websense

WHO'S TARGETING YOUR SENSITIVE DATA AND HOW?

Gerry Tucker

Regional Director – ANZ

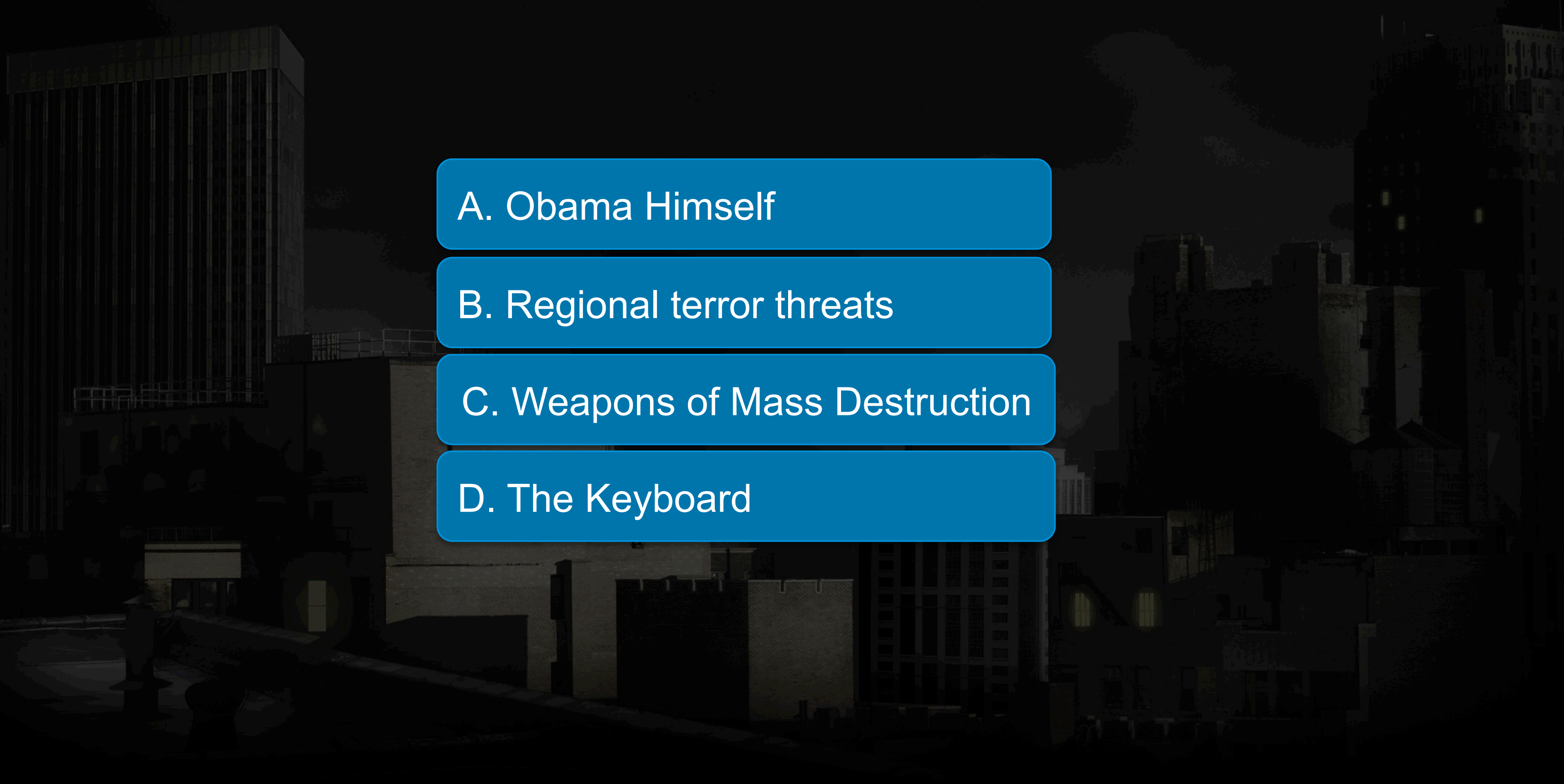
TRITON STOPS MORE THREATS. WE CAN PROVE IT.

