CSIR Conference

Cyber Threats and Responses in the banking sector

Paul Strauss
Chief Information Risk Officer

October 2017

Cyber Risk Drivers

Meet the Threat Actors

What they want and what they get…

Hacktivists

- Hacktivists are politically and socially motivated individuals
- Use computer systems in order to **protest and promote their cause**
- In an exclusive conversation with the hackers behind this breach, HackRead was told that:

Cyber Criminals

- Hostile by nature with the target being **financial gain**. High skill level

"We are Anonymous and supporters of LulzSec and we will make sure the corrupt governments would listen to us or we will keep on embarrassing them — It's time to end their corruption and feed the poor."

Corporations

- Organisations involved in offensive tactics
- Aim to **gain competitive advantage**.

Employees

- Staff and contractors. Insiders assisting syndicates
- possesses a significant amount of **knowledge** that allows them to place effective attacks against assets of their organisation.

Terrorists

- Preferred targets of cyber terrorists are mostly critical infrastructures (e.g. public health, energy production, telecommunication etc.), as their failures causes **severe malicious impact** in society and government.

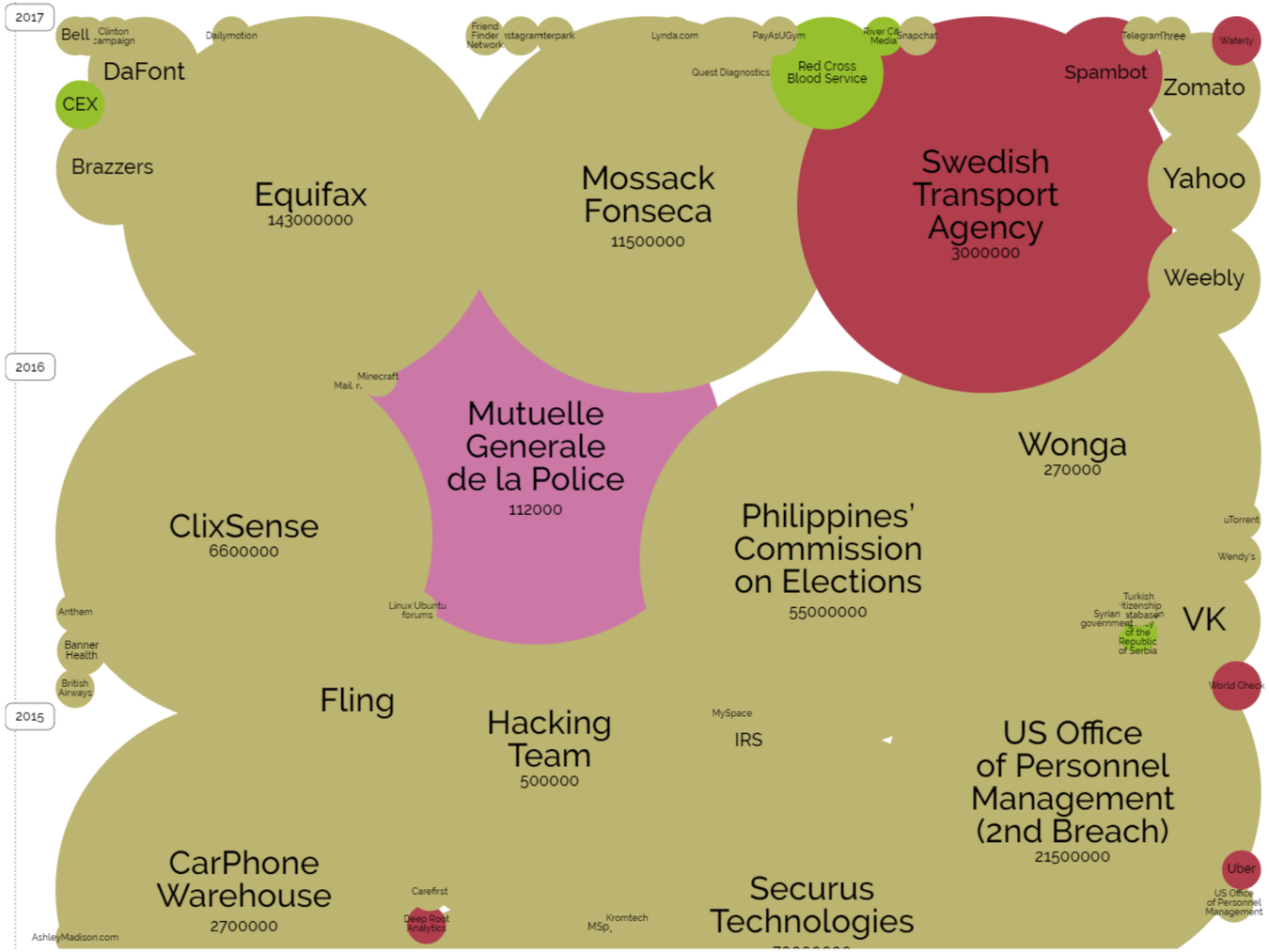
Nation States

- Nation states can have offensive cyber capabilities and could potentially use them against an adversary. **Cyber warfare**

***Majority of incidents – Hacktivism and Cyber Crime*

Some of the world's biggest data breaches

Greater than 30 000 records, as on 10 September 2017



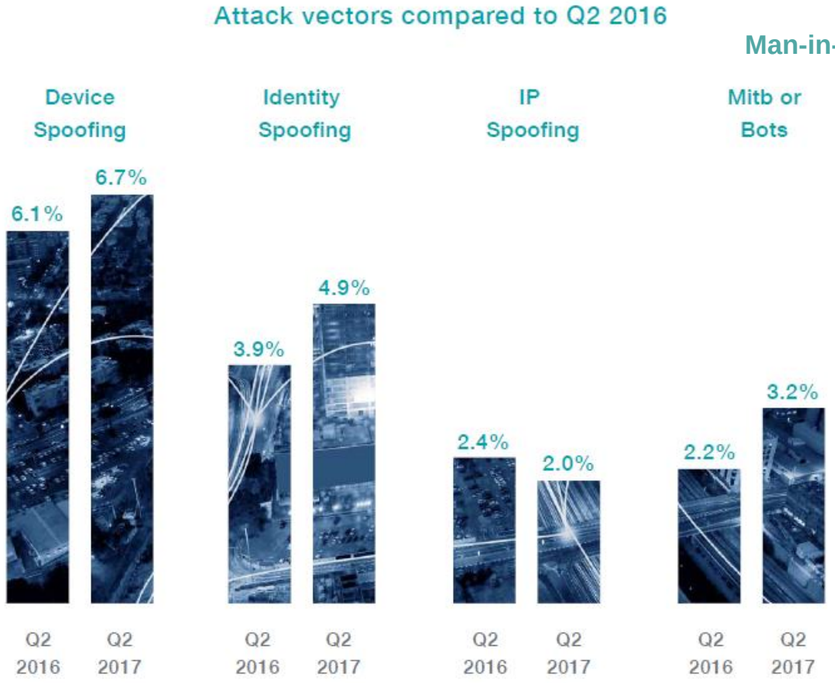
Bubble size = sensitivity of records
Bubble colour = method of breach

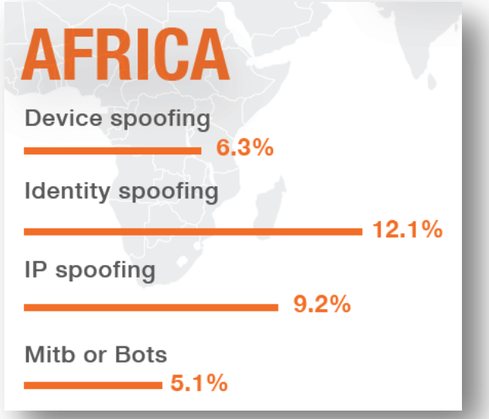
METHOD OF LEAK

- all
- accidentally published
- hacked
- inside job
- lost / stolen device
- poor security

Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Are we at risk?





The WannaCry malware attack infected more than 300,000 computers in over 150 countries in less than 24 hours.

