RSA Conference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: **ECO-T09**

Leveraging Global Threat Intelligence: Raising the Cost of Cyber-Warfare

Dean Thompson
(Dean.Thompson@anz.com)

Senior Manager, Global Threat Intelligence & Advanced Response
Australia and New Zealand Banking Group Limited

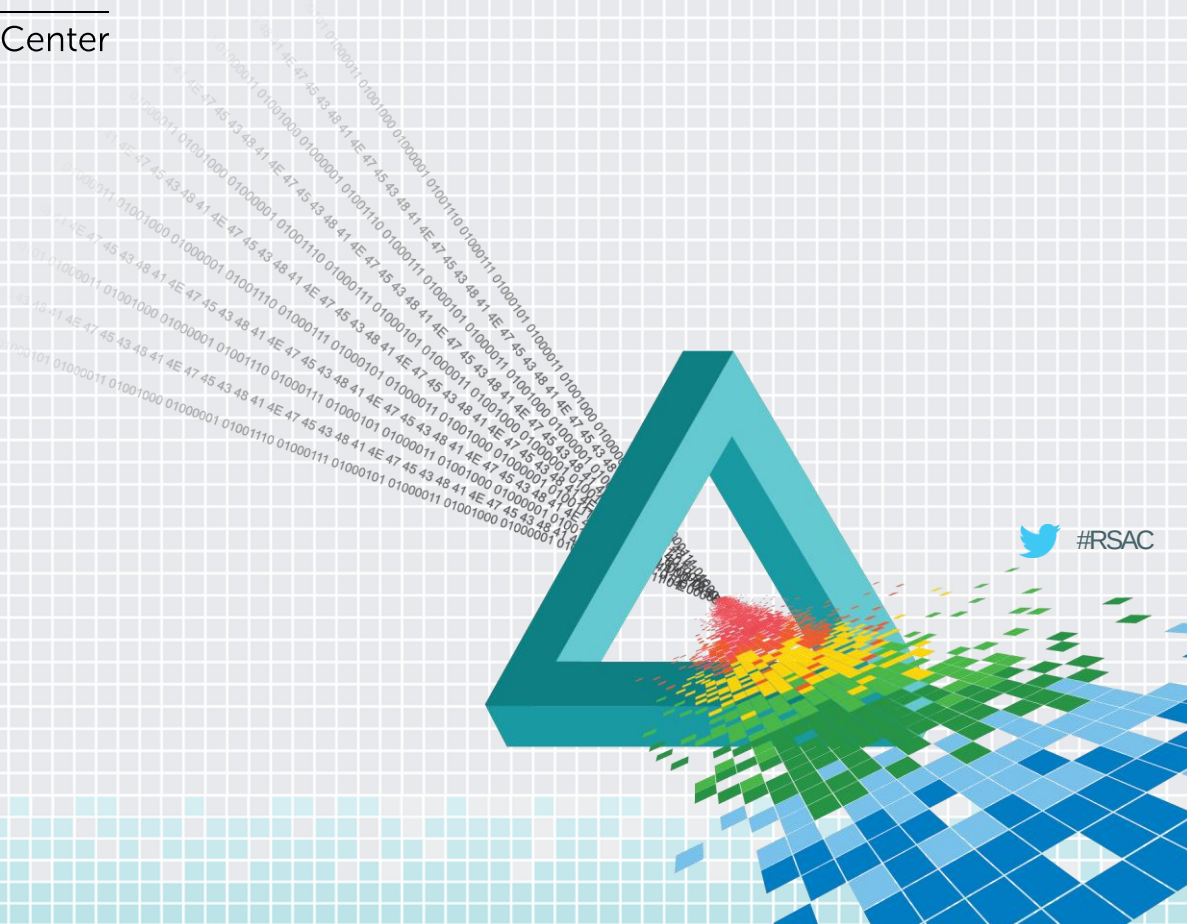
Agenda

- Introductions
- Sophistication of Actors vs Tools over Time
- Modus Operandi
- Operational Environment
  - Considerations for ANZ
  - Problems faced within ANZ and Globally
- Harnessing the power of the community
  - Benefits
  - Limitations
- What needs to change / Your in the driver seat
- Parting thoughts …

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Introductions



Introductions – Dean Thompson

- Senior Manager, Global Threat Intelligence & Advanced Response
- Manager, Global Security Operations Centre
  - 24 x 7 Computer Security Incident Response Team
  - Respond to all sorts of Computer Security Incidents
  - Forensic / Boutique / Delicate Security Incidents
  - Technical Subject Matter Experts (SME's)

