WHO'S TARGETING YOUR SENSITIVE DATA AND HOW?

Simon Carlson

Senior Sales Engineer – ANZ

TRITON STOPS MORE THREATS. WE CAN PROVE IT.

Start with a question...

What does the National Security Advisor to the Obama administration think is the greatest threat to the world today?

Answers on a # tag please…

A. Obama Himself

B. Nuclear Weapons

C. Weapons of Mass Destruction

D. The Keyboard

Answers on a # tag please…

D. The Keyboard

"..today we see that same level of capability being exercised by lone individuals armed with keyboards instead of bombs."

‘the times they are a-changin’

TARGETED

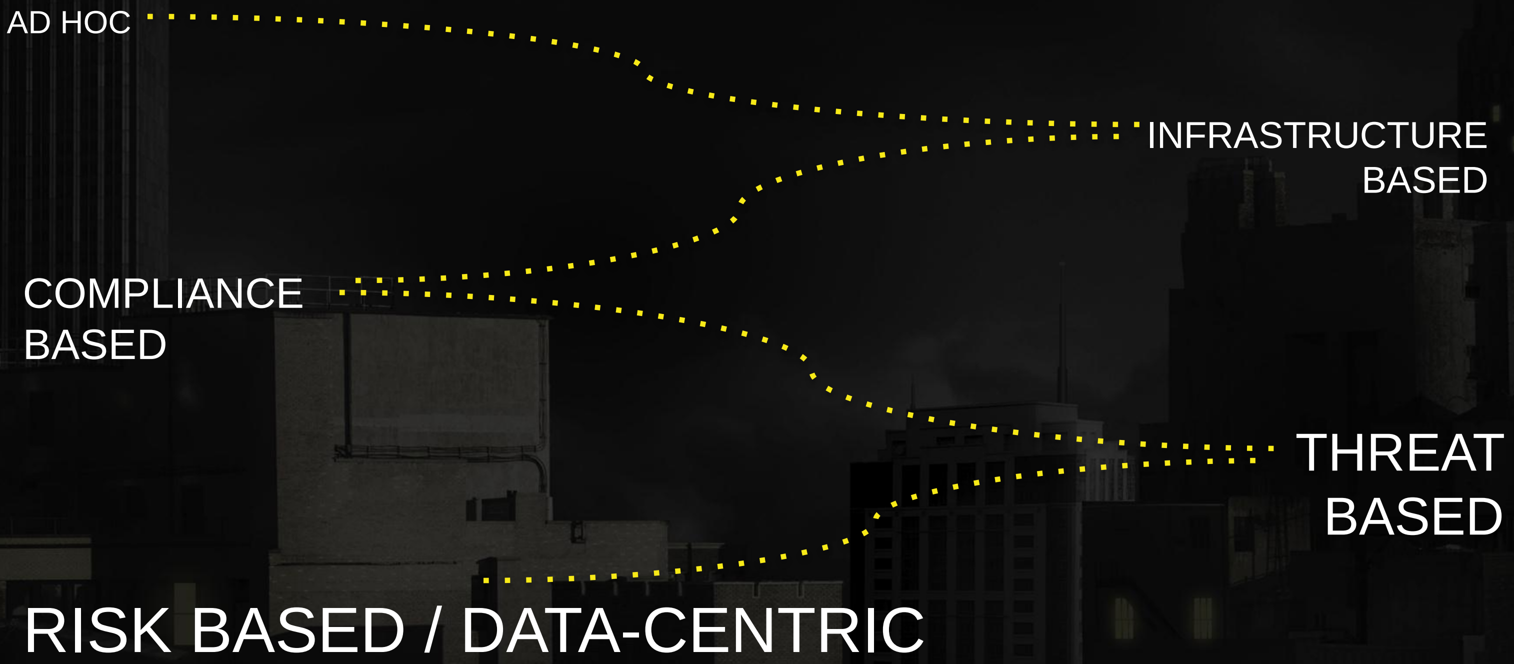
PERSISTANT

EVASIVE

COMPLEX

The Cyber Security Journey (so far..)

