TRANSFORMING CYBERSECURITY AT GRIFFITH UNIVERSITY

A Roadmap to Success

SECURITY CAN BE HARD

- University's are traditionally hard to secure
  - Multiple industry verticals
  - Highly valuable information
  - A **LOT** of external threat sources (students)
  - Fear over disrupting academics and researchers (they might go elsewhere)
  - Relatively low understanding of security from the business
  - ACADEMIC FREEDOM!

WHAT AM I DOING HERE?

- Ash starts at Griffith in 2015
- No real security Manager for a long time
- Two security staff
  - One of them monitored internet uptime through YouTube
  - Very quickly had one security staff
- Lack of consistency
- Lack of formal processes (lack of formal anything)
- Many headaches ensue

GAPS

- Review of current Information Security Policies and documentation
- Monitor current processes to determine improvements/streamlining opportunities
- Started documenting a gap analysis (pick a framework that you can work with – ISO/COBIT/NIST etc.)
- Looked for areas where the least amount of work would yield the best results

CONSISTENCY + PROCESS = SUPPORT

- Created transparent processes where possible
  - Security reviews
  - Risk exceptions
  - Compliance activities
- Ensured consistency (where possible)
- Showed that the team cared about the outcomes and provided value to the business
- Earnt trust and support over time

DON’T BE A ROADBLOCK!

ENABLE THE BUSINESS OBJECTIVE

REPORTING

- Determined security related metrics
  - Easier said than done – still a work in progress
- Got regular security reports to senior stakeholders
  - Yearly Council reports, regular reports to Audit Committee etc.
- Frame security problems in business risk
  - Security doesn’t live in isolation, it’s a by-product of business risk

A TURNING TIDE

- Created a Security Steering Committee
  - Ensured senior stakeholders were involved
  - Ensured regular meetings
  - Provided reporting and metrics
  - Got consensus & decisions made

- This is when things started to fall into place

A FORMAL GAP ANALYSIS

- We formalised the gap analysis by doing an ISO27001 assessment
- The University finally had visibility into both the good and bad areas of security
- Worked with the University to decide upon a maturity level that they wanted to achieve

STRATEGY & ROADMAP

- From the ISO27001 assessment and desired maturity level the University could determine areas of improvement
- A formal strategy was created to align with these goals that the University wanted to achieve
- Metrics for near, mid and long term strategy goals were created to track progress
- A formal technical roadmap was also developed to enable the objectives of the strategy over a 3 year period

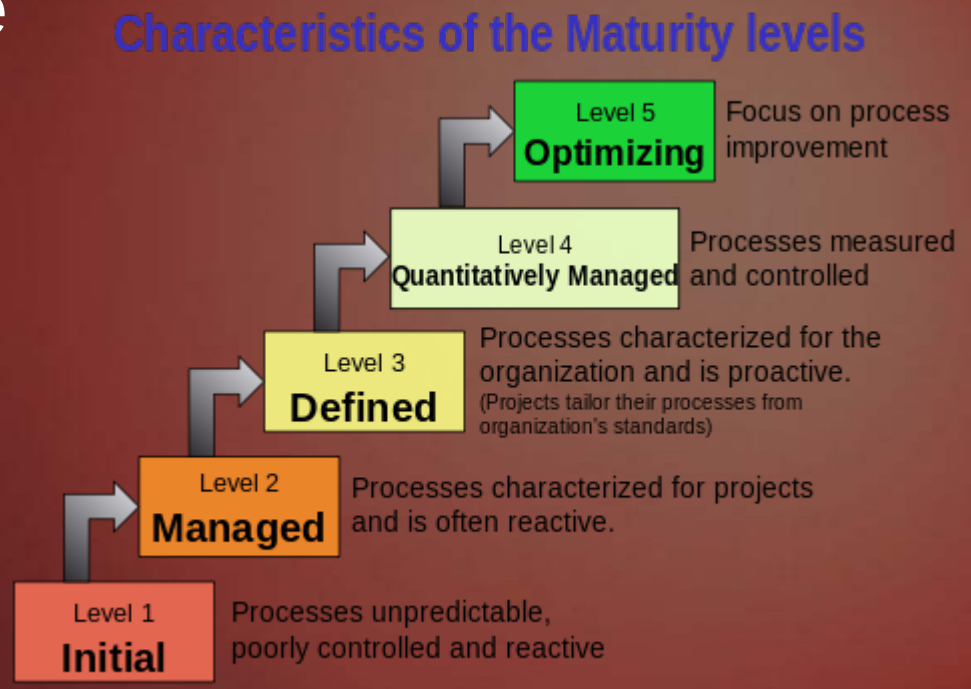
VALIDATING THE ROADMAP

- The technical roadmap contains a program of works that aligns with the strategy
  - However, there is no formal way to validate the criticality of each item
- Formal project to implement ISO27001 & ISO27002 requirements is underway
  - This project looks at the University's most critical information assets, the inherent risks associated with them, the maturity of the current technical controls, the desired level of acceptable risk, and then creates a Risk Treatment Plan
  - This is the formal prioritisation, and justification for the technical program of works
- Hopefully ongoing approval of funding

CURRENT MATURITY VS DESIRED MATURITY

- Current maturity level is somewhere between 2.5 & 3 (CMMI scale)
- Target maturity level is between 3.5 & 4

- This will be able to provide the University with defined metrics & quantitative values for risk
  - Can then derive ROI for security



STRATEGIC ROADMAP & COMMONWEALTH GAMES

- Activities for Commonwealth Games had overlap with the current strategic roadmap
  - Allowed for re-prioritisation of certain activities (Security