- Assisted with the Cyberstorm II & Cyberstorm III scenarios for Australia
- PhD (Computer Science) -- Monash University, Australia
- Security / Network Engineering background
- Systems Administrator & Developer

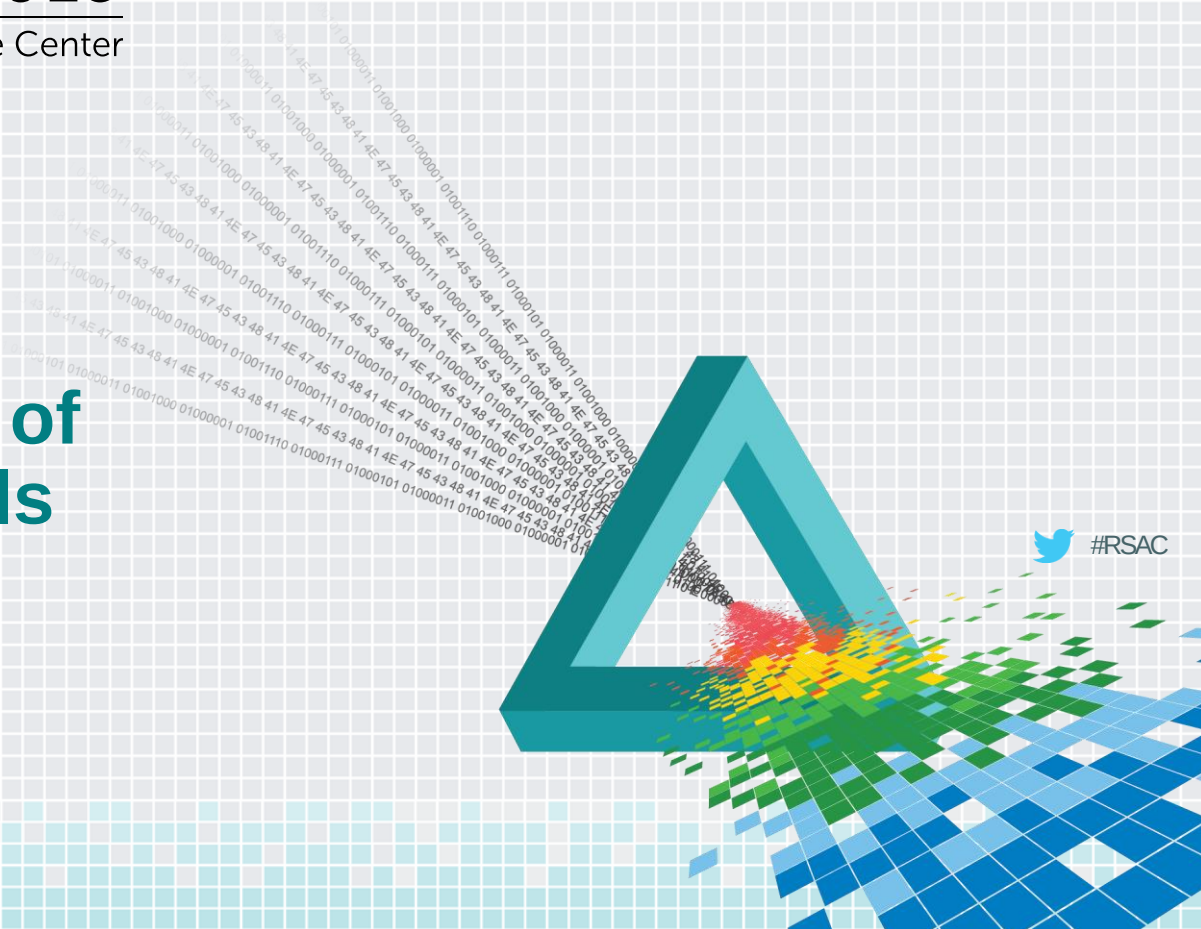
Introductions – ANZ Bank

- World headquarters located in Melbourne, where it first opened as an office of the Bank of Australasia in 1835
- Assets of $772.10 (AUD) billion / Profit $7.27 (AUD) billion (Sep 2014)
- 1,220 worldwide points of representation
- 486,596 shareholders (Sep 2014)
- 50,824 employees worldwide
- Super regional bank with a specific focus on Asia