Today's goal is Risk Based/Data-Centric with Threat Modelling



AD HOC

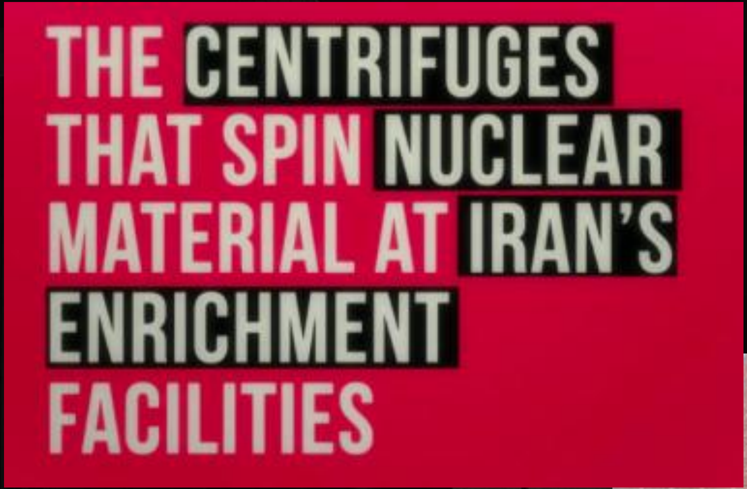
INFRASTRUCTURE BASED

COMPLIANCE BASED

THREAT BASED

RISK BASED / DATA-CENTRIC

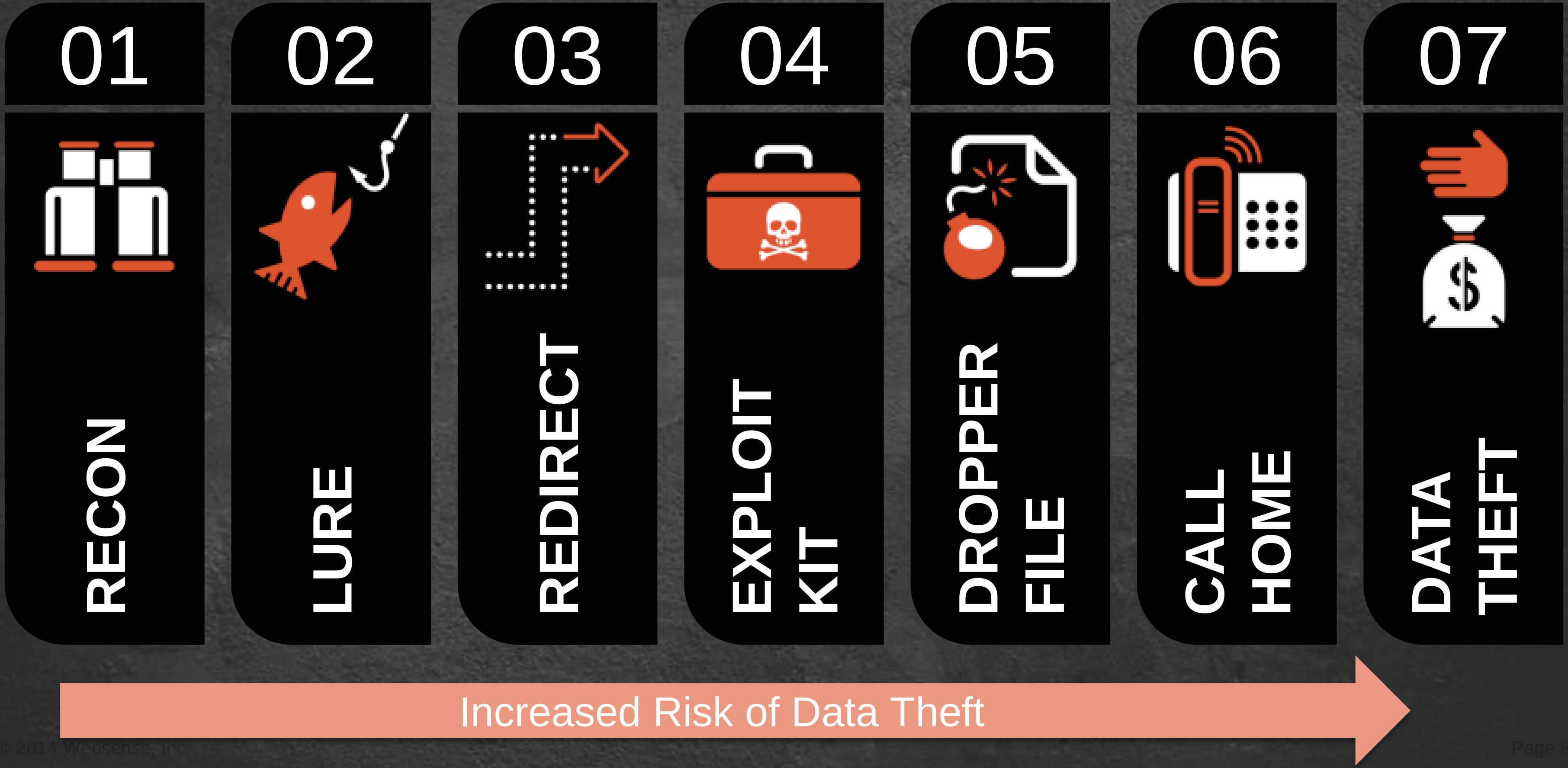
But we are still 10 years behind…



THE CENTRIFUGES THAT SPIN NUCLEAR MATERIAL AT IRAN'S ENRICHMENT FACILITIES

These Advanced Attack can be broken into stages...

websense TRITON



01 RECON

02 LURE

03 REDIRECT

04 EXPLOIT KIT

05 DROPPER FILE

06 CALL HOME

07 DATA THEFT

Increased Risk of Data Theft

For example: Target Corp – Late 2013

01 Attackers Identified Faizo (HVAC and billing system MS provider) as potential target

02 Spear-phish emails target Faizo employees

03 Likely that emails direct Faizo employees to rouge site

04 Unknown but likely method of Citidel trojan install

05 Citidel trojan finds network credentials and information on accessing Target's Ariba billing system

06 07 Credentials ex-filtrated from Faizo's network

Modern Attack: Target Corp – Late 2013

websense TRITON

08

Lateral movement: attackers access Target’s network using stolen Faizo credentials

09

Installs RAT on internal Target web server to act as control server

10

Lateral movement: BlackPOS variant (common POS malware) installs onto POS systems

11

BlackPOS uses RAM-scraping to dump memory then parses the dump to identify CCNs. Findings uploaded to control server

12

A constant stream of updates and instructions. Attackers performed a ‘test run’ of BlackPOS in early Nov, before going ‘live’ in Dec

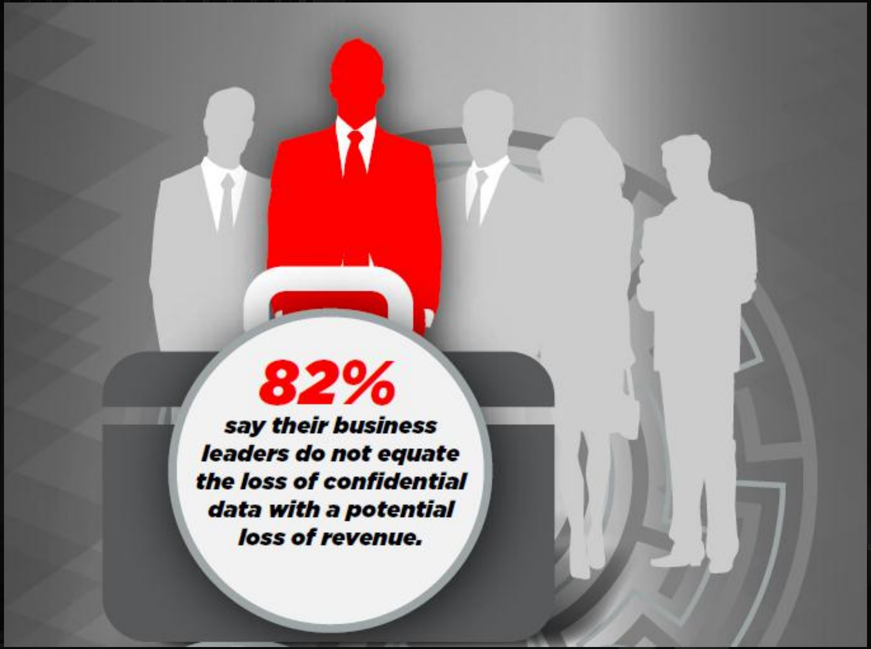
13

Financial records of over 110M customers, including 40M customer CCNs, uploaded to servers in Russia, Brazil and Miami