websense® TRITON™

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…



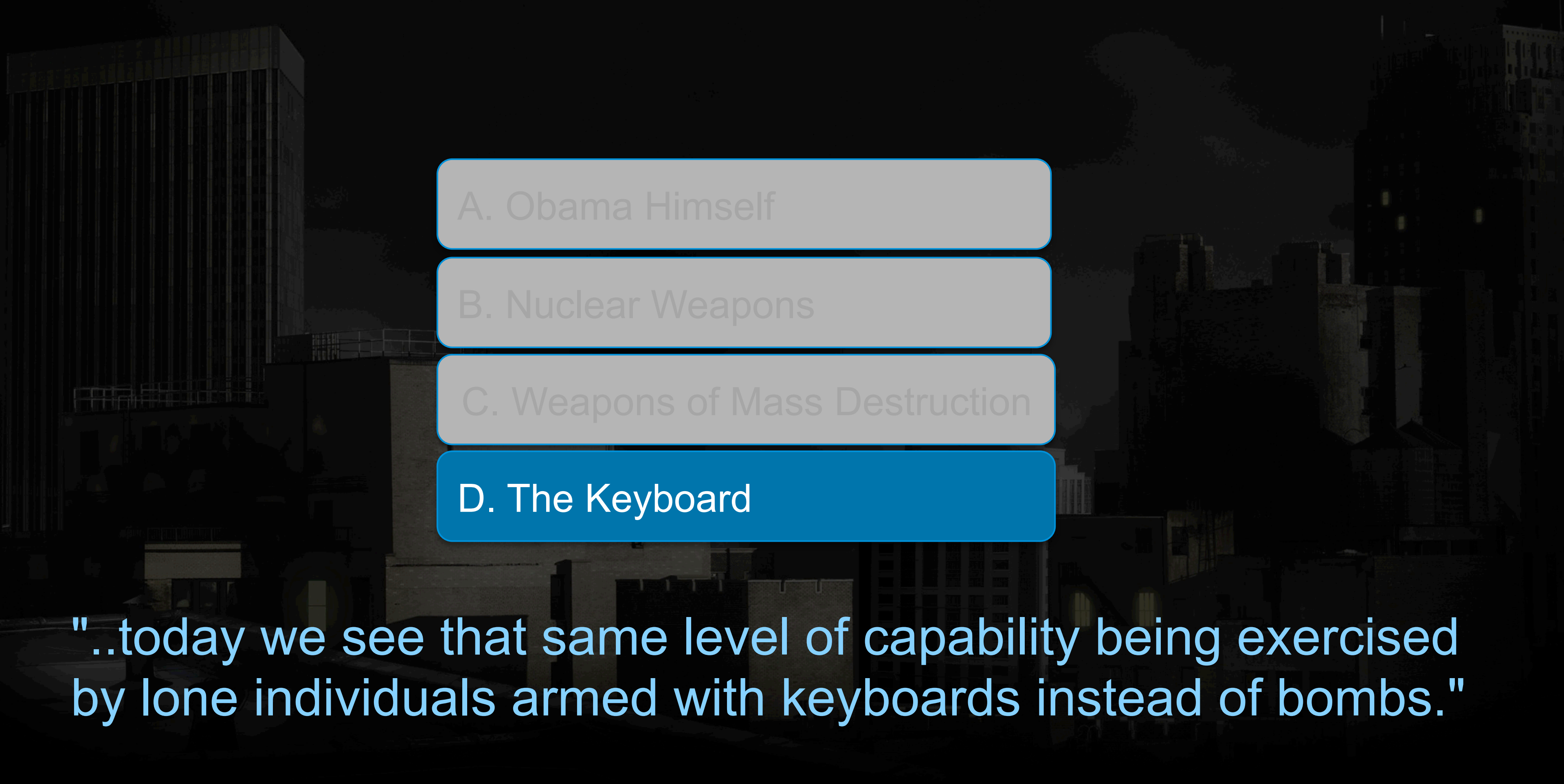
A. Obama Himself

B. Regional terror threats

C. Weapons of Mass Destruction

D. The Keyboard

Answers on a # tag please…



A. Obama Himself

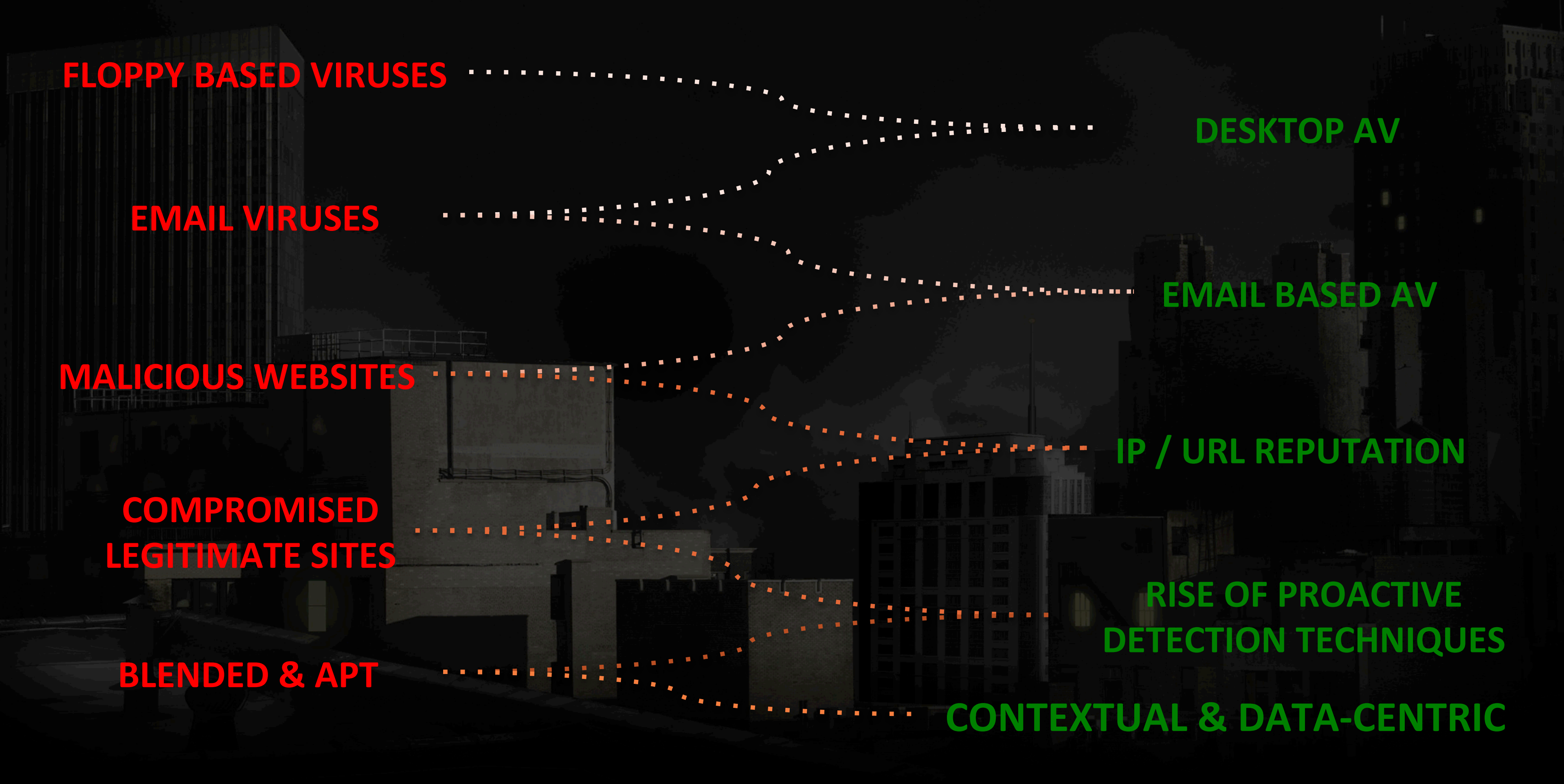
B. Nuclear Weapons

C. Weapons of Mass Destruction

D. The Keyboard

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

Ever changing landscape…



FLOPPY BASED VIRUSES

EMAIL VIRUSES

MALICIOUS WEBSITES

COMPROMISED LEGITIMATE SITES

BLENDED & APT

DESKTOP AV

EMAIL BASED AV

IP / URL REPUTATION

RISE OF PROACTIVE DETECTION TECHNIQUES

CONTEXTUAL & DATA-CENTRIC

Advanced Attacks: Its just another business process

Target Market Research	01	01	RECON
“The Offer”: Email/Social Media campaign or print mail	02	02	LURE
Offer accepted and credentials verified	03	03	REDIRECT
Customer asset access requested	04	04	EXPLOIT KIT
Assets access granted	05	05	DROPPER FILE
Assets researched and registered for acquisition	06	06	CALL HOME
Assets acquired and transferred	07	07	DATA THEFT