RSAConference2015

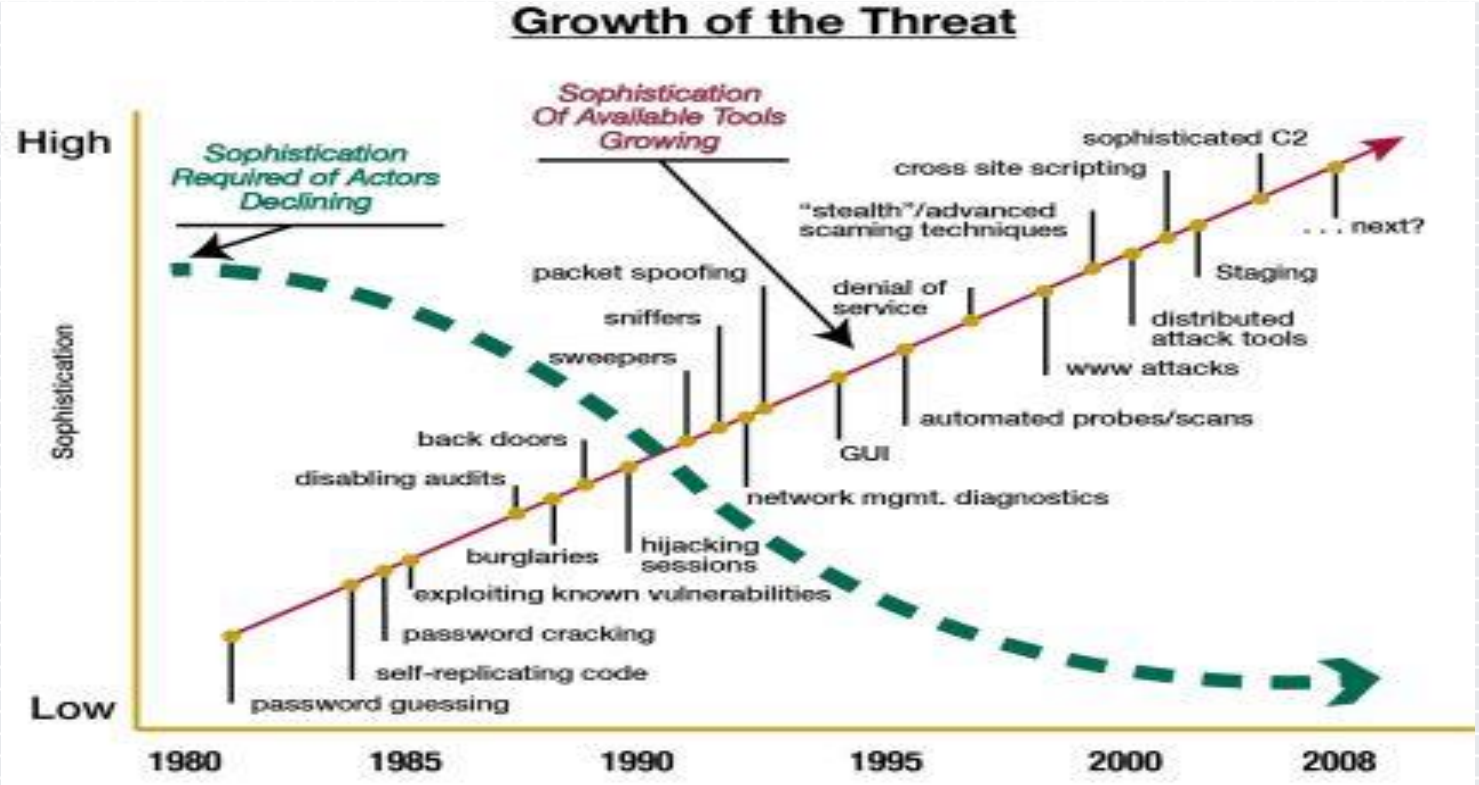
San Francisco | April 20-24 | Moscone Center

Sophistication of Actors vs Tools over Time



#RSAC

Sophistication of Actors vs Tools over Time



Source: Booz Allen Hamilton. www.boozallen.com

Implications of Sophisticated Attack Tools and the lack of Sophistication to use them

- Imbalance exists with the Return On Investment (ROI) proposition for cyber-criminals vs. organisations
- Organisations spend large amounts on security infrastructure and threat intelligence (% of their overall budget) on trying to equalise the equation
- Regardless of these investments by numerous companies, there have still been breakdowns in security controls:
  - JP Morgan Chase
  - Sony Pictures Entertainment
  - Home Depot
  - Anthem

