products, hardware / firmware
- Increase in **Zero Days**
- **People** and process gaps

Threats

- Cash and Card systems
- Payment systems
- Payment channels
- Data Breach
- Data Exposure
- Phishing
- Ransomware
- Denial of Service attacks



Impact

- Specific to attack path

Financial Loss *(Money)*

- Specific to attack path

Steal Information *(Data)*

- Specific to attack path

Disrupt Services *(Time)*

Impact Assessment by Industry

Retail

- Ticketmaster – 5% of userbase
- Under Armor – 150m records through app
- Adidas – client records exposed through website

Finance

- Cosmos Bank ATM Cash out / SWIFT transfer - $13.5m
- Bank of Valletta goes dark after hackers go after €13m
- Bithumb crypto exchanges attack - 35 billion Korean won

Medical

- Atrium Health - 2.6m records
- SingHealth – Singapore Health 1.5m records

Government Services

- Aadhaar, India's national ID database - 1.1b records
- US Postal Services – 60m records

Hospitality

- Starwood Hotels 500 million records
- $700k GDPR fine for Hilton Data Breach
- British Airways – 380k records

ISP / Hosting

- DDoS attack on Github sets a new record for attack size
- Hackers destroy VFEmail Service, deleted all its Data and Backups

Business- Aligned strategy

How to improve cyber resilience

Business Impact Assessment

- Which assets does you **business/customers prioritise** (money, data, time)?
- What does a **"bad day"** for your business look like?
  - ✓ Is it a customer losing their wealth?
  - ✓ Is it loss of strategic information or customer data?
  - ✓ Is it loss of productivity?
- Are you prioritising your time/effort on the **right problem**?
- **Not all risks are the same to your business**

Business Aligned Priority =

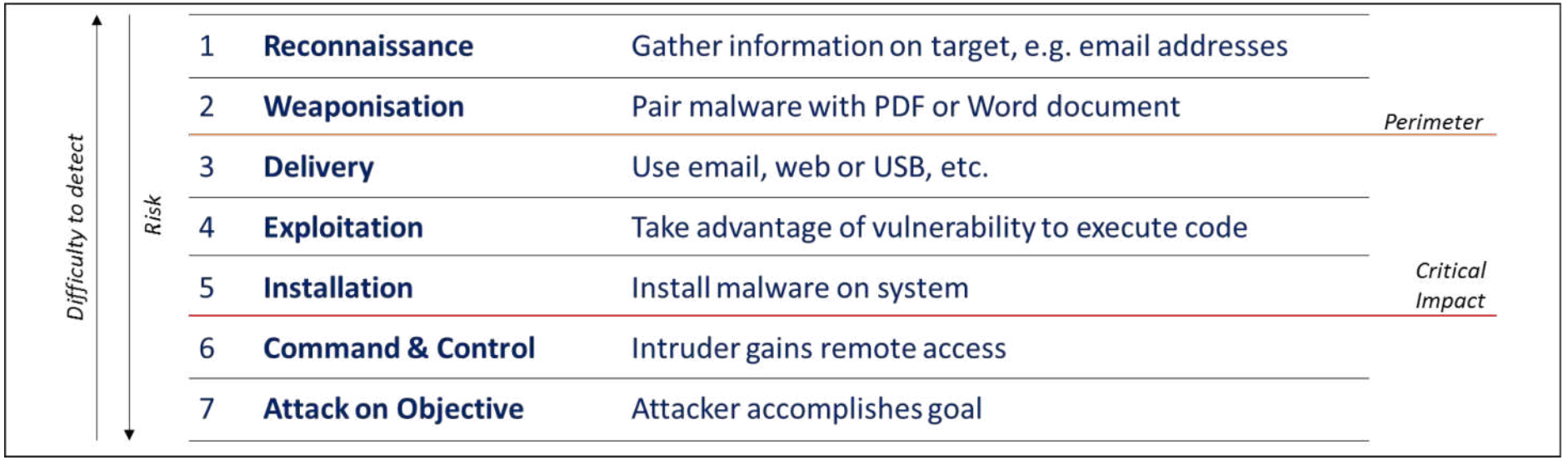
Finance Risk (Financial Loss through Malware, 3rd Party)

Data Risk (Confidential Data Breach, Extortion, 3rd Party)

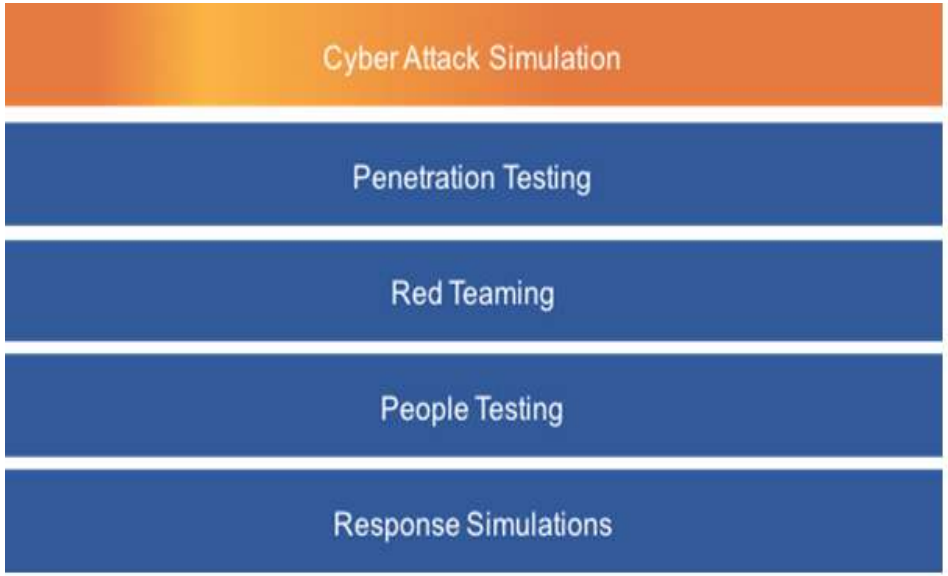
Service Risk (Disruption, Extortion, 3rd Party)

Threat Modelling / Attack Path Mapping

- **Identify assets (system, people, 3rd parties)** that can cause the business impact
- **Map attack paths** to the asset and identify the vulnerabilities in the path
- List all possible controls for the vulnerabilities
- Balanced controls across **Predict, Prevent, Detect and Response**
- Focus effort on common **exposure points** (user, endpoint, web) and **lateral movement** (network, AD and services)



Continuous Testing / Continuous Monitoring



- Real life testing of most likely cyber incidents on most likely targets – continuous testing for improvements
- Better visibility of people, process and technology weaknesses and failures – continuous monitoring of these for effectiveness
- People testing through mock phishing campaigns and password cracking

Improvement in posture must be measurable through testing

Intelligence-Led Cyber Strategy….

- Know which **impact** will most **affect your business**
- Assess your **readiness to respond** to that impact
- Invest in blanket controls to provide **maximum visibility and protection**
- Protect **common points** for different risks to optimise effort
- Selective use of controls in the **right place at the right time**
- Continuously **test and monitor** controls

Thank You