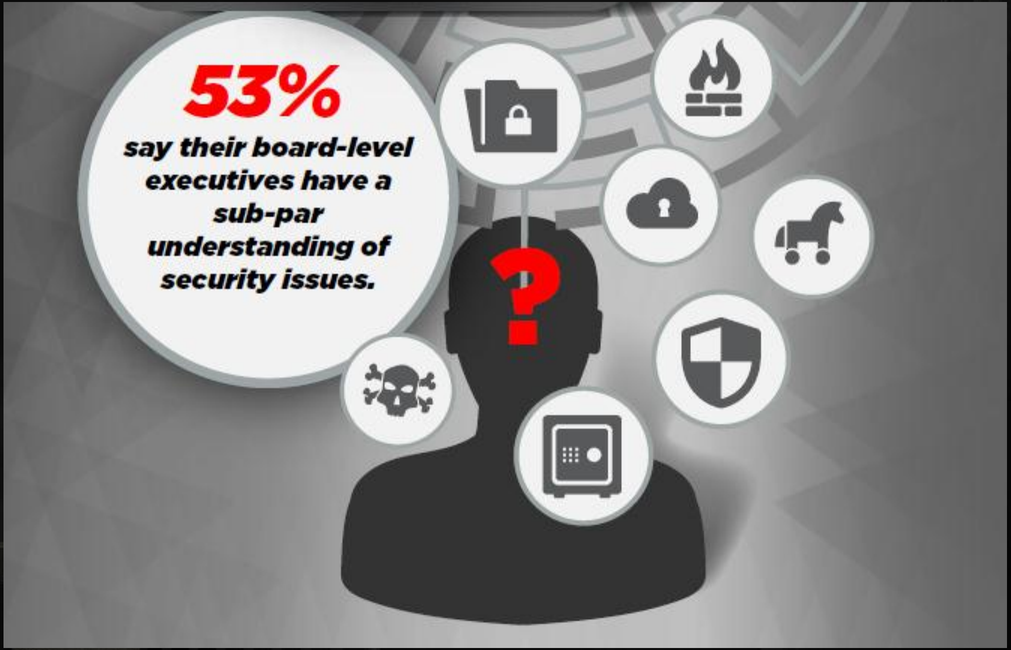
Why these attacks happen from a CISO Perspective

websense TRITON

WARNING: GRATUITOUS STATS FOLLOW!



82% say their business leaders do not equate the loss of confidential data with a potential loss of revenue.



53% say their board-level executives have a sub-par understanding of security issues.

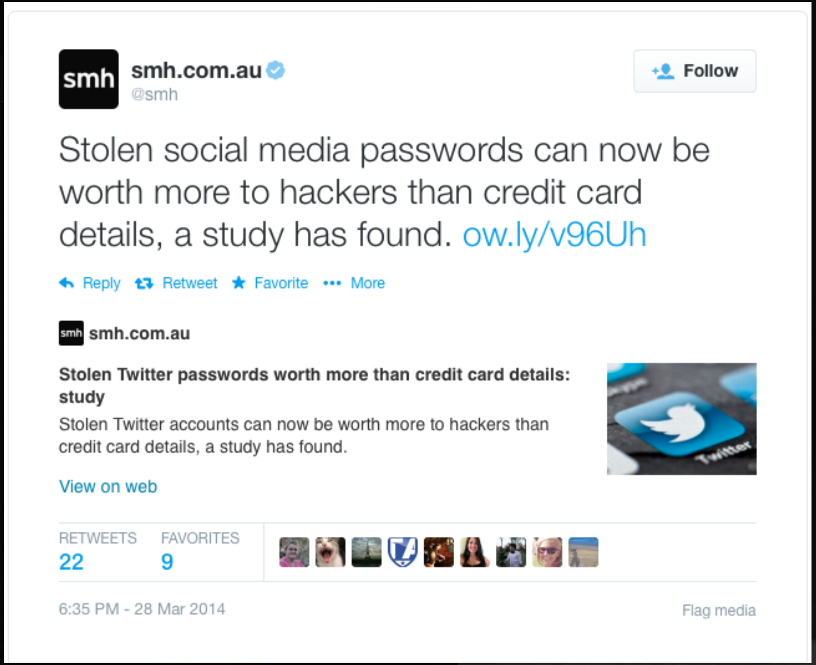
So where do we see the risk to Data Security today?

Broken Business Processes

Insider Threat

Malicious Threats

And we can sum up the why in 140 words...



smh.com.au
@smh

Stolen social media passwords can now be worth more to hackers than credit card details, a study has found. ow.ly/v96Uh

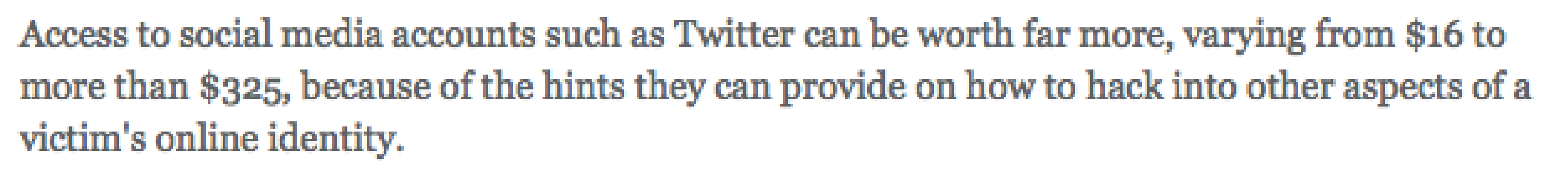
smh.com.au

Stolen Twitter passwords worth more than credit card details: study

Stolen Twitter accounts can now be worth more to hackers than credit card details, a study has found.