For example: Target Corp – Late 2013

websense TRITON

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

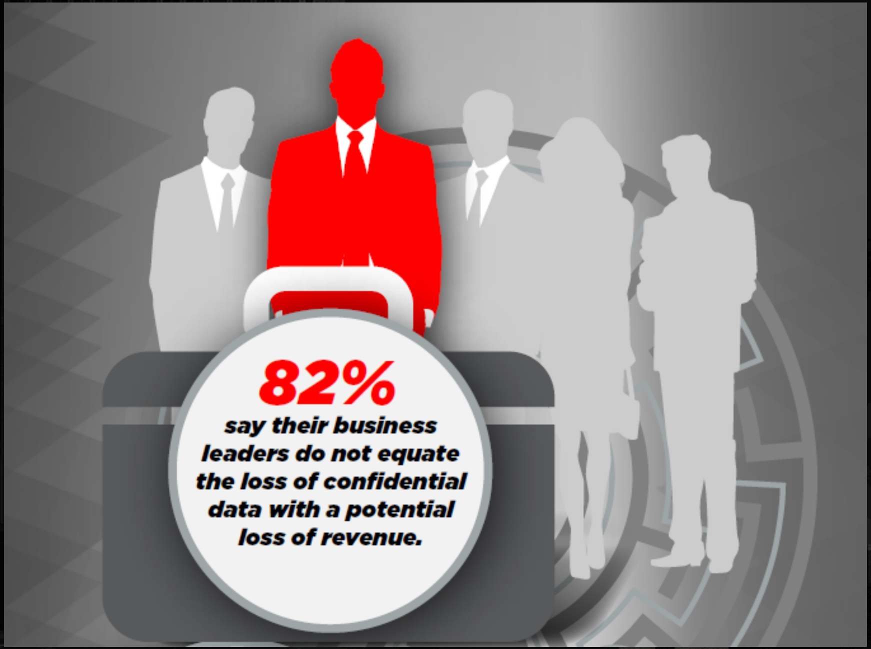
A constant stream of updates and instructions. Attackers performed a 'test run' of BlackPOS in early Nov, before going 'live' in Dec

13

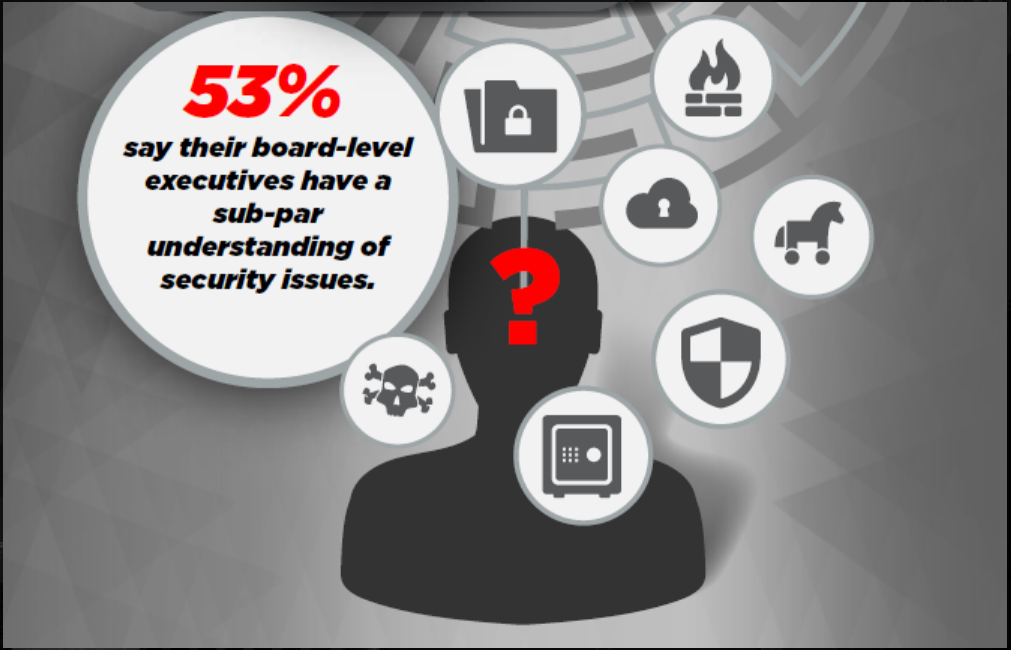
Financial records of over 110M customers, including 40M customer CCNs, uploaded to servers in Russia, Brazil and Miami

