auDA ISS for Accredited Registrars

- Provides a set of technical, operational and policy requirements designed to protect the confidentiality and integrity of sensitive domain-related data held by registrars.
- Compliance is mandatory for all auDA accredited registrars
  - existing registrars must be ISS compliant with 24 months
  - new registrar applicants must be ISS compliant before they are granted full accreditation
  - non-compliant registrars may have their accreditation suspended, and ultimately terminated
Registrars must have adequate capability for providing information systems security procedures to prevent systems hacks, break-ins, data tampering and other disruptions to its business (Registrar Accreditation Criteria)

Registrars must notify auDA immediately of a security breach to its systems (Registrar Agreement)
In Feb 2009 the AFP notified BD and auDA that a copy of a database containing BD customer data (inc. credit card data) had been offered for sale on an online forum.

Investigations revealed that BD was made aware of the security vulnerability in April 2007, but did not notify auDA or take necessary corrective action at the time.
4 June 2011 – Distribute IT detected unauthorised access to its network

11 June 2011 – hackers launched coordinated attack on Distribute IT’s network, destroying almost all servers and backups

23 June 2011 – Distribute IT’s business sold to NetRegistry Group
Other Security Incidents

* Intrusion via third party software by submitting support ticket with attachment that executed code on the server
* Hacker contacted registrar to report software vulnerability, listing server login details
* Staff desktops compromised via an sshd exploit, program installed allowing remote login
Industry reaction to Distribute IT and our communications with registrars showed that they wanted auDA to “do something” about security.

auDA set up a Registrar Security Group in November 2011 to consider ways of improving registrar security.

auDA, AusRegistry, 5 registrars, security consultants.
Starting Assumptions

- Current security practices of most registrars are deficient
  - high compliance and audit costs
  - lack of in-house knowledge/expertise
- Registrar business models are varied
  - small through to large
  - reseller and retail
  - hosting and other services
Policy Objectives

1. To assist registrars to manage and improve the security of their own businesses – develop a ‘security culture’ among registrars

2. To protect .au registrants and the integrity and stability of the .au domain
To set a mandatory baseline standard for information security for registrars

- flexible, adaptable to different registrar business models
- aligned to well-established international standards (ISO 27001, PCI DSS)
- risk-based – registrars do their own risk assessment and select appropriate security controls
Draft ISS and Compliance Program

* ISS contains 15 security controls, similar to ISO 27001
* Registrar self-assessment via online portal, followed by on-site assessment by auDA appointed ISS assessor
* Compliance signed off by auDA ISS Committee
* Compliance valid for three years
* All ISS assessment costs are paid by auDA (does not include registrar internal costs)
Stakeholder Consultations

- 12+ month process
- Industry Panel – broader stakeholder group including resellers, consumers, government
- Individual registrar consultations – email, phone, face-to-face
- Two rounds of general public consultation
- Submitted for auDA Board approval

universal support for mandatory security standard
ISS Implementation

* auDA appointed Vectra Corp as ISS assessor, worked with Vectra to determine assessment procedures
* ISS pilot conducted with two registrars in April/May 2013
* ISS came into effect on 17 October 2013
  * existing registrars must be compliant by 17 October 2015
Follow Up

* Six registrars are ISS compliant to date
* Ongoing communications with registrars – email, phone, face-to-face
* Promotion of ISS benefits
* Registrar survey
* Review of ISS after October 2015
Thank You 😊

www.auda.org.au
jo.lim@auda.org.au