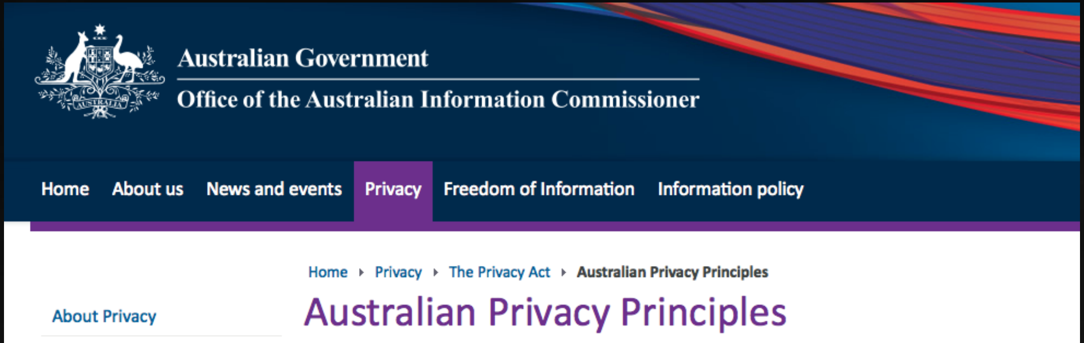
RETWEETS 22 FAVORITES 9

6:35 PM - 28 Mar 2014



Access to social media accounts such as Twitter can be worth far more, varying from $16 to more than $325, because of the hints they can provide on how to hack into other aspects of a victim's online identity.

Which is where the Privacy Act comes in...



Australian Government

Office of the Australian Information Commissioner

Home ▸ Privacy ▸ The Privacy Act ▸ Australian Privacy Principles

Australian Privacy Principles

Fines of up to $340k and $1.7m for serious breaches

Adds new definitions for health care and credit providers

Covers personal and sensitive information

Introduced in March 2014 to replace the NPP's.

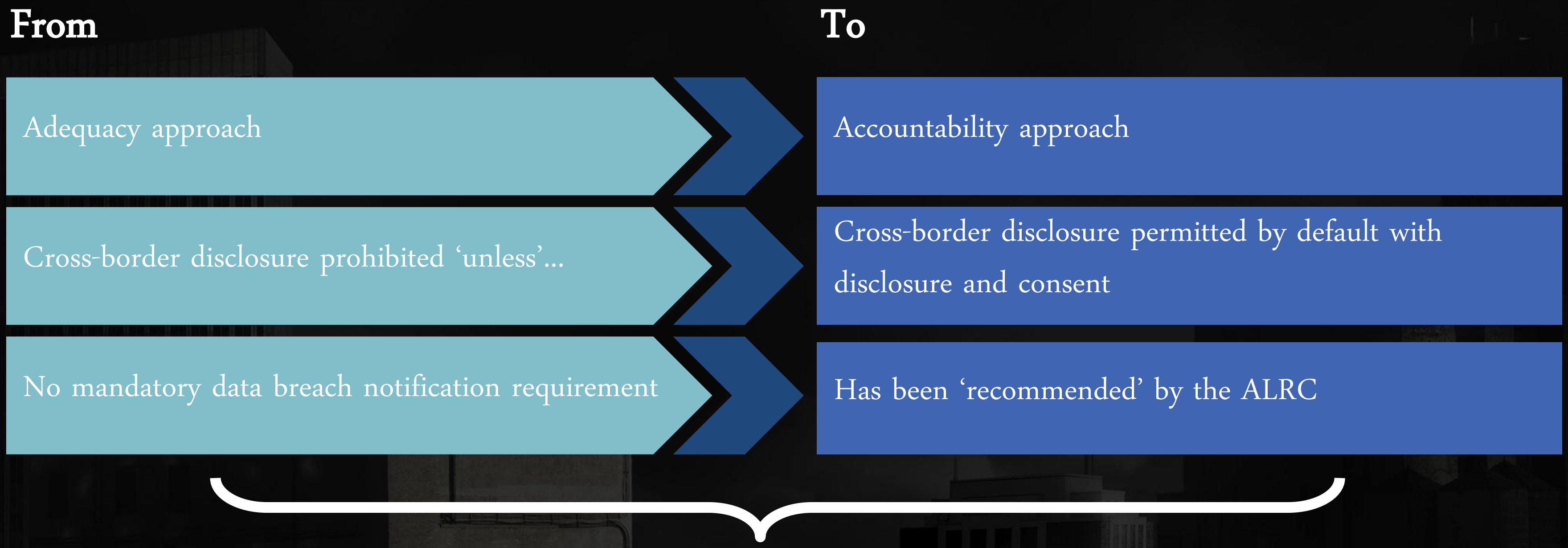
Applies to all organisations with >$3m turn over

Makes Australian entities responsible for cross border data

But the essence of the new act is...

For organisations to handle personal (and sensitive) information in an open and transparent manner.

So which key changes in the Privacy Amendment bill are likely to impact technology?