Why these attacks happen from a CISO Perspective

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.

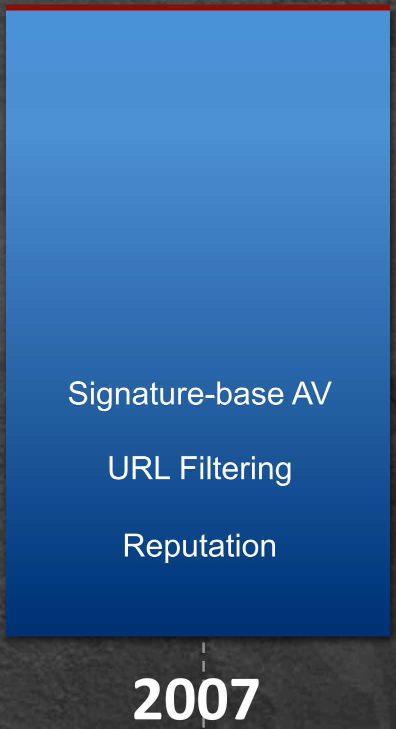
Why current solutions fail

Reactive Security Controls

Security vendors need to see, analyse, create signatures and update their customers before being able to block…

Technology examples:-

- *URL Filtering*
- *IP Reputation*
- *AV Scanners*
- *IDS/IPS Solutions*
- *Application Firewalls*



Signature-base AV

URL Filtering

Reputation

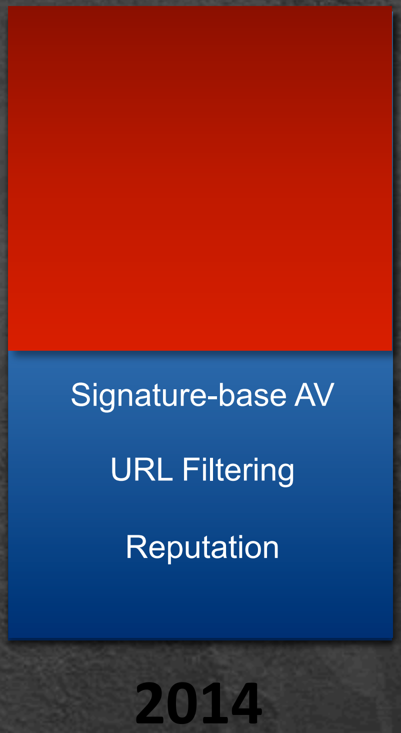
2007

3% **Malware Gap**

97% **Covered by Legacy Security Technologies**

Why current solutions fail…

- ***“Signature based tools are only effective against 30-50% of current security threats, this effectiveness is expected to decline rapidly.” – IDC***
- ***“In 2013 85% of malicious content was found on compromised legitimate websites.”***
- ***“4.1 billion live attacks were prevented by Websense in 2013. Nearly all exhibited techniques to bypass traditional defenses”***



60% **Malware Gap**

What Has Changed?
- Malware has become more:
- Dynamic
- Prolific
- Stealth
- Targeted