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Modus Operandi

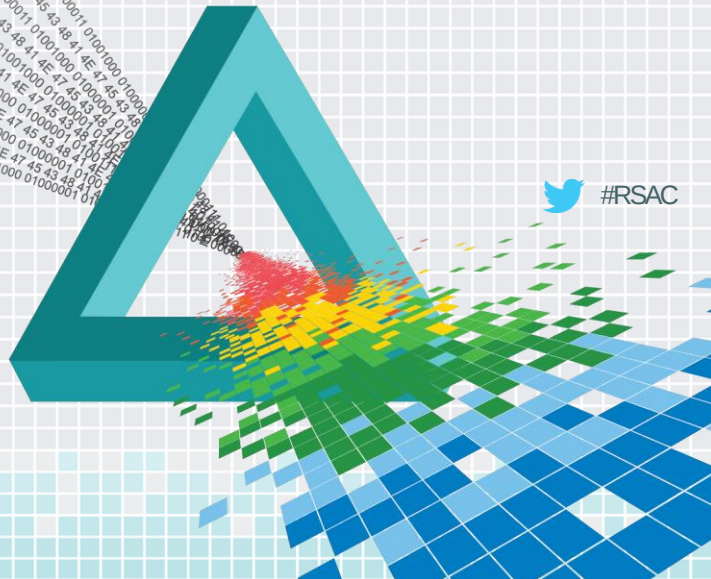
Modus Operandi / Threat Actor Groupings

- Criminals
- Hacktivists
- Information Gathering / Espionage
- War / Kinetic

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Dealing with the Threat Landscape @ ANZ



#RSAC

Back to ANZ Bank

- Operate across 33 markets and have 28 regulators to appease
- Tightest Regulator we deal with: Monetary Authority of Singapore (MAS)
  - Impose tight limits on banks reporting security incidents
    - Definition of security incidents becomes interesting
    - Timelines to report these incidents extends to hours with root cause having to be identified within days
- Banking Operations within:
  - China
  - Hong Kong
  - Taiwan

What does this mean to ANZ ?

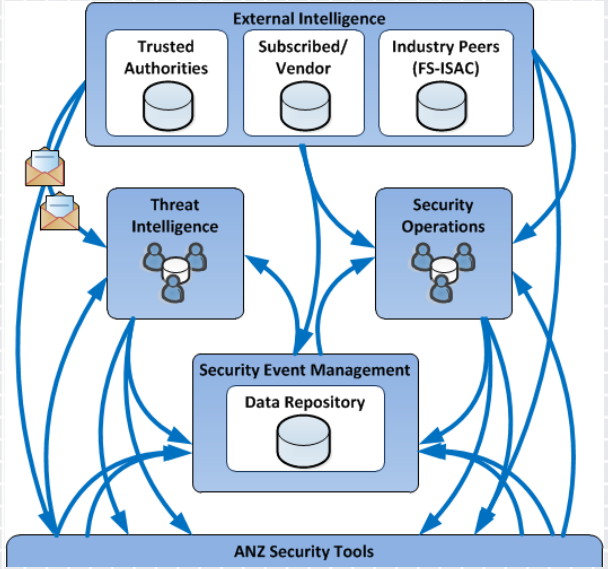
- Operate in a challenging environment
- Geographically positioned in some interesting places across the world
- Consequently, our environment is large and prone to be subjected to various levels of badness from various sorts of actors

What does this mean to ANZ ? (cont.)

- Operate within the confines of various regulations and regulators
  - Some have preconceived ideas, outdated security models and theories
- Signature-based detection does not always work
  - We observe threats before signatures are available to detect them
  - Threats are polymorphic and obscured so straightforward detection doesn't work

