Cyber security resilience

ert
AUSTRALIA
PROTECTING OUR NATIONAL
INTERESTS ONLINE

Patricia Alfheim
Assistant Director, Strategic Engagement
CERT Australia

Overview

- CERT Australia

- Cyber threat landscape

- What is at stake

- Improving cyber resilience

An Australian Government Initiative

**Risk Day Forum
27 November 2015**

CERT
AUSTRALIA
PROTECTING OUR NATIONAL
INTERESTS ONLINE

CERT Australia

- the national computer emergency response team

- the point of contact in government for Australian businesses

- provides advice on cyber threats, vulnerabilities and mitigation strategies

An Australian Government Initiative

Cert AUSTRALIA
PROTECTING OUR NATIONAL INTERESTS ONLINE

**Risk Day Forum
27 November 2015**

Proactive

Publications
- Technical advisories
- Indicator sharing
- Good practice guides

Information exchanges
- Regional & national

Training and Exercises
- ICS / domestic training
- Regional & international exercises
- Custom exercises

Industry engagement & events

Assistance / support
- Australian businesses (500 +)
- ACSC agency partners
- International CERTs

Activities
- Onsite assistance
- CND advice
- Offsite malware, log and other analysis

Reactive

CERT AUSTRALIA IS PART OF THE AUSTRALIAN CYBER SECURITY CENTRE

The environment

- cyber threat is real, ever present & growing

- broad based through to targeted

- routine through to sophisticated
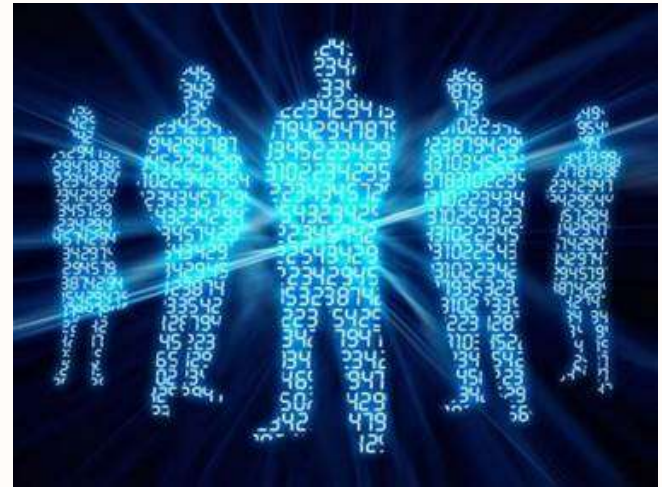
Threat actors

- individuals
- issue-motivated groups
- organised criminal syndicates
- foreign governments

11,073 incidents (2014) including **153** related to systems of national interest

- Energy
- Government
- Banking and financial services
- Communications
- Defence industry
- Transport
- Water
- Information technology
- Education and research
- Health
- Mining and resources
- Food and agriculture
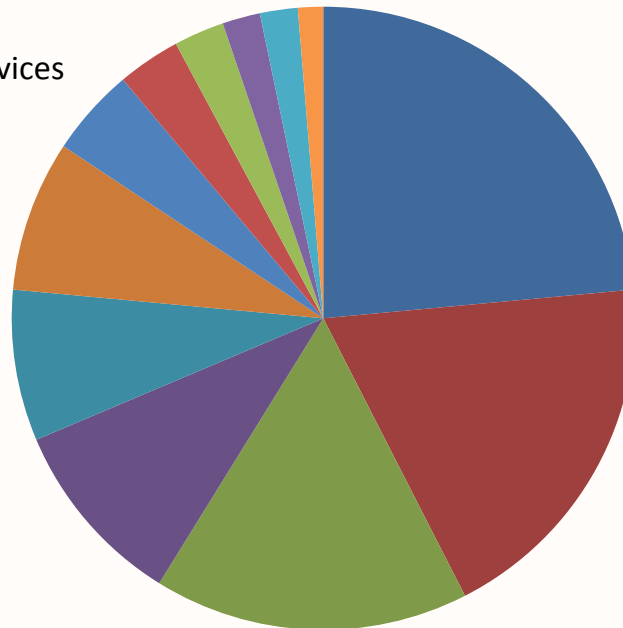
Incident categories

- Compromised system

- Malicious email

- Data exposure, theft or leak

- Scanning, recon or brute force

- Sighting report or indicator sharing

Office of Personnel Management (2015)

Ashley Madison (2015)

Kmart & David Jones (2015)