40% **Covered by Legacy Security Technologies**

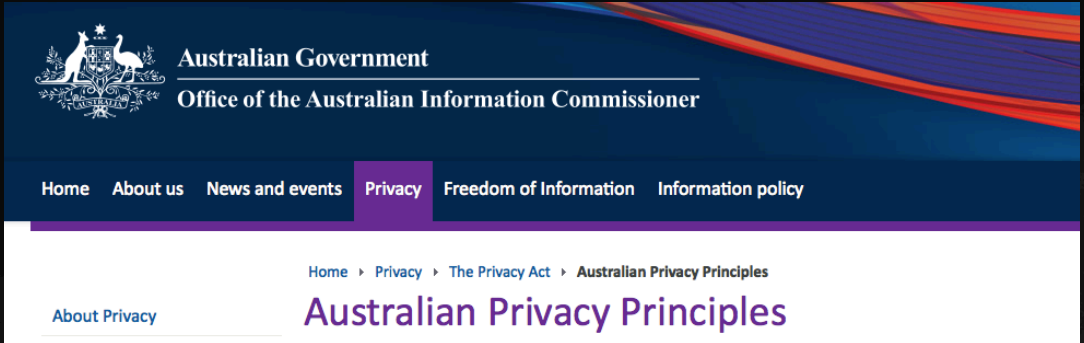
So where do we see the risk to Data Security today?

Broken Business Processes

Insider Threat

Malicious Threats

So what about Privacy ...



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.

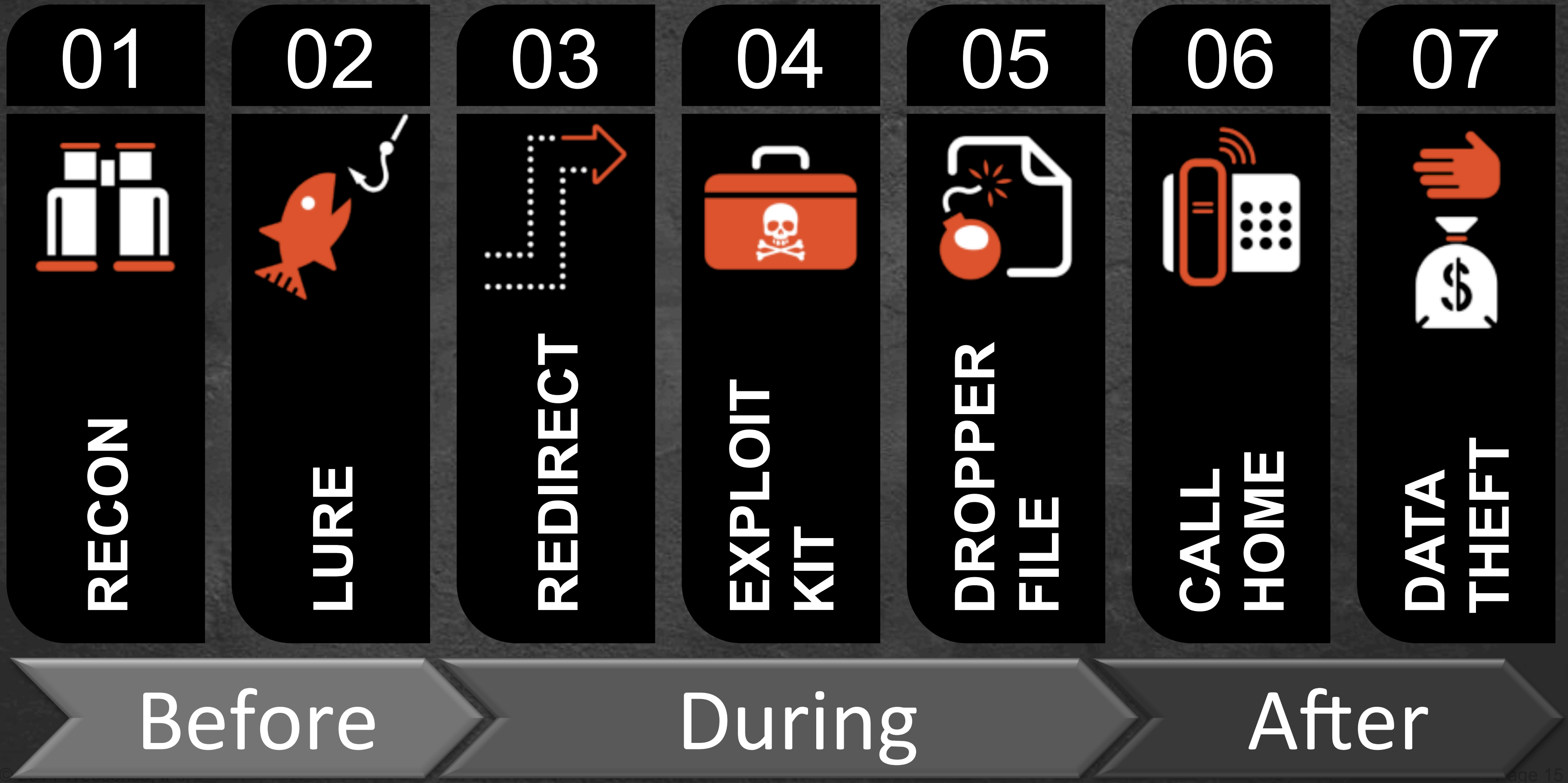
Applies to all organisations with >$3m turn over