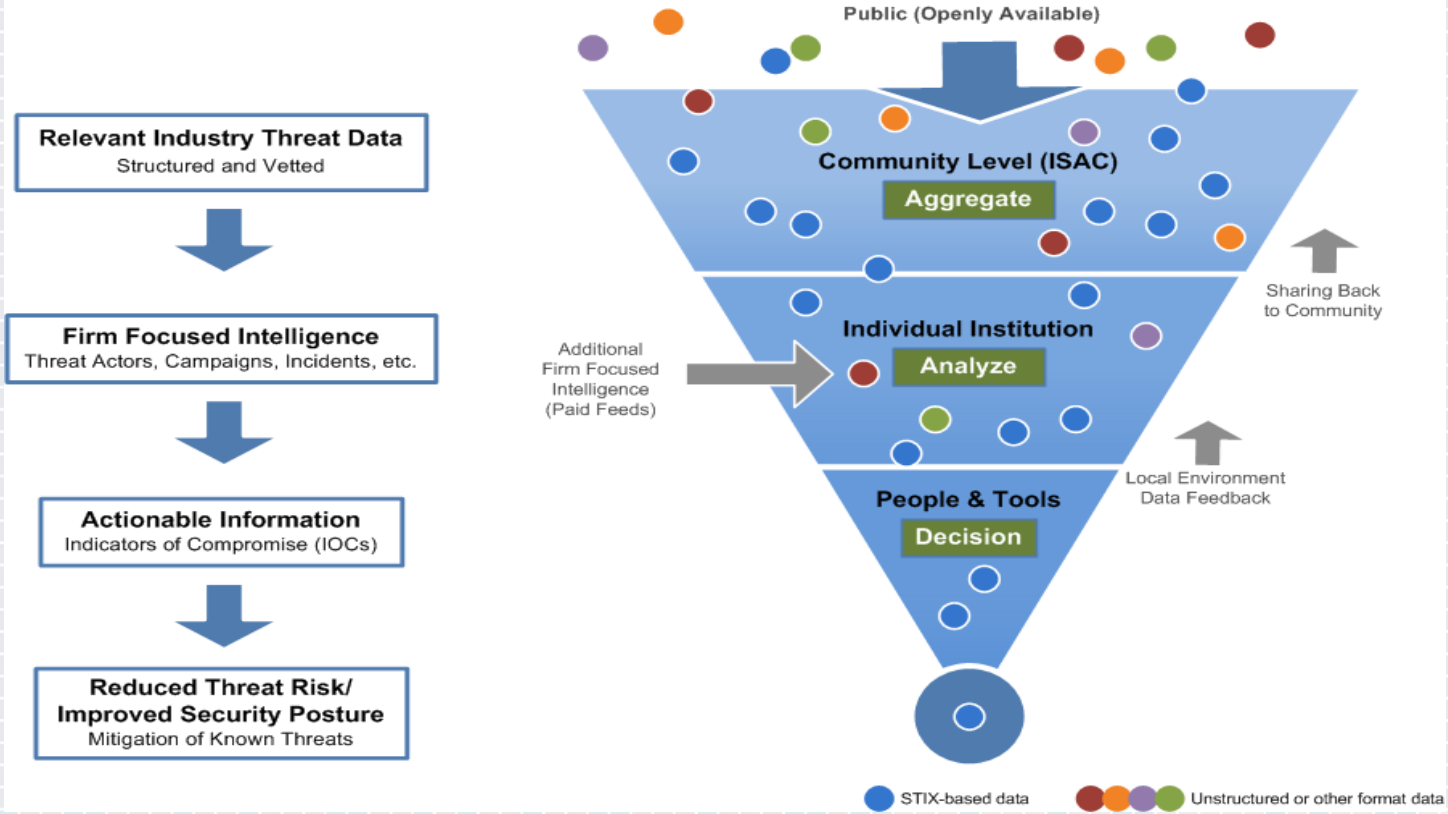
Problems faced by ANZ and others

- We have a number of security tools and products
  - Each of these tools provide a high level of intelligence output
  - Issues we initially faced
    - Data is present within the environment
    - Data flows everywhere and is often duplicated
    - Transmitted without any context
    - Not being used effectively
- We need to respond quickly to threat intelligence
  - Both internally and externally
  - It needs to be actionable intelligence that we can use in our environment



Source: ANZ Security Threat and Vulnerability Strategy (2014)
Author: Steven Mond