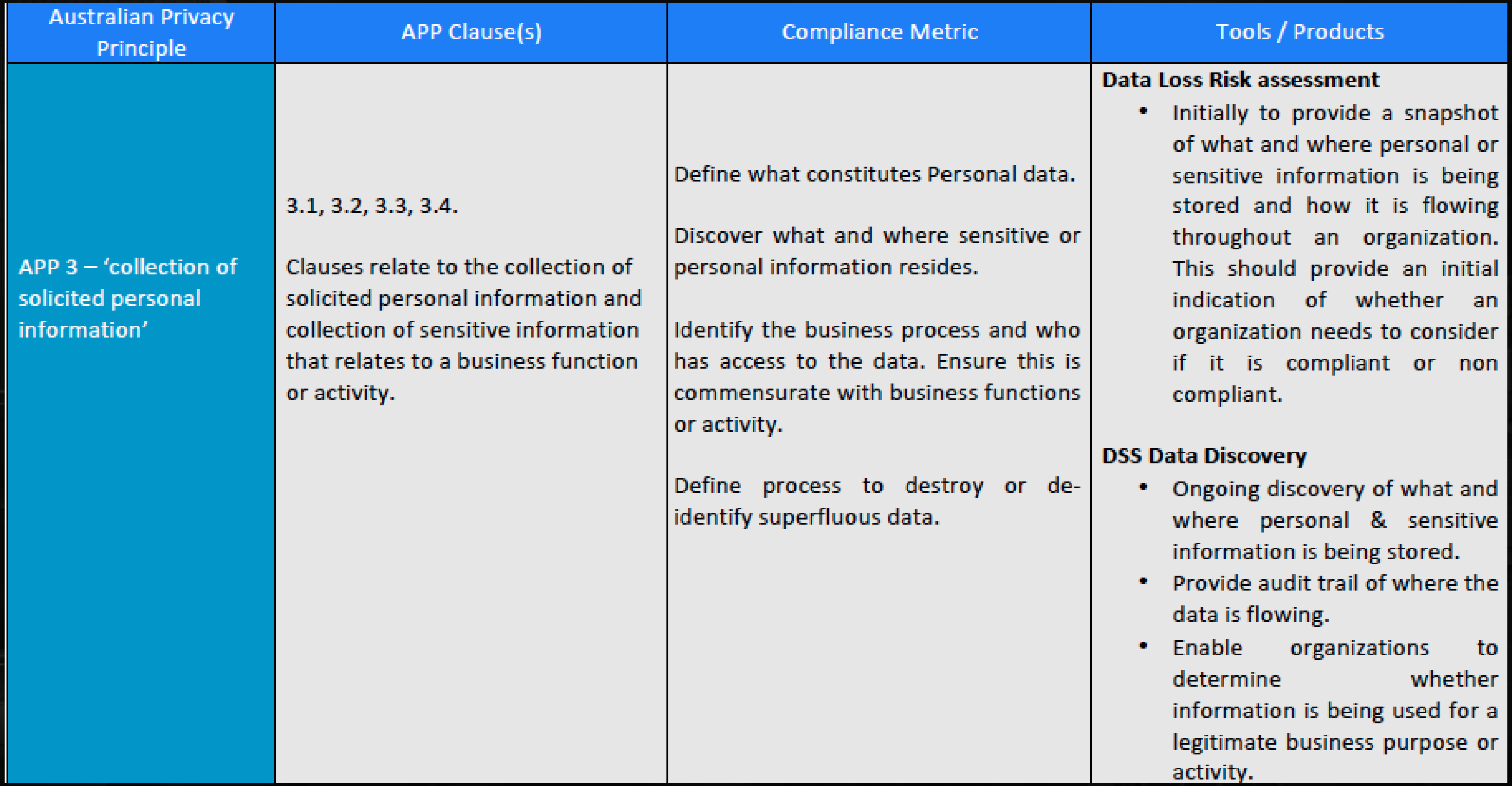
From	To
Adequacy approach	Accountability approach
Cross-border disclosure prohibited ‘unless’…	Cross-border disclosure permitted by default with disclosure and consent
No mandatory data breach notification requirement	Has been ‘recommended’ by the ALRC

Compliance with the APPs requires organisations to know:

- **What** Personally Identifiable Information (PII) is held?
- **Where** it is located?
- **Who** has access?
- **How** it is secured?