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



01 RECON

02 LURE

03 REDIRECT

04 EXPLOIT KIT

05 DROPPER FILE

06 CALL HOME

07 DATA THEFT

Before

During

After

Combatting Data Theft: Before

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

websense TRITON

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

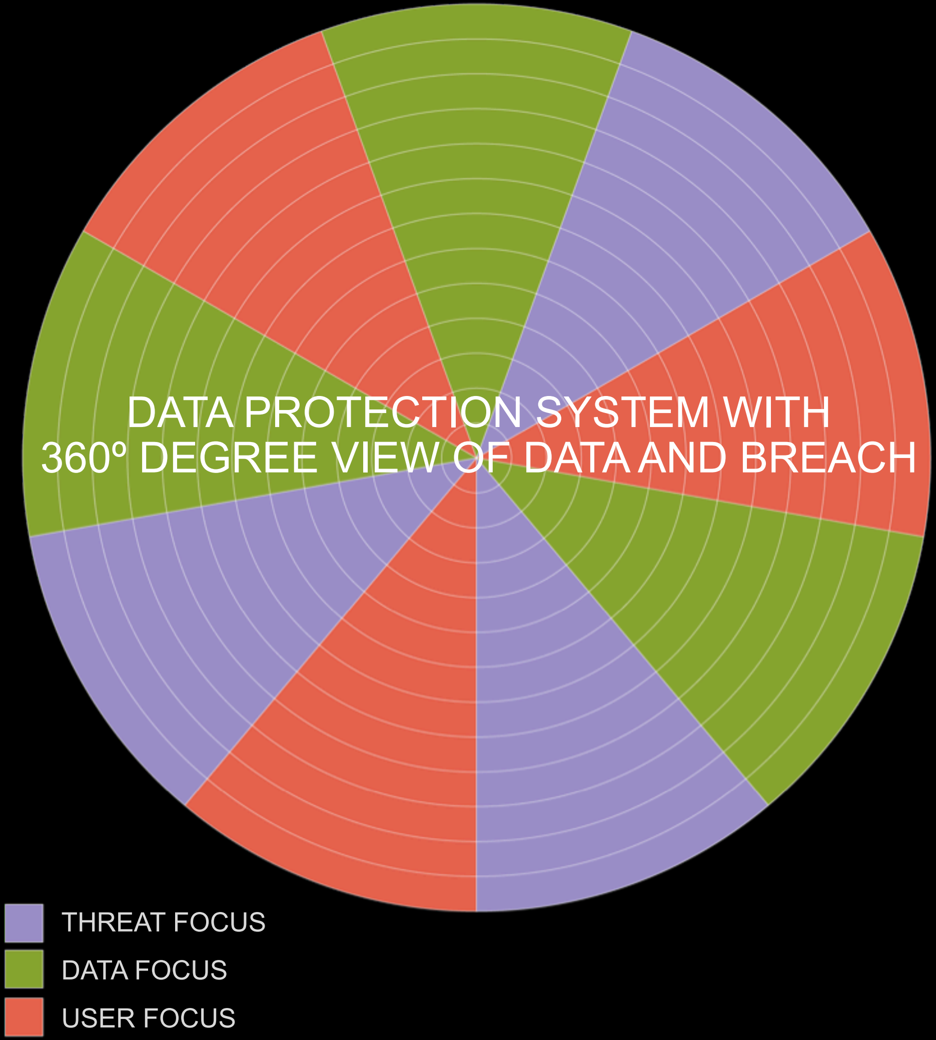
Risk Assessment

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.