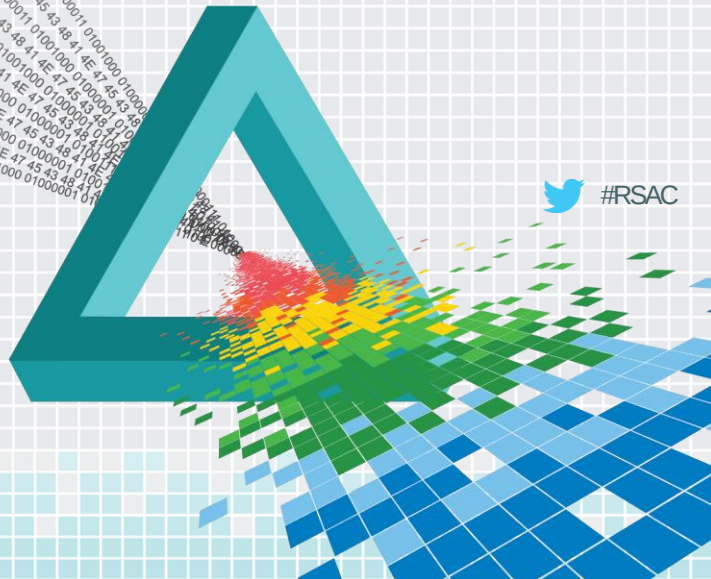
Problems faced by ANZ and others (cont.)



RSAConference2015

San Francisco | April 20-24 | Moscone Center

Dealing with the Threat Landscape Globally



#RSAC

Problems faced more globally

- Return On Investment (ROI) for cyber-criminals is high
- Return On Investment (ROI) for organisations is low
- Organisations have to invest a considerable amount to defend themselves (and in some cases that still isn't enough)
- To balance the equation
  - Need to work more closely with one another
  - Share data and information with context within trust groups to further defend against these threats

Problems faced more globally (cont.)

- We need to work as a community
- Reverse the ROI equation
  - Make it harder for cyber-criminals to attack organisations
  - Tip the balance in our favour
- Adopt Knowledge Hierarchy
  - Companies have data
  - Valuable when pooled together with others' data
  - Data becomes information

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Addressing Threat Landscape Issues @ ANZ

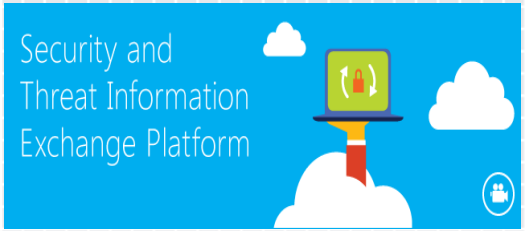
#RSAC

ANZ's approach to the problem

- Establishment of a Cyber-Threat Intelligence Repository
  - We use Soltra's Edge platform for this repository (but there are others available)

SOLTRA

CRITS



- Expression of Cyber-Threat Intelligence in STIX notation
  - Enforces a common standard for the representation of cyber-threats
  - Use of known definitions and relationships allows consumers of the information to understand the meaning and intent of that being expressed

STIX™

ANZ

ANZ's approach to the problem (cont.)

- Establishment of a Cyber-Threat Intelligence Repository
  - Assists with providing information and knowledge
  - Most importantly it provides 'context' to our Security Operations Centre
- Integration of Cyber-Threat Intelligence Repository
  - Global Threat Intelligence & Advanced Response Group
  - Security Operations Centre
- Streamline flow of information from tools within the environment