And APP's can be mapped to what, where, who and how

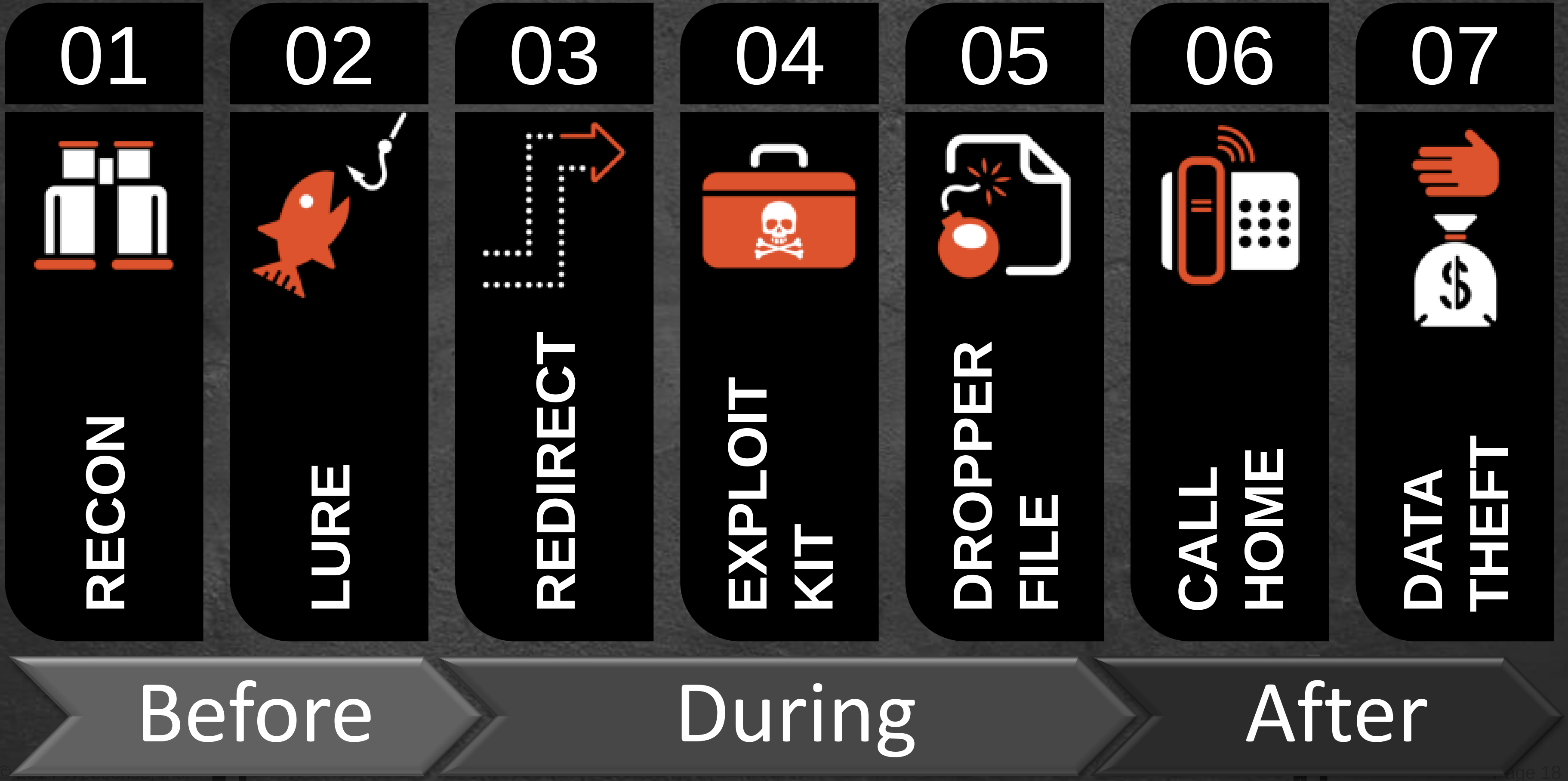
websense TRITON



Australian Privacy Principle	APP Clause(s)	Compliance Metric	Tools / Products
APP 3 – 'collection of solicited personal information'	3.1, 3.2, 3.3, 3.4. Clauses relate to the collection of solicited personal information and collection of sensitive information that relates to a business function or activity.	Define what constitutes Personal data. Discover what and where sensitive or personal information resides. Identify the business process and who has access to the data. Ensure this is commensurate with business functions or activity. Define process to destroy or de-identify superfluous data.	**Data Loss Risk assessment** • Initially to provide a snapshot of what and where personal or sensitive information is being stored and how it is flowing throughout an organization. This should provide an initial indication of whether an organization needs to consider if it is compliant or non compliant. **DSS Data Discovery** • Ongoing discovery of what and where personal & sensitive information is being stored. • Provide audit trail of where the data is flowing. • Enable organizations to determine whether information is being used for a legitimate business purpose or activity.

So what can we do to reduce the risk to our data?

websense TRITON



Combatting Data Theft: Before

websense TRITON

01

RECON

02

LURE

TECHNOLOGY

URL Link Analysis at point-of-click

Anywhere URL Link Analysis/ Roaming/OWA user coverage

Log & Event Correlation

Phish attack reporting

Phishing education

PROCESS

Spear-phish/Social Engineering Assessments

Incident Handling and Workflow

Social Media Monitoring

PEOPLE

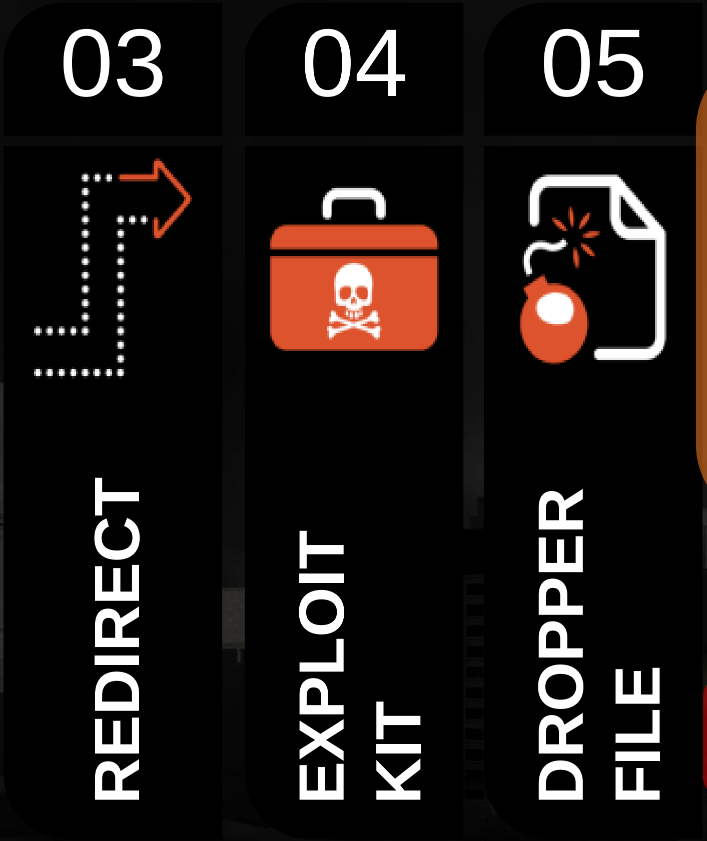
Security/Phishing awareness

Social Media/Web-smart training

Combatting Data Theft: During

TECHNOLOGY

- Real-time Behavioral & statistical analysis
- File Sandboxing
- Content Decryption
- Roaming/off-network user coverage
- Patch Management



03 REDIRECT

04 EXPLOIT KIT

05 DROPPER FILE

PROCESS

- Incident Handling/ Response & Workflow
- Forensic Investigation
- Event Correlation