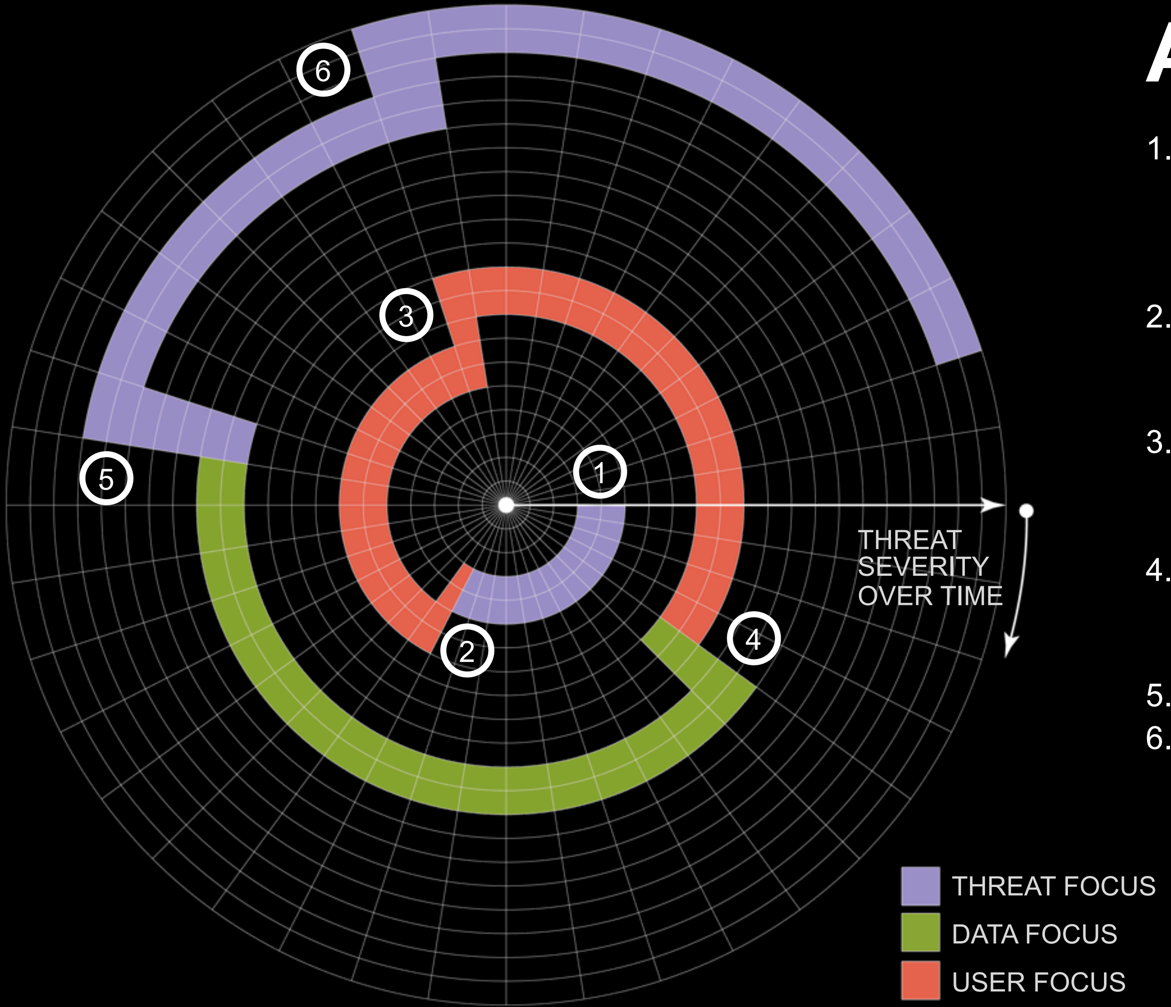
A CONTEXTUAL UNDERSTANDING OF DATA AND USER BEHAVIOR IS NEGLECTED.

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.



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

websense®

How can you protect your organisation?

- FREE Data Loss Risk Assessment
- Websense first focuses on what’s most critical within your business. Data is analysed as it enters, moves around and leaves the network so that policy breaches can be identified through the web or email channel.
- Websense works with your organisation to identify these critical data types and build policies to suit your requirements.
- www.websense.com/freeriskassessment

THANK YOU

TRITON STOPS MORE THREATS. WE CAN PROVE IT.