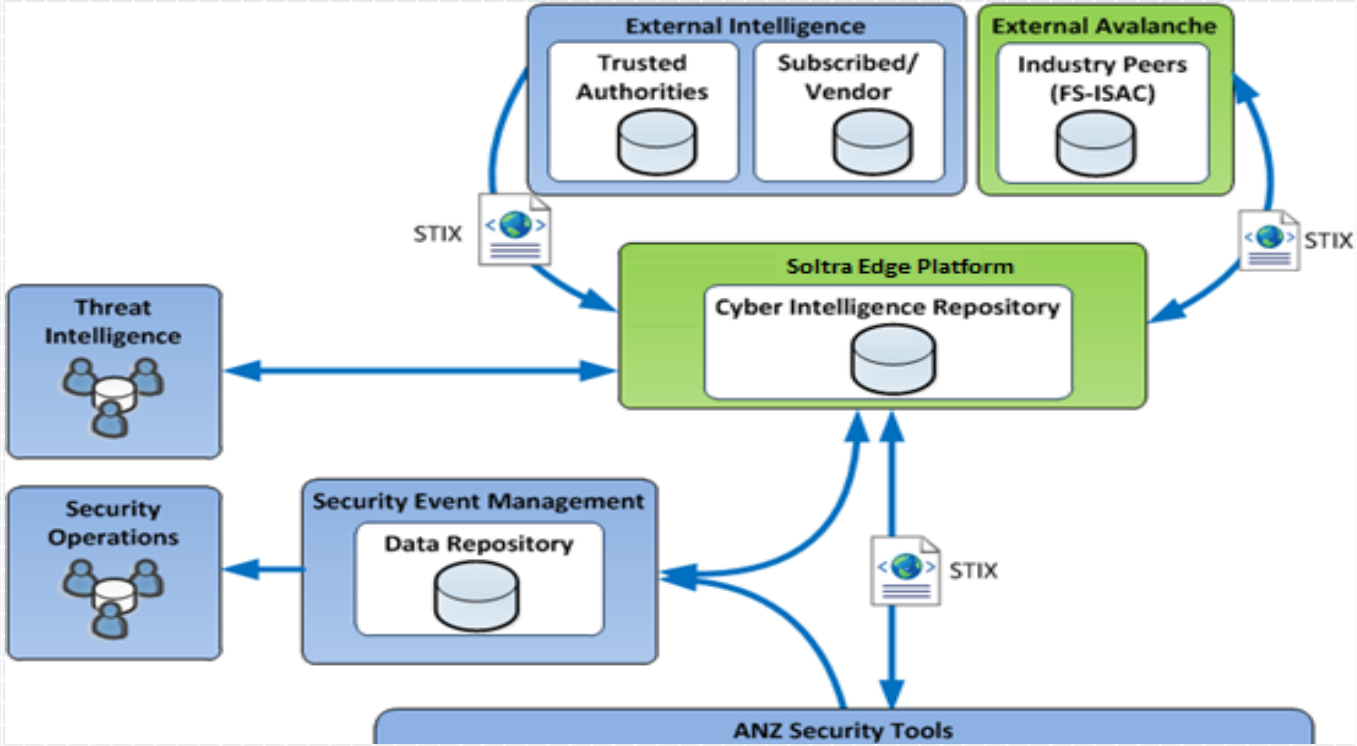
ANZ's approach to the problem (cont.)

```
<NetworkConnectionObj:Layer7_Connections>
    <NetworkConnectionObj:HTTP_Session>
        <HTTPSessionObj:HTTP_Request_Response>
            <HTTPSessionObj:HTTP_Client_Request>
                <HTTPSessionObj:HTTP_Request_Line>
                    <HTTPSessionObj:HTTP_Method datatype="string">GET</HTTPSessionObj:HTTP_Method>
                    <HTTPSessionObj:Value>http://enterthename14.bbsindex.com/ts/in.cgi</HTTPSessionObj:Value>
                    <HTTPSessionObj:Version>HTTP/1.1</HTTPSessionObj:Version>
                </HTTPSessionObj:HTTP_Request_Line>
```

ANZ's approach to the problem (cont.)

```
<HTTPSessionObj:HTTP_Request_Header>
    <HTTPSessionObj:Raw_Header>Accept: application/x-ms-application, image/jpeg, application/xaml+xml, i
    <HTTPSessionObj:Parsed_Header>
        <HTTPSessionObj:Accept>application/x-ms-application, image/jpeg, application/xaml+xml, image/gif
        <HTTPSessionObj:Accept_Language>en-AU</HTTPSessionObj:Accept_Language>
        <HTTPSessionObj:Accept_Encoding>gzip, deflate</HTTPSessionObj:Accept_Encoding>
        <HTTPSessionObj:Host>
            <HTTPSessionObj:Domain_Name xsi:type="URIObj:URIObjectType">
                <URIObj:Value>enterthename14.bbsindex.com</URIObj:Value>
            </HTTPSessionObj:Domain_Name>
            <HTTPSessionObj:Port xsi:type="PortObj:PortObjectType">
                <PortObj:Port_Value>80</PortObj:Port_Value>
            </HTTPSessionObj:Port>
        </HTTPSessionObj:Host>
        <HTTPSessionObj:User_Agent>Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0
    </HTTPSessionObj:Parsed_Header>
</HTTPSessionObj:HTTP_Request_Header>
```

ANZ's approach to the problem (cont.)



