Internet Presence Protection Audit & Planning to eliminate Pain Points

Ben.Livson@bal.com.au

+61.414.250.437

Common Pain Points in Internet Backbone

We believe the following pain points are common and offer audit to map out and plan to remediate:

- Control of Internet Backbone lost to Outsourcing
- Poor Disaster Recovery and Business Continuity
- Single Points of Failure / Degradation
- Disjoint Internet Backbones from M&A
- Forced to Test Internet Backbone in Production

Common Pain Points continued /2

- Autonomous System Set-up, Peering & Coverage

- Protection of IP-Ranges

- Reverse DNS Set-up

- 75% of External DNS Configurations have Anomalies {we audit and test extensively}

- Vulnerability to Service Denial, DNS Poisoning and Storms .. Failures to Secure Internet Backbone

- Damage to Brand & Reputation from Poor Domain Name Administration

Need for Audit: Why are Failures to Protect Internet Presence so common?

- **Protection of Internet Presence often involves non-technical Paralegal Intellectual Property IP Staff;**

- **Mergers & Acquisitions are often overlooked;**

- **Business Unit DIY** bypass both Corporate IT and Outsourcer to register domains and get hosting services directly. **There is no control or even visibility of who is doing what!**

Failings in Internet Presence? /2

- **There are too many cooks:** Corporate Paralegal, Business Web & Application Owners, Corporate IT, Information Security, Network & Telecommunications Services, Outsourcer, Carriers, Domain Registrars, RIR/NRO/ASO;

- **Very few understand how it all works end-to-end**. This is partly Architectural partly Administrative partly by Convention.

Multiple Views of Internet Presence

1. **B2B & B2C End User Client View** {We have no involvement in this space};

2. **Paralegal Internet Presence Protection** {Our Service offers major value add in this space};

3. **Technology View** {We offer major value add};

4. **Competition View** {We offer major value add};

5. **Hostile View** {Whilst we do NOT offer any Security Service our information does add value}.

Our Internet Presence Protection Analysis, Audit, Planning and Testing Services

Phase 1 External Analysis, Audit & Testing

Done without any information of your systems and without any access to your ICT staff.

– **Phase 1a**   **<$100K**   **Your Company**
– **Phase 1b**   **>$100K**   **Your Competition**

– **Phase 1c**   **25%**   **On-Demand and Annual**

Our Analysis, Audit and Testing Report Covers:

– Graphing of your Internet presence;

– RIR Analysis of IP-Ranges & AS-Systems;

– Testing of External DNS & Reverse DNS;

– Analysis of your Domain Name Administration

Phase 2 of Internet Presence Analysis

- Phase 2 is internal to your company to plan in consultation with your Internet, network and security architects;

- Knowledge Transfer to your **permanent** staff;

- Final Analysis and Testing is possible only with inside knowledge and access;

- Comprehensive recommendations;

- Cost depends on the complexity of your Internet presence and infrastructure.

Competitive Landscape

- Your **Internet Presence** is only as good as your **Internet Backbone (IB) – Is IB your weakest link**?

- Your **IB** is **Visible to Competition {and Hackers}**

- **Understanding & Restricting IB Visibility is Critical**

- We have the capability to discover, collect evidence, analyse, rank and advise you on your **Internet Backbone Competitive Landscape**

- **Internet Backbone Visibility is the No 1 Threat to your Security, Business Continuity, Brand and Reputation of your Business. Understand your Information out there!**

Why DNS Audit is so Critical?

- 75% of DNS Servers are incorrectly configured. 25% had the same DNS-setup that caused Microsoft a 24hr Outage. Many leading blue chips have suffered major DNS Outages.

- 50% of Internet Domains lack DNS failover. Comcast and Google both had major Internet Outages from DNS failure.

- Some of the many DNS Security Vulnerabilities include:
  - Denial of Service Attacks incl. DNS Amplification & Storms
  - Phishing and Pharming Attacks e.g. DNS Poisoning & Spoofing
  - Website Defacement
  - DNS Compromise to distribute Spam, Viruses and Botnets

- Insecure DNS leads to Blackmail and/or Irreparable Damage to Enterprise Business Continuity, Brand and Reputation.

Our Code of Conduct for Audits

- We make no comments about the strength of your Internet Security;

- We do not try to access any of your Online Systems and are not involved in any ethical hacking or penetration testing;

- We do not put any load on your systems or Internet connections.