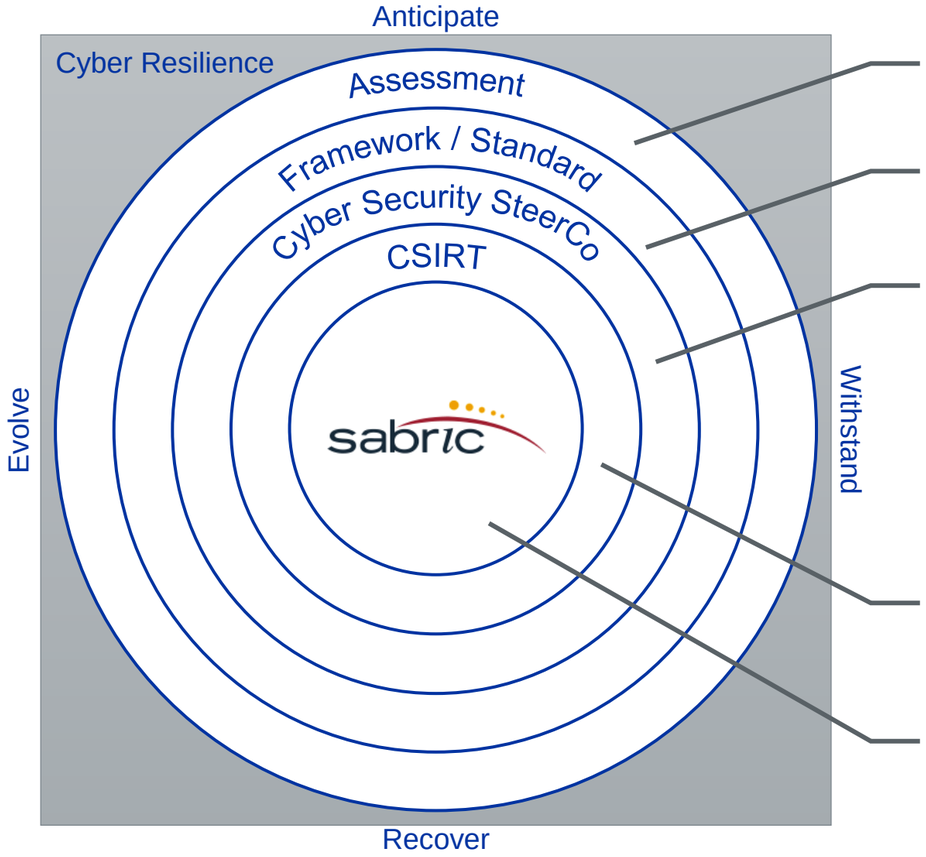
Source: ThreatMetrix Cybercrime 2017 report

Financial Services' Response to Cyber Crime

Creation of Industry Sectors stipulated in Cybercrimes and Cybersecurity Bill
"encourage and facilitate the establishment of nodal points and private sector computer security incident response teams in the private sector; and respond to cybersecurity incidents" (chapter 10, section 54, 4.cc and 4.dd)

Critical for Success:
Convening Body

- SARB
- BASA
- International Forums
- Memberships
- SAPS
- National Cyber Security Hub
- BankSETA



- Self-assessment
- Aligned with NIST
- All representative Banks
- Daily, Weekly, Information Exchange + Co-location
- Convening Body + Overall Threat Profile + Board

Challenges:
- Mandate to share
- Participation
- Maturity levels
- Strategic vs Operational
- Interpretation of Cyber Crime vs Cyber Security

Cyber Risk in Context

Impact:

- Reputational
- Operational Efficacy
- Customer Loss
- Fiancial Loss
- Delayed Strategies
- Outage of Critical Infrastructure if systemic

Cyber Risk:

Cyber Extortion

Cyber Extortion is a crime involving an attack or threat of attack coupled with a demand for money to avert or stop the attack.

Large Scale Data Breach

A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorised to do so (e.g. Panama Papers).

