IT Security Risks and Mitigation Strategies

Auckland Transport

An Auckland Council Organisation

The Cyber Threat Landscape of a Modern Organisation

- Staff stealing information
- Malware – the ever evolving threat
- Network based attacks
- Information and Identity thefts
- Social Engineering
- Threats to Physical Security
- Balancing the Costs and Benefits of Countermeasures

Potential Impacts of Data Breaches

- Legal costs
- Loss of revenue due to unavailability of service
- Privacy compliance violation fines
- PCIDSS violation and fines
- Loss of intellectual, competitive or proprietary information
- Loss of future profits resulting from an inability to
- demonstrate a strong security process to clients, vendors and partners

Strategies for a Safer Network

- Build and Maintain a Secure Network and Systems
  - By Implementing and installing firewalls to protect data
  - AT uses F5 Firewalls – industrial strength devices used by the likes of Trademe and other large organisations
- Regularly Monitor and Test Networks
  - Conduct regular security audits using external specialist companies
  - This includes both internal and external security scans
  - We alternate vendors to ensure different methodology and tools used.

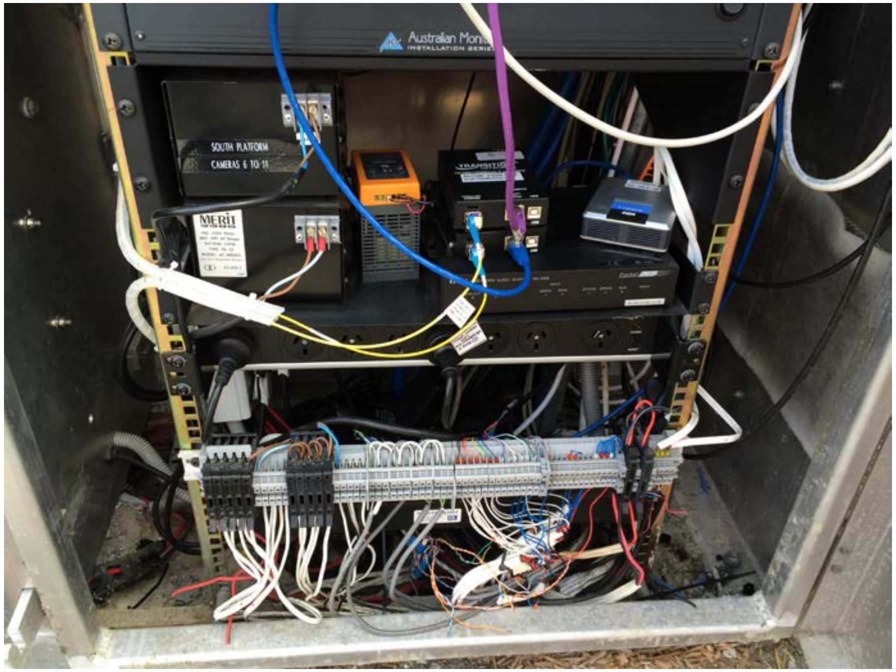
PCI Compliance

- .PCI /DSS compliance
  - Achieved Level 1 compliance for banking industry required to operate HOP and take banking transactions by AT.
  - Fines for failure to comply and potential withdrawal of online banking services.
  - Requires :
    - full time Certified Security Officer
    - Regular scanning and penetration testing of the network certified by 3rd party
    - Regular scanning of every database and system in AT to check we are not storing Credit Card Numbers

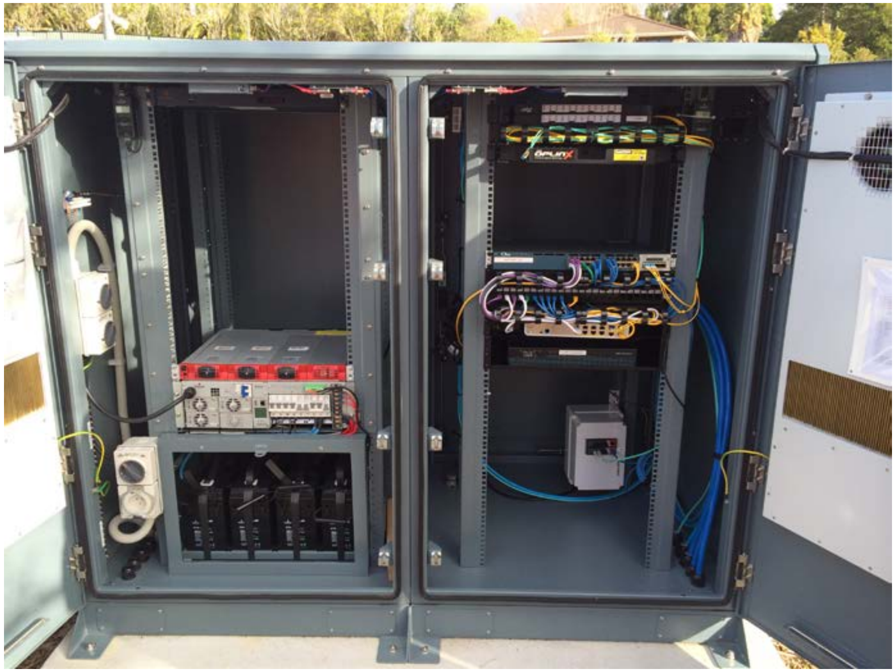
Infrastructure Physical Security

- Network Security
  - Network physical security
  - Rail network fully secured
  - Other networks secure but in process of being further secured in terms of physical access constraints
  - Alarmed access
  - Physical environment monitored
  - UPS – battery power backup

Physical Security – bye product



Prior Wiring



Post upgrade

Device Physical Security

- Device Security
  - Implemented bit locking on all mobile devices- encryptes data on drive and needs pin password to access laptops
- Access Security
  - Moving to 2 factor authentication. Means users accessing remotely have to have a unique key that is generated randomly each time access required

Future – Network based security

- Network Security Information and Event Management (SEIM)
    - Implement Monitoring of data travelling along network
        - Detects new type or traffic or unusual traffic moving across network
        - Provides additional security against connections to network

- Network Monitoring
    - Implementing additional audit tools across all the firewalls and switches to proactively monitor attacks
    - Implemention of Software Defined Network (SDN) to regulate and direct known traffic across the networks.

- CCTV
    - Implementation of SEIM and SDN is required to securily manage the large volumes of CCTV traffic traversing the network.

Balancing the Costs and Benefits of Countermeasures

- Cyber Security is a risk v cost v impact analysis.
- There is always more that can be done.
- AT conforms to best practice and is moving into leading practice with network traffic monitoring.
- AT is a little behind in terms of audit tools, but that is in the program of work for this year.