

# Organisational Resilience

Information Security in practice

Alex Webling RSecP

[www.resilienceoutcomes.com](http://www.resilienceoutcomes.com)

# A resilient approach to information security

- 🌐 ACSP
- 🌐 A resilient approach
- 🌐 The threat
- 🌐 What are you protecting?
- 🌐 Syrian Electronic Army vs NYT
- 🌐 After you get done over??




But first - Just a couple of points...

🌐 On the Internet – everyone's your neighbour



- 🌐 Information - lifeblood of the 21<sup>st</sup> Century organisation
- 🌐 Islands of order in seas of chaos, but that's not really right, interdependencies
- 🌐 Humans are a problem ;)

# A resilient approach

-  Resilience is the capacity for complex systems to survive, adapt, evolve and grow in the face of turbulent change. Resilient enterprises are risk intelligent, flexible and agile (Adapted from [www.compete.org](http://www.compete.org))
-  Resilient infosec is about the organisation evolving faster than competitor – businesses, insiders and crackers.
-  Requires leadership and dedication



# The Threat

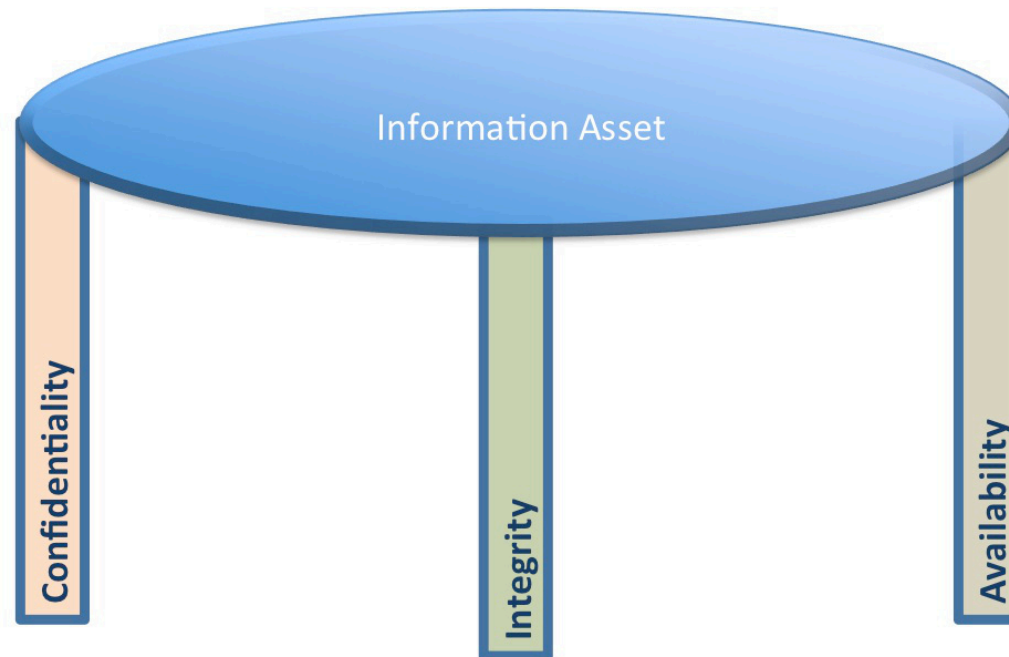
- 🌐 Everything with a processor can be cracked
  - 🌐 Natanz, Stuxnet
- 🌐 WHEN
- 🌐 Insiders
- 🌐 210






# Threat

- 🌐 During 2012, the average time to discover a data breach was 210 days (Source Trustwave)
- 🌐 14 percent of attacks aren't detected for up to two years, with one in twenty taking even longer than that.  
(<http://news.techworld.com/security/3425734/serious-data-breaches-take-months-to-spot-analysis-finds/>)
- 🌐 IT executives - “65% ”

# Infosec - You can't have it all



# What are you protecting

-  Understand your business – what information would hurt to lose?
-  Customer data
-  What is loss ?? C I A



# What are you protecting

- 🌐 How do you respond and recover
- 🌐 Can you respond if you don't know if you've been breached
- 🌐 Have to assume that you have been
- 🌐 Adaptability – information centric warfare