Internet Governance Framework
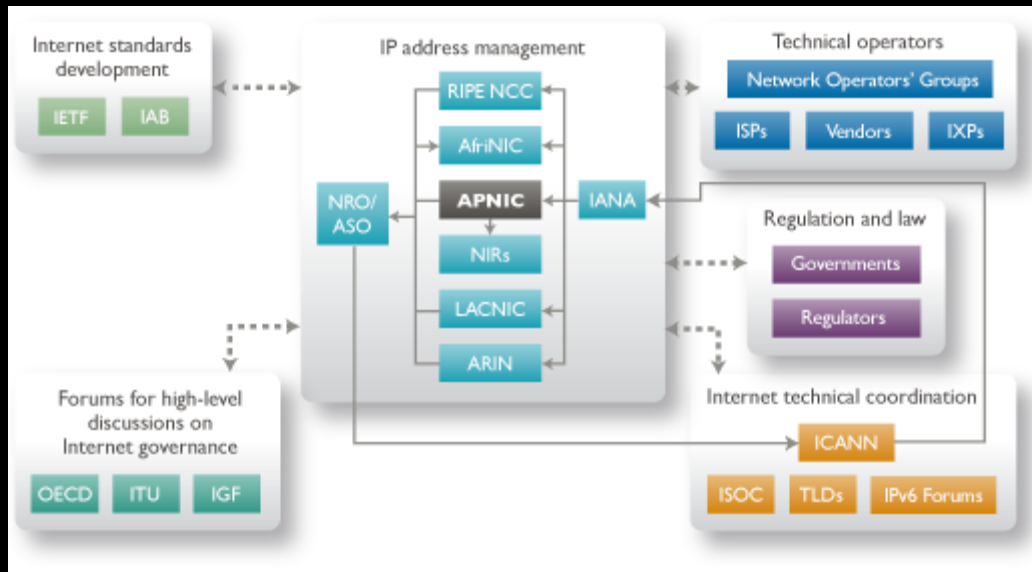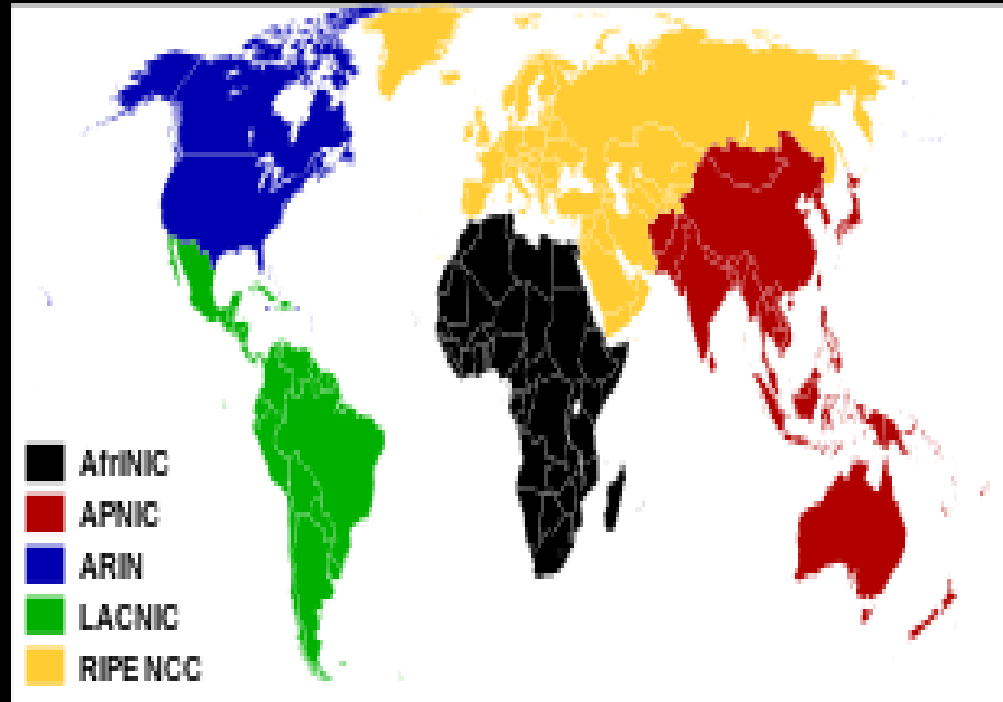
Map of Regional Internet Registries

Regional Internet Registration Services

- IPv4 address allocation and assignment

- IPv6 address allocation and assignment

- AS number assignment and analytics - <u>ASRank</u> is CAIDA's ranking of <u>Autonomous Systems (AS)</u>

- Directory services including:

- Registration transaction information (WHOIS)

- Routing information (Internet Routing Registry)

- Routing Public Key Infrastructure (RPKI)

- DNS (Reverse)

Key Terminology

ARIN	**American Registry for Internet Numbers**
AS	Autonomous System {Internet Backbone}
ASO	Address Supporting Organization
BGP	Border Gateway Protocol
DNS	Domain Name System
IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
IB	Internet Backbone
ICANN	Internet Corporation for Assigned Names and Numbers
IXP	Internet eXchange Point
IGF	Internet Governance Forum
ISOC	Internet Society
ISP	Internet Service Provider
ITU	International Telecommunications Union
NIR - RIR	National Internet Registry – Regional Internet Registry
NRO	Number Resource Organization
RIPE NCC	Réseaux IP Européens Network Co-ordination Centre
TLD	Top Level Domain