PEOPLE

- Security Awareness

Combatting Data Theft: After

TECHNOLOGY

Password/SAM DB Detection

Decryption & Custom Encryption

PII, PHI, IP and Sensitive Data

Data Dripping Detection

Optical Character Recognition

Geo-location based policy

PROCESS

Identify & Classify

Incident Handling and Workflow

Forensic Investigation

Event Correlation

Risk Assessment

PEOPLE

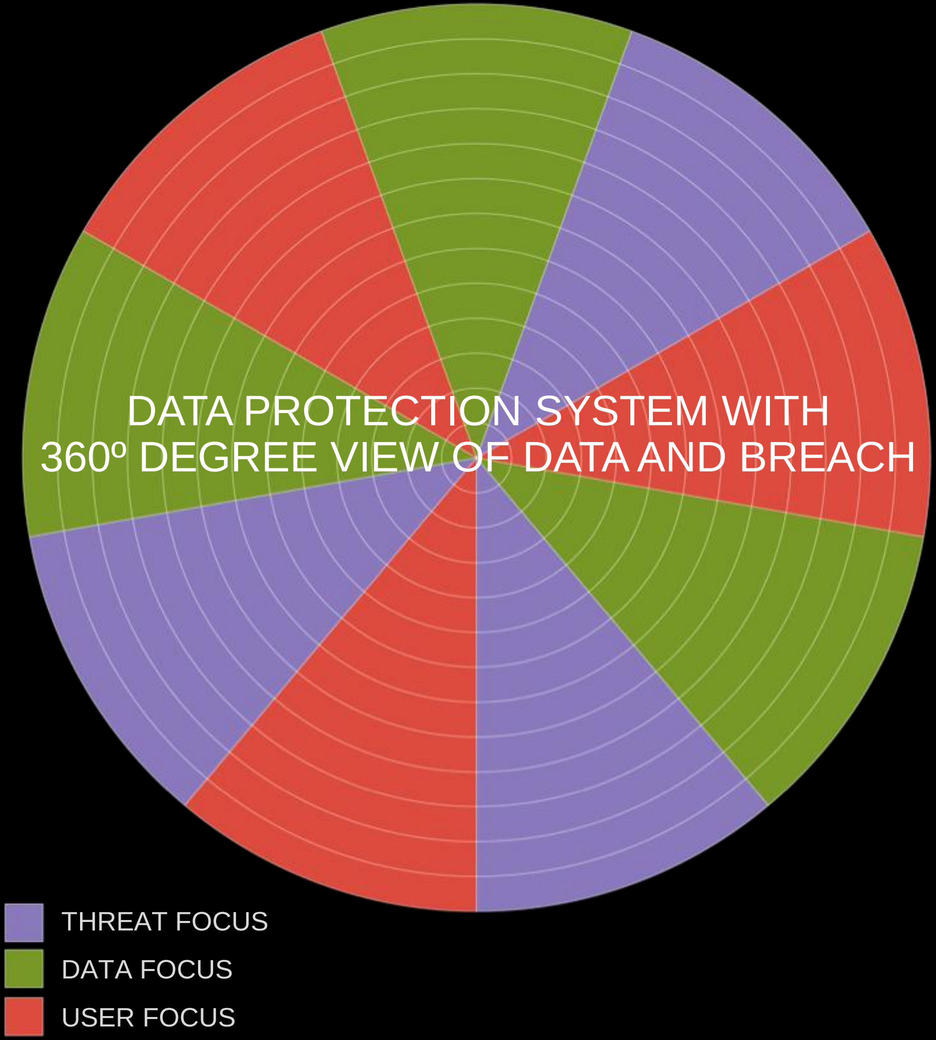
Data-smart education

06

CALL HOME

07

DATA THEFT



USERS: THE NEW PERIMETER

THE FOCUS OF MODERN SECURITY IS SKEWED TOWARDS A PERSPECTIVE THAT LOOKS PRIMARILY AT THREATS.

A CONTEXTUAL UNDERSTANDING OF DATA AND USER BEHAVIOR IS NEGLECTED.