Threat- website defacement

An Australian Government Initiative

Risk Day Forum
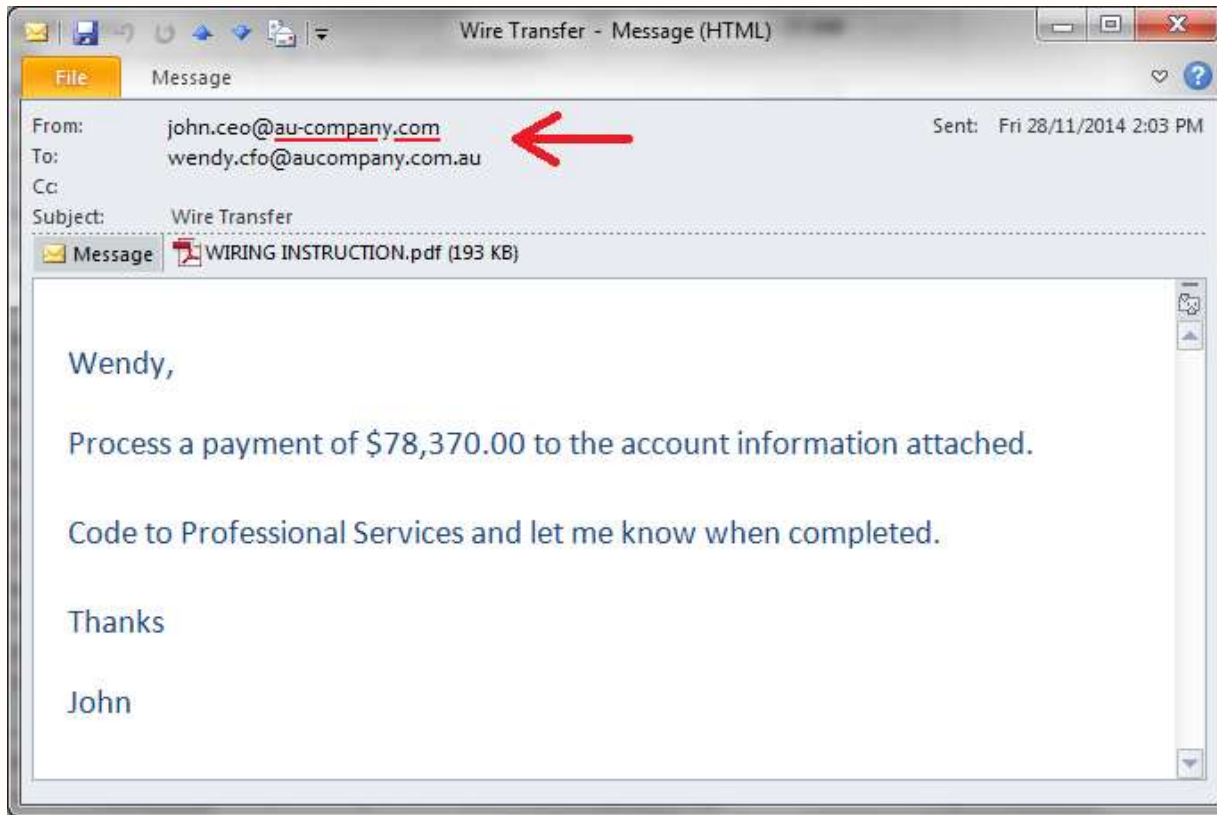**27 November 2015**

ert
AUSTRALIA
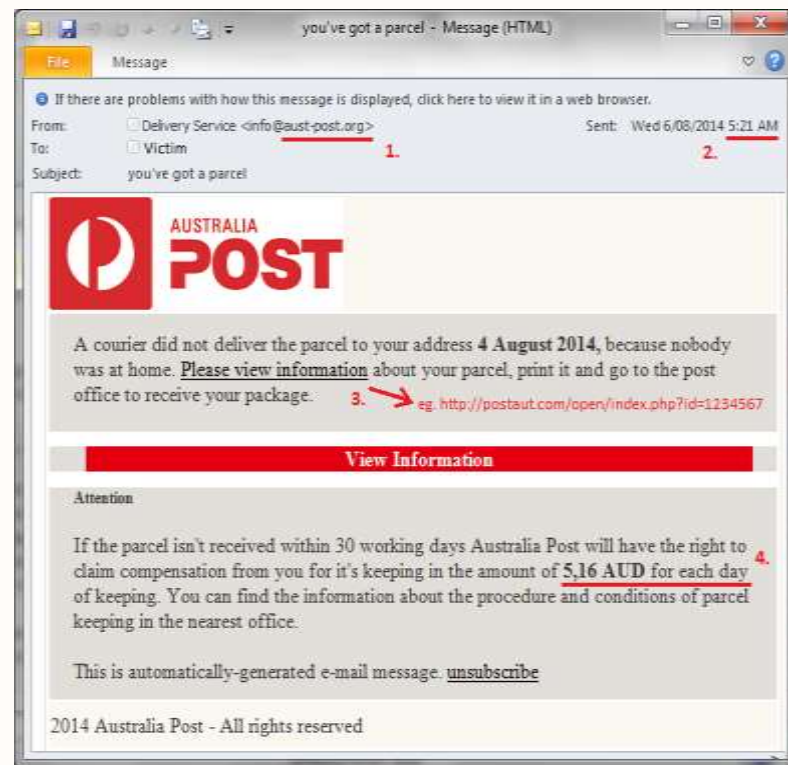PROTECTING OUR NATIONAL
INTERESTS ONLINE

Threat - wire fraud

- From tens of thousands to over $40 million
- Typo-squatting/similar looking domains
- Combined phone and email social engineering
- Extensive recon and research – highly targeted
- Transfer of funds mostly to overseas accounts, some examples used Australian banks
- Bank account owner may be complicit or also victims of crime, e.g. online dating scam victim