Source: ANZ Security Threat and Vulnerability Strategy (2014). Author: Steven Mond

RSAConference2015

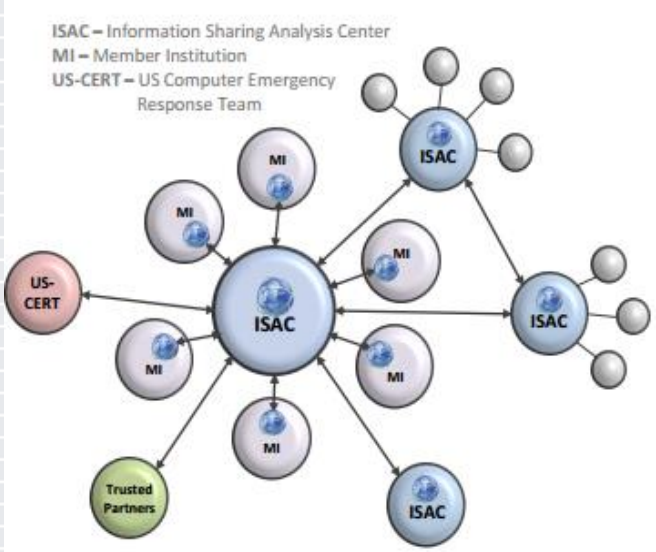
San Francisco | April 20-24 | Moscone Center

Threat Landscape
‘Power of the Community’

#RSAC

Harnessing the power of the community

- Being in Australia, we do not see all attacks evolve during our business hours (they normally occur after hours)
- The power of "Community" allows us to gain visibility into:
  - Threat indicators
  - Observables & Indicators
- Cyber-Threat Intelligence Repository allows rules for our other security controls to be built automatically
- Provides context and access to time sensitive data fast



Benefits of adopting this approach

- Sharing of attack information
  - ANZ saw attack information on threats like HeartBleed / Shellshock in 2014
    - Information collected was a subset of the overall knowledge base
    - Sharing this attack information assisted those that had not been attacked by those particular hosts
    - Those participating in the exchange would get additional information about other hostile hosts that could be used as a basis for filters within their environment

Benefits of adopting this approach (cont.)

- Sharing of attack information (cont.)
  - Other examples include Dyre malware information
    - Malware targeting financial institution
    - Sharing of Dyre proxies
      - Sharing technical information makes it possible to limit the effectiveness of this malware and realign ROI indicators back into our favour
  - Sharing provides a deeper pool of data
  - Data can be mined to develop signatures based on event-based information that you have received

Limitations of this approach

- Solution is not a panacea, it does not stop bad things from happening
- Issues exist around processing information received:
  - Block vs. Alert
  - ANZ monitors and alerts on intelligence it receives
- Does not resolve problems relating to:
  - Confidence of data and the association of information
  - Context of the data
  - Threat Model

Limitations of this approach (cont.)

- How is the data being used
  - Producer vs. Consumer of the information
- Integration issues
  - Most vendors do not support data interchange formats such as STIX
  - Custom development required for translations of data
    - CSV to STIX
    - JSON to STIX
    - XML to STIX

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Applying Cyber-Threat Intelligence within your Organisation

What needs to change … you can help

- Share information about what you are seeing in your environments
- By sharing observations/indicators:
  - You will be helping others defend
  - In turn they will publish what they are seeing
- Encourage security tool vendors to consider STIX as a valid means of sharing data with the community
  - Some have started but more a needed to join in so that the data can be used properly and shared accordingly

What needs to change … you can help (cont.)

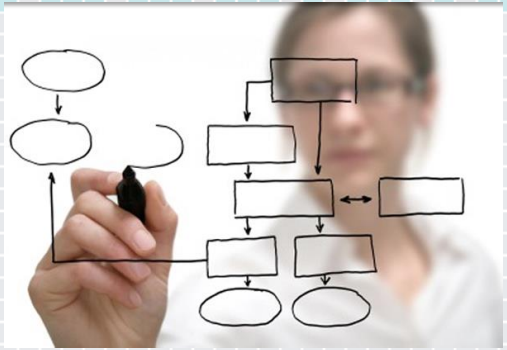
- Data / Information needs to be shared in a format that we can ingest into Threat Intelligence Platforms
- Working together we can actually lift the barrier that exists to protect ourselves from Cyber-Warfare
  - As a security collective we can re-balance the ROI equation in our favour and in turn make the investment proposition too expensive for them to operate

TOGETHER WE CAN MAKE AN IMPACT!!

Parting Thoughts …

"If we all work together we can actually make a difference and result in making it to expensive for the various adversaries to perform Cyber-Warfare."

Parting Thoughts … Let's Apply



- Next week you should:
  - Explore a Cyber-Threat Intelligence Repository
- In the next three months you should:
  - Consider what security data your organisation collects
  - Understand how this data can be used to defend your sector
  - Come up with a standard/guidelines on what you can share
- Within six months you should:
  - Look at standing up a production Cyber-Threat Intelligence Repository
  - Integrate some of your production data into it
  - Set up peering relationships with others in your sector

Questions