September 2018

Cross-Sector Threat Intelligence Sharing

An Australian Perspective

pwc

It all started such a long time ago - (in a land far, far away) .....

A brief discussion of relatively ancient history

2009

1st Australian Cyber Security Strategy is released

2010

CERT Australia and CSOC commence operations

2014

Australian Cyber Security Centre launched

2013: a first attempt

The story from business

- Government won't share the good stuff
- They're too slow
- Classification & clearance gets in the way
- The information isn't actionable - what am I supposed to do with a "bad IP"?

2013: a first attempt

The story from government

- They aren't mature enough for what we've got
- Security is important, we often get our intel from sharing partners and have to keep classification in mind
- They never share anything back to us or let us know how they use it

2013: a first attempt

We failed to come together

- The moment wasn't right
- We didn't make the right case
- Companies and Government blamed each other

It took time, but the environment changed


AUSTRALIA'S
CYBER SECURITY STRATEGY

61%

of Australian CEOs were concerned about Cyber threats in 2014

Source: PwC's 18th Global CEO Survey.

80%

of Australian CEOs were concerned about Cyber threats by 2016

Source: PwC's 20th Global CEO Survey.

Industry was ready to answer the Prime Minister's challenge


Welcome
to...


TISC

The participants

A large Telco

One of Australia's big four banks

Another one of Australia's big four banks

One of Australia's largest logistics companies

Australia's largest professional services firm

A large insurer

An airline

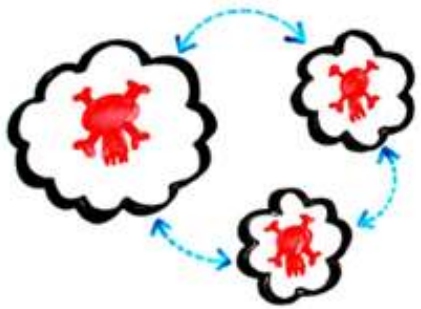
A mining & resources company

A fast moving consumer goods (FMCG) company

THE CASE FOR SHARING...

THE CYBERCRIME BUSINESS MODEL IS THRIVING...

SHARING IS HOW WE CAN DISRUPT IT



25% OF CYBER ATTACKERS CLAIM THE NUMBER 1 REASON FOR THEIR SUCCESS IS INCREASED COLLABORATION...

39% OF ATTACKS WOULD HAVE BEEN HINDERED BY EFFECTIVE INTELLIGENCE EXCHANGE ACROSS COMPANIES...

CYBER ATTACKERS SHARE INFORMATION...

...AUSTRALIA SHOULD TOO.

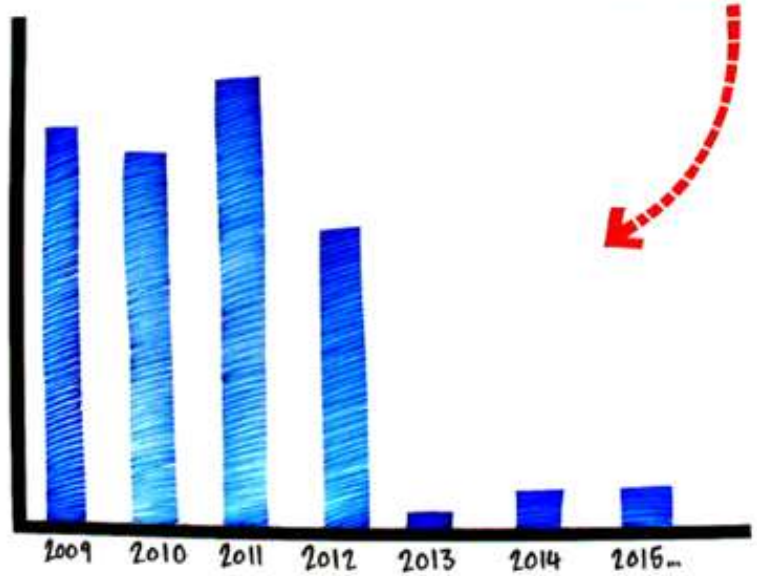
A SURVEY OF INFORMATION SECURITY LEADERS FOUND:

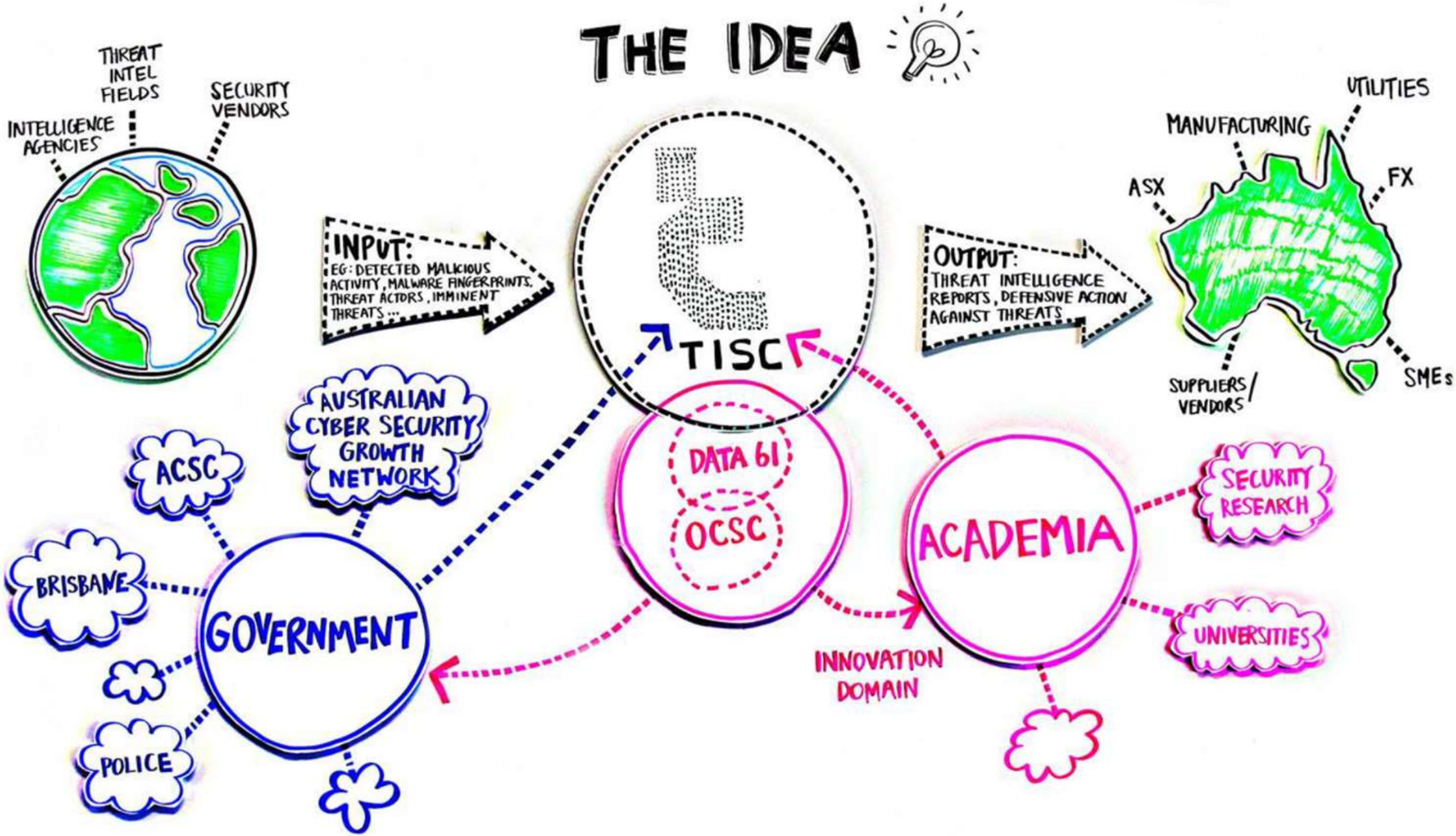
63% NOTED THAT SHARING INTELLIGENCE IMPROVES VISIBILITY INTO ATTACK TYPES...

51% SAW SHARING INTELLIGENCE LED TO FASTER AND MORE ACCURATE DETECTION AND RESPONSE...

48% CITED REDUCTION IN INCIDENTS THROUGH EARLY PREVENTION...

EXTENT OF COMPROMISE OF THE FEDERAL GOVERNMENT




THE IDEA
THREAT INTEL FIELDS
INTELLIGENCE AGENCIES
SECURITY VENDORS
INPUT:
EG: DETECTED MALICIOUS ACTIVITY, MALWARE FINGERPRINTS, THREAT ACTORS, IMMINENT THREATS ...
TISC
OUTPUT:
THREAT INTELLIGENCE REPORTS, DEFENSIVE ACTION AGAINST THREATS
UTILITIES
MANUFACTURING
ASX
FX
SUPPLIERS / VENDORS
SMEs
AUSTRALIAN CYBER SECURITY GROWTH NETWORK
ACSC
DATA 61
OCSC
ACADEMIA
SECURITY RESEARCH
BRISBANE
GOVERNMENT
UNIVERSITIES
INNOVATION DOMAIN
POLICE

We were looking for more

The proposed JCSC:

- Led by the Government
- Advisory board
- Manual online web platform
- Dedicated staff

The proposed TISC:

- Led by the private sector
- Governance board
- Automated sharing platform
- Dedicated staff

We came together

A unified vision

- JCSCs would adopt the TISC ideas
- Government funded
- Private sector led governance boards
- Automated sharing / platform would come later
- Dedicated staff, plus co-location of partner company staff at sites in each major city

ACSC – 16 August, 2018

A lot has been achieved -
but there is so much more to do

Ongoing developments

ASD now an Executive Agency

ASD used to be a part of the Defence Department, but now reports directly to the Minister, giving them more independence to pursue their mission.

New location/building

The Australian Cyber Security Centre moved out of the highly restricted building it shared with the rest of ASD and into a multi-security zone building to enhance collaboration with industry

ACSC new leadership

The Prime Minister's Cyber Special Advisor was appointed as head of ACSC, giving him operational control of the Government's defensive cyber capability

We’ve still got work to do

Long term

- Our progress has not yet given the CEOs comfort that we are doing enough
- ACSC as an independent agency?

Short term

- We are still behind on automated sharing
- We need to do more to systematise the relationships that are the foundation for trusted sharing

89%

of Australian CEOs are concerned about cyber threats.

Source: PwC’s 21st Global CEO Survey

1 – This is a Team Event

2 – Cultural Change

3 – Need for Speed!

Thank you

pwc.com