Department of
Transport

Australia's 2020 Cyber Security Strategy – A call for views

1. What is your view of the cyber threat environment – a Department of Transport, WA (DoT) bird's eye view

- **Key threat is loss of 'Confidentiality, Integrity, Availability' (CIA) of DoT Systems or Data**
- **Security is invisible by default** – It is challenging to identify legitimate attacks, let alone breaches
- **Confidential data can be held in a variety of places** – On premise, cloud, thumb drives, mobile devices, 3rd parties – ensuring the right people can access data at the right place and right time is paramount
- **There is a complicated regulatory landscape – including breach disclosure** – Navigating complex Commonwealth and State Laws and the constraints they apply impacts the reporting and sharing of breach information.
- **Ramifications of potential losses involved due to cybercriminal incidents and data breaches can be staggering** - The resultant fall-out of a major security incident can range from financial (often measured per record) to reputational damages, and it can take a lot of money and a long time to recover from a major incident
- **TRELIS** holds the crown jewels of DoT that being - Personal identifying data and collection agency for licenses/fee payments. There are many primary interfaces with other agencies (state, federal), partners and contractors. There are also a number of secondary interfaces such as WA local government, HR systems, financial systems, including e-Business.
- **Autonomous Vehicles** concerns around safety-critical systems and sensor-enabled IoT emergent technologies.

Key Threat vectors continue to be social engineering, malware (email/web) and abuse of privilege.

Key Threat Actors include 'Insiders', 'Insecure Service, Providers and Partners', 'Corporate Espionage' and 'Organised Crime'.

2. What are our key risk factors?

- Expanding online presence
- Credit Card Merchant
- Expanding integration footprint
- Weakening Economy
- User/Staff Competencies
- Increased use of mobility technology
- Increased use of social media
- Transition to "Cloud"
- Digital Transformation

3. Key vulnerabilities/risks for a Department of Transport, WA (DoT) in the trenches.

- Software patching
- Privileged access management
- Key System Availability
- User Security Awareness
- Skilled workforce in new technology systems
- Security incident detection
- 3rd Party (vendor/partner/provider)
- Machinery of Government – Merge/unmerge of Agencies
- Machine to Machine interfaces (API's Public and Private) – data sharing and classification across government and private industry.
- Bots screen scraping public available web site information and using this information via other commercial and public available web sites to create identities, then repurpose those identities for criminal purposes
- Cloud solutions within Government such as MS AZURE where 130 agencies in WA all will potentially share and extend their network access boundaries to the same internal and external identity Manager solutions where access roles and privileges directories/stores, are defined within agencies and likely to be exposed to a number of attack vectors within and externally to Government – e.g. partners, intermediaries, contractors, internal staff.

4. What does our DOT's cyber security strategy look like?

Our strategy is part of a phased approach to improve cyber maturity and security posture across DOT that includes securing People, Processes, Information and Infrastructure. The lack of funding has been challenging in providing the scale, skills and expertise to assess the risk and vulnerabilities and implement solutions that will continue to develop better DOT cyber resilience and preparedness. Although threats and malicious cyber activity has increased significantly over the past five years resourcing to defend has not increased.

To continue moving forward in this space, Mr Christian Thompson ED, BIS of the Department of Transport has started a cross-collaborative partnership with DOT, Main Roads and The Public Transport Authority (PTA) of Western Australia with the view of an anticipated sharing of expertise and solutions across cyber security information, incident response, cloud security, and security culture change. Robust risk discussions and conversations regarding challenges, situational awareness and considerations of current and future of implications is now on the agenda.

5. Responsibility of managing and understanding cyber risk across critical infrastructure as part of overarching initiatives of GovtNext, Office of Digital Government.

The Department of Transport's Information Security Profile is extensive, including 'Key Information/Data Assets", "Key Partners" (including WAPOL, Department of Justice - DOJ, Insurance Commission of WA - ICWA, Fisheries etc), Licensing agents, "Key Service Providers" (data management, personal identity data).

GovNext is a key initiative of the Digital WA strategy developed by the Office of Digital Government, Department of Premier and Cabinet WA. The key strategy is to transition IT expenditure from a capital-based model to a consumption-based model.

The leading objective is to reduce IT expenditure across government.

However, issues do exist;

- There is a risk that cyber security is viewed as being 'baked in' across enterprise architecture. Agencies need to challenge and confirm level of security.
- The future impact of encryption strength on Data at Rest and potential issues for DoT.

Infrastructure is currently targeted under GovNext/GCIO plan; however, all government agencies are mandated to use three (3) Primes for their infrastructure and for their service type arrangements.

These are

1. Atos
2. Datacom
3. NEC

With respect to the use of these vendors there is still a lack of clarity in security assurance and compliance requirements.

A request for sufficiently evidenced certification (APAC region) of security standards have not been provided by the three government primary providers and alongside the merging of service delivery in an aggressive time frame makes this an urgent requirement of DOT business operations.

Understanding the threat environment is key, for both DoT's data at rest and in motion, significantly with the move from social engineering to more targeted cloud individualised attacks to compromise DoT user credentials.

Ideally, DoT would like to see increased collaboration between state and federal agencies cyber-solutions for mitigating, managing, threats/threat vectors and federal/state help in implementing and setting priorities, developing strategies and plans. Currently, alerts are received from multiple sources creating an overload of similar information and in some instances not timely; a single source would be a great improvement.

Mitigation strategies would include timely and relevant intelligence – i.e. new attack techniques and countermeasures– including social engineering campaigns, DNS Sec, understanding deception technologies, discussing the latest Tactics, Techniques, and Procedures (TTPs) for defrauding financial services of DoT (laundering of connections through various clouds), monitoring of Deep and Dark Web for exfiltrated DoT data and information.

Government could implement a clearinghouse/vetting capability concept to the marketplace, so the federal government could take advantage of its buying power on behalf of state and local government agencies.

Pip van Wanrooij
Contractor, ICT Security Administrator
on behalf of

[redacted]

Mr Christian Thompson
Executive Director | Business Information Systems
Department of Transport WA