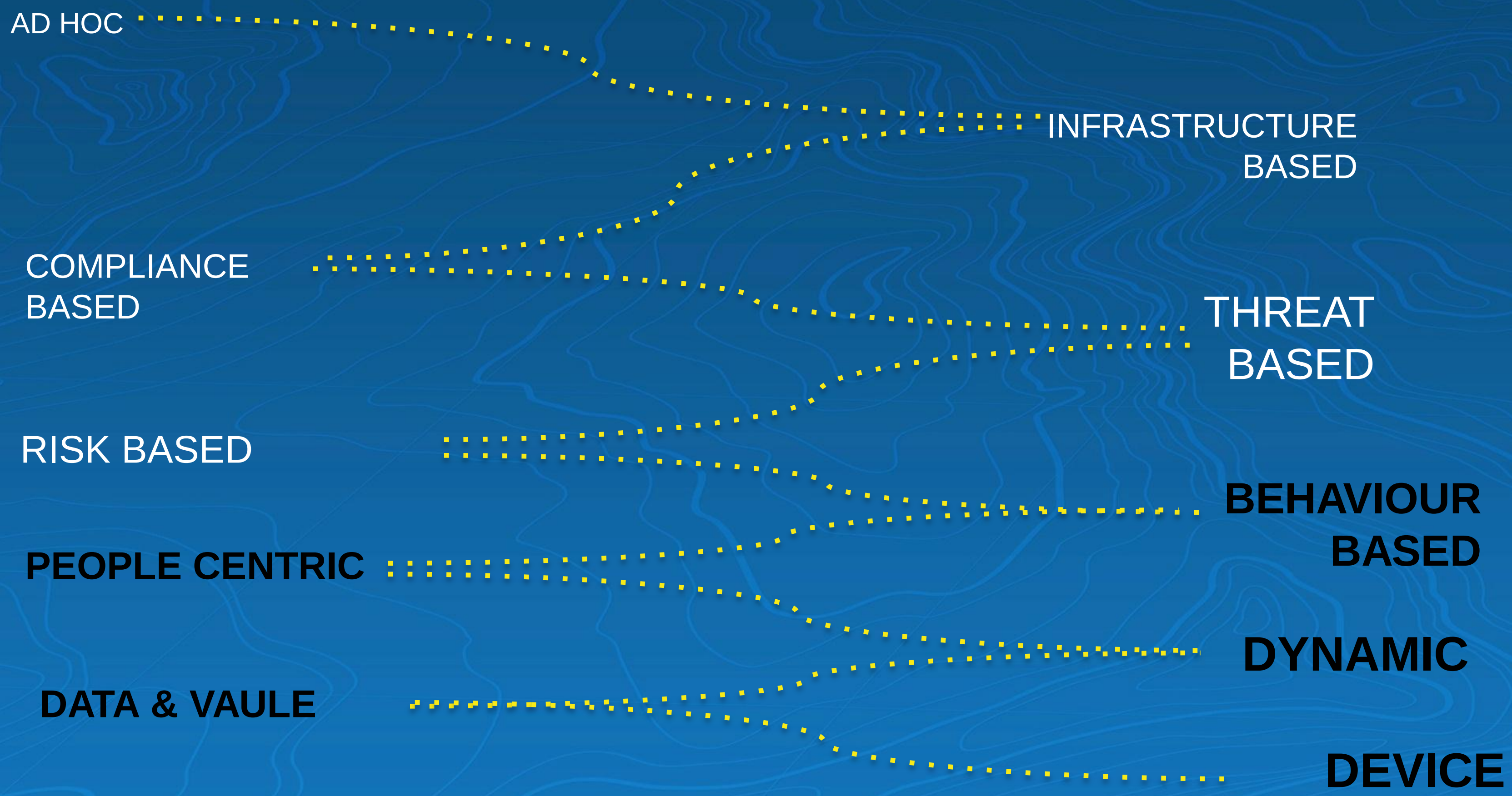
websense®

Company evolution – collaborative flows of data

Business will become fluid and dynamic. Value will come from the flows of information, not in the data assets.

Communicating it & exploiting it faster than other people will be the key business driver.

So the security journey needs to extended…



AD HOC

INFRASTRUCTURE BASED

COMPLIANCE BASED

THREAT BASED

RISK BASED

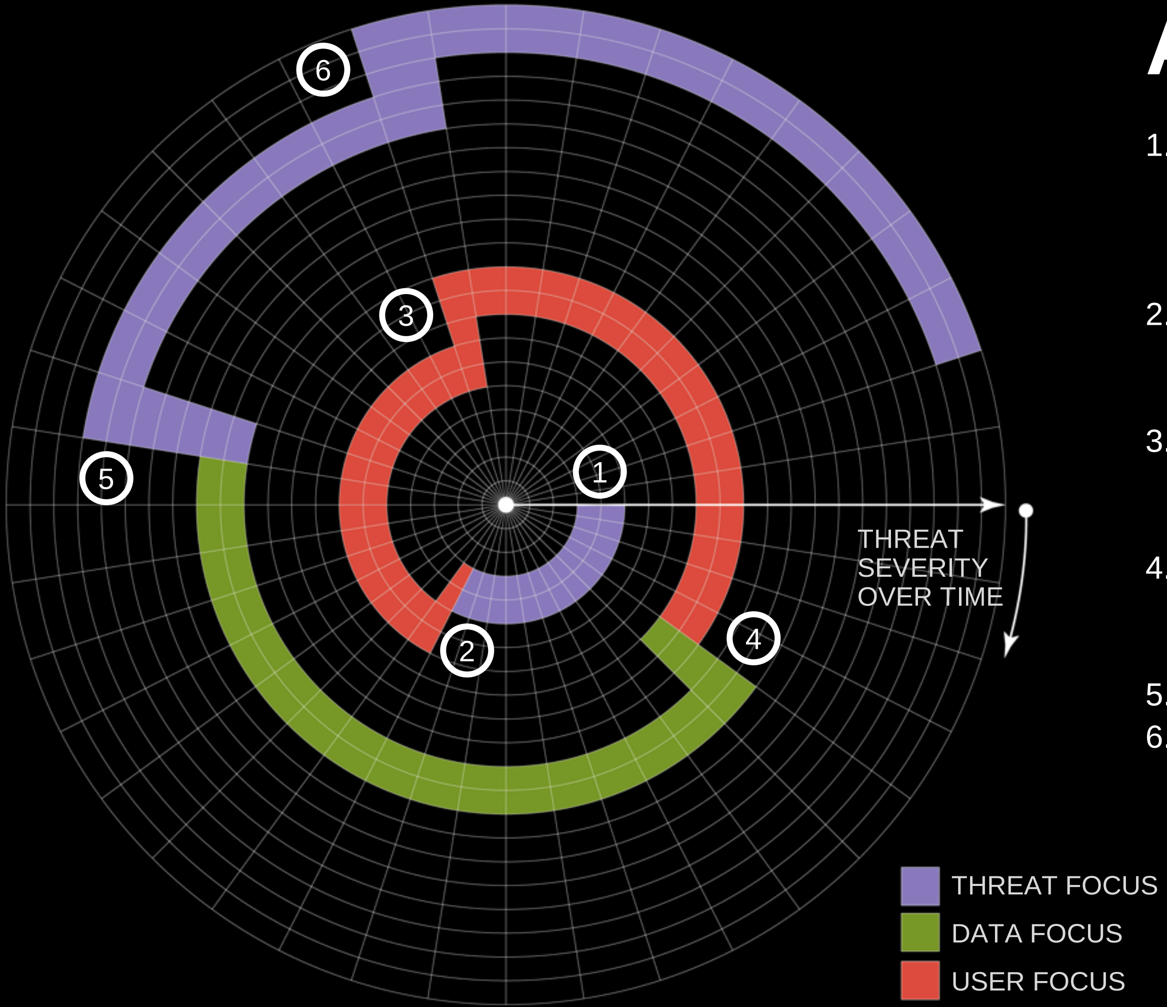
BEHAVIOUR BASED

PEOPLE CENTRIC

DYNAMIC

DATA & VAULE

DEVICE



APT ATTACK:

1. For the last couple weeks we noticed Joe & a few people in engineering was targeted by spear phishing attacks, which we blocked.
2. Last week Joe logged into VPN from a China or new IP address we have not seen before.
3. This week Joe authenticated to a few application he has not accessed in 6 months.
4. Today Joe accessed the source code (this is part of his job, but he normally doesn’t download the entire tree)
5. Joe machine accessed bittorrent sites
6. Noticed Joe’s computer transmitted a large data set externally via bittorrent

And Always end with a quote....

”Procrastination in the name of reducing risk actually increases risk.”

THANK YOU

TRITON STOPS MORE THREATS. WE CAN PROVE IT.