An Australian Government Initiative

Threat - ransomware

- Same actors since late 2013

- Constantly evolving threat

- Regular theme updates

An Australian Government Initiative
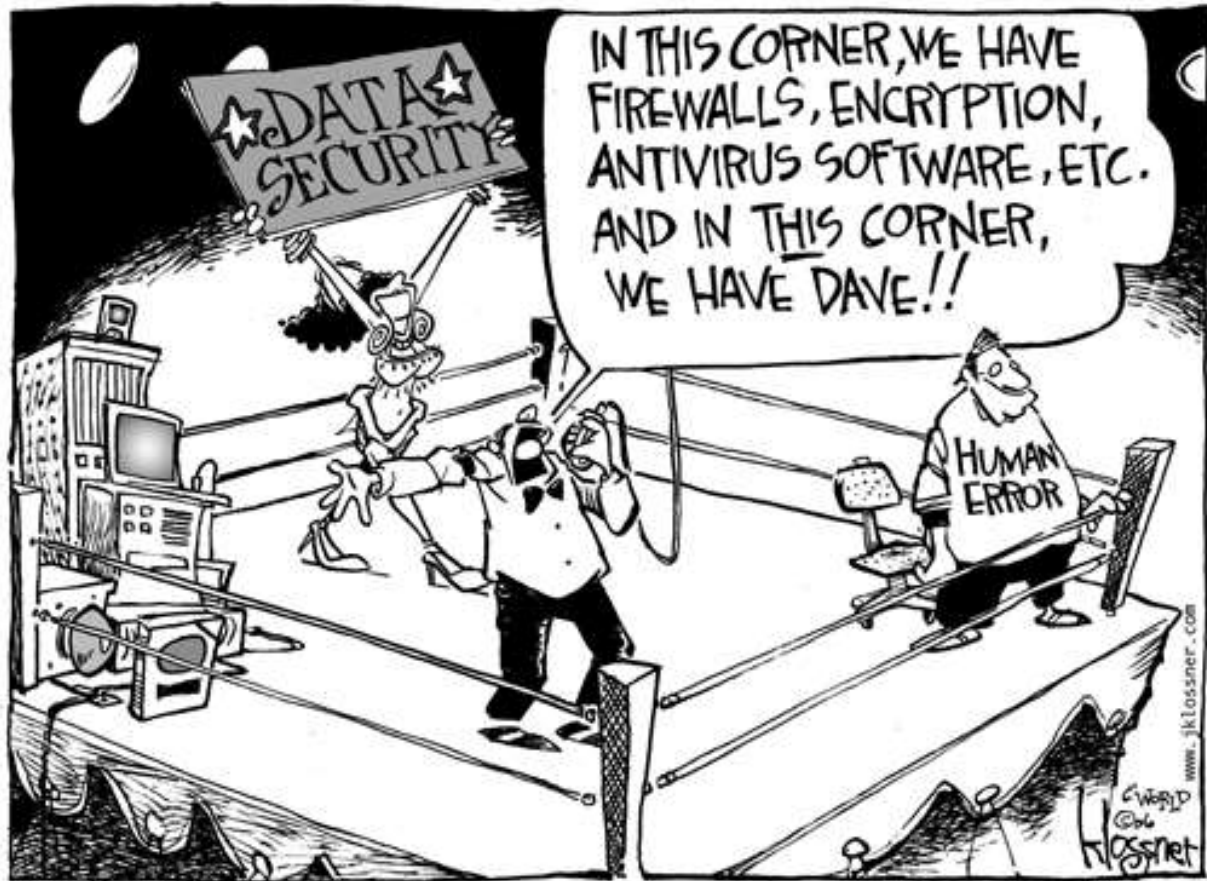
cert
AUSTRALIA
PROTECTING OUR NATIONAL
INTERESTS ONLINE

Risk Day Forum
27 November 2015

This is not a plan...

Our Disaster Recovery Plan Goes Something Like This...

HELP! HELP!

DILBERT SCOTT ADAMS

…and this is not the best preparation or response

http://bettertax.org/images/headinsand.png

Where to start

- Be informed – know your network and the threat

- Know the drill if an incident occurs

- Connect with those who can help

- Work with those who have close international relationships (such as CERT Australia)

Key messages

- the cyber threat is real and ever present

- be prepared *before* an incident occurs

- CERT Australia – we're here to help

Thank you

https://www.cert.gov.au

info@cert.gov.au

1300 172 499