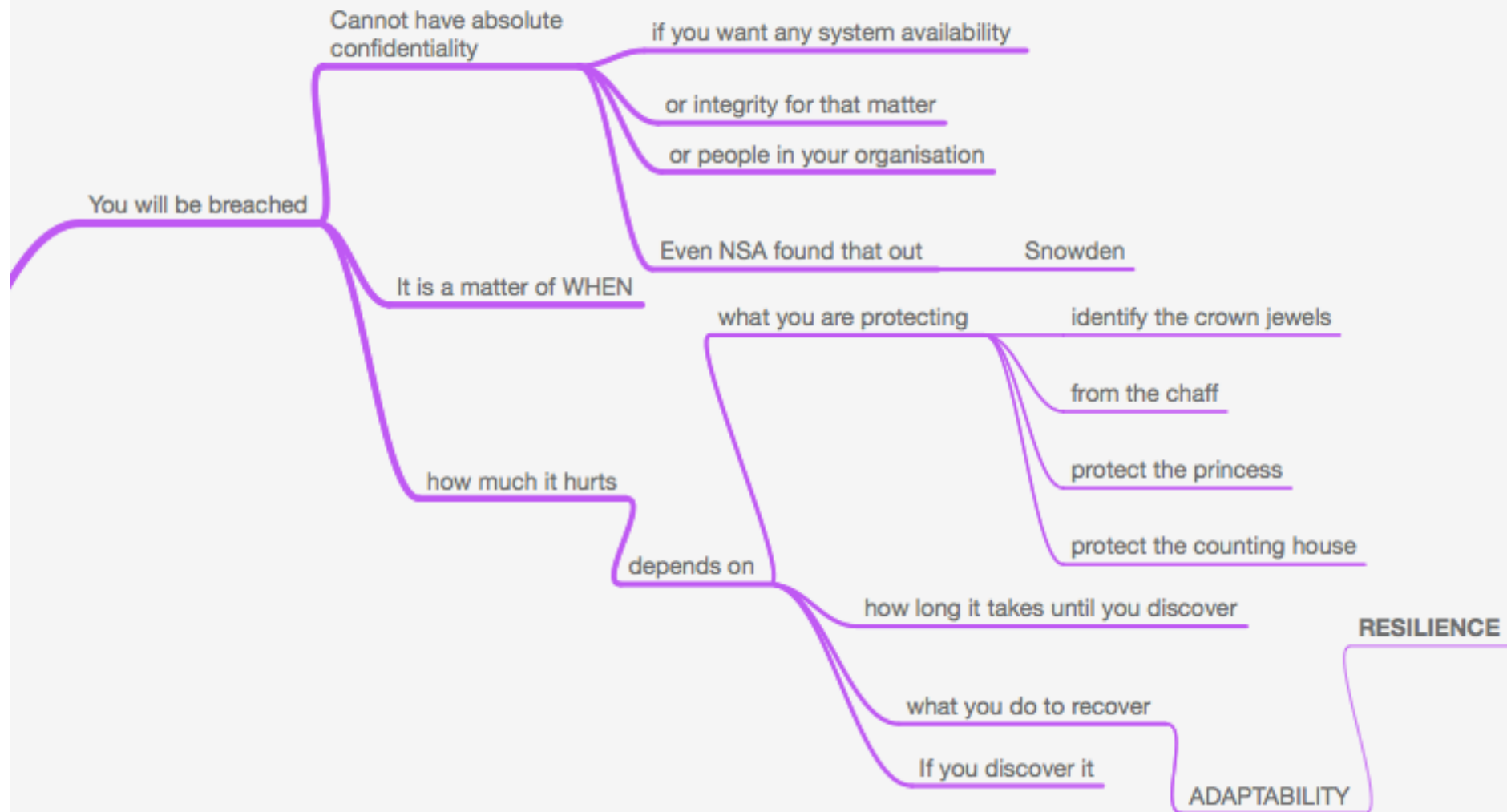
# NYT vs Syrian Electronic Army

- 🌐 Aug 2013 NYT offline, DNS
- 🌐 NYT – excellent perimeter security, motivated staff
- 🌐 Motivated attacker – lots of effort
- 🌐 Variety of methods used
- 🌐 Key breach boring (Mitnick)
- 🌐 Upstream dependencies (Melbourne IT)
- 🌐 NYT quick to recover and adapt processes

# After you get done over??

- Does the organisation need to think further about the balance between confidentiality of personal information and the availability to internet facing systems.
- From a marketing and public relations perspective is the organisation talking to its customers to show that the organisation is taking their personal information seriously;
- What changes does the organisation need to make in terms of digital evidence gathering – was this adequate enough to deter future attacks – in the long term the rule of law is the only way to reduce the power of the attackers;
- Did the organisation understand how to respond to the breach, does this need regular exercising;
- Was there an agreed direction from senior management in the event of a breach, so that the technical staff could 'get on with the job' as quickly as possible;
- Are the relationships with service providers adequate, were the levels of service and measures taken to recover sufficient.
- It is important to recognise that the best value gains for the organisation come not from IT changes like forensics, but business process rearrangement.

## A quick summary





# Thanks

 **Alex Webling, RSecP**

**Director, Resilience Outcomes Australia**

**Treasurer, Australasian Council of Security Professionals**

**07 31031207**

**[services@resilienceoutcomes.com](mailto:services@resilienceoutcomes.com)**