System Infiltration

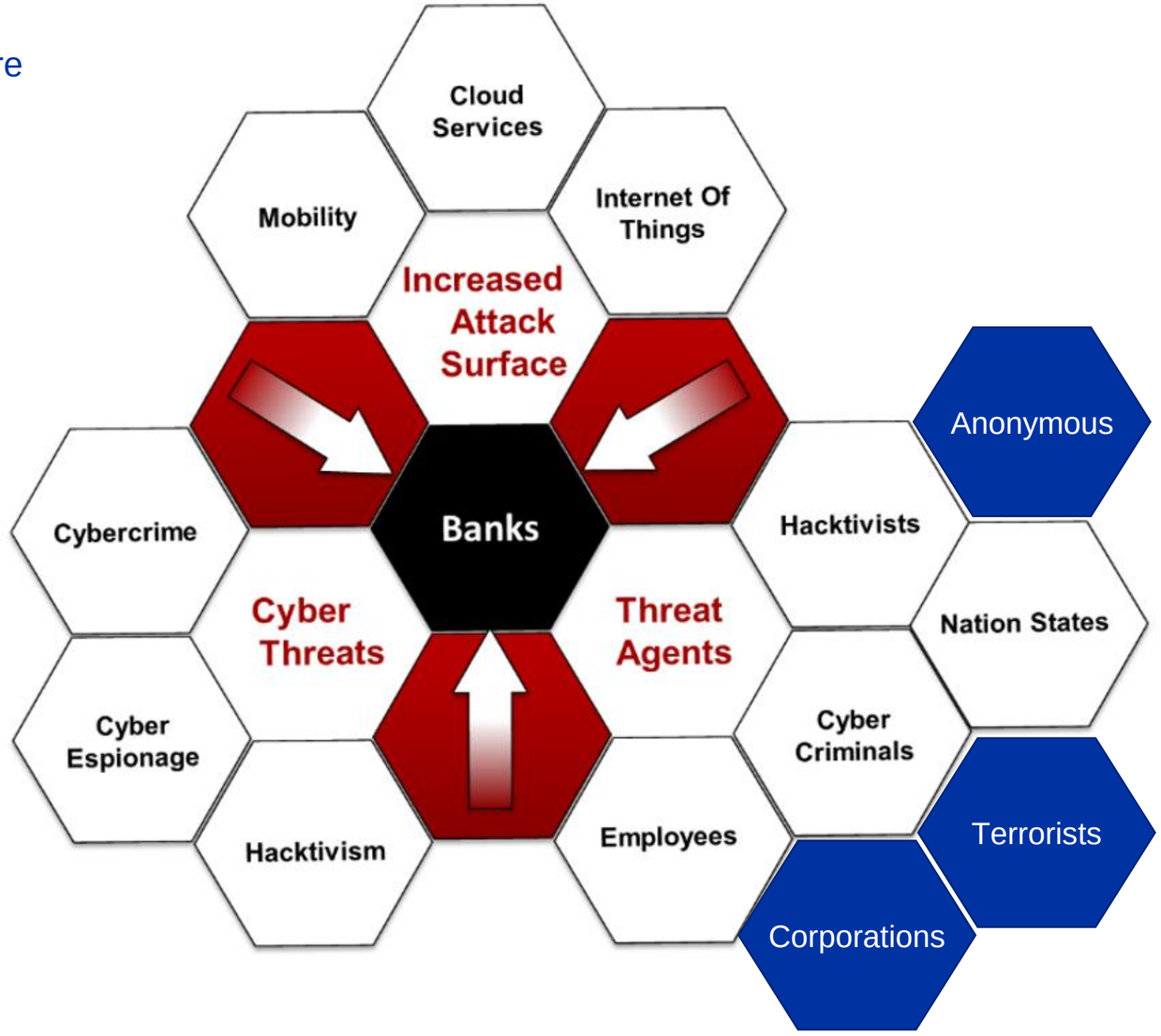
Unauthorised access to the network or system with the intent to defraud, manipulate or impede business operations.

Concerted Cyber Attack

Well planned and thoroughly executed Cyber attack, impacting on the organisation impacting group wide operations with large scale negative public sentiment

So What?

Threat Landscape Architecture

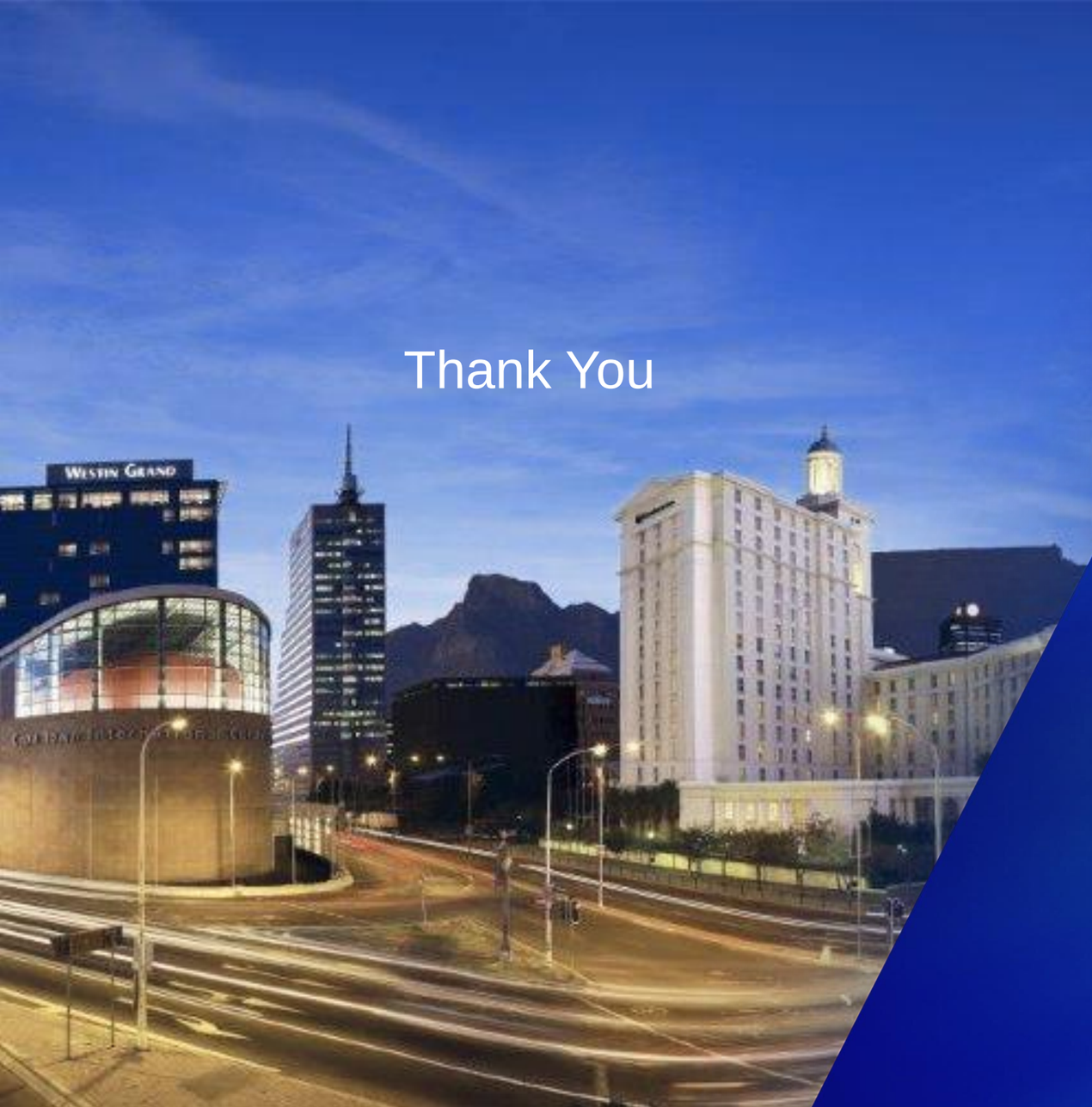


Source: South African Financial Services Sector Cyber Threat Framework

Conclusion

Cyber Crime is profoundly different to traditional crime:

- Requires high levels of technical expertise and skills;
- Large scale investigations across multiple borders;
- What works one day won’t work the next (virus being changed in character i.e. WannaCry – Petya);
- Intelligence changes on a daily basis (new threats, change in modus operandi);
- Attacks very sophisticated and targeted; and
- Tools, techniques, skills used are at a level that was once only reserved for nation states (leaked NSA recipies).



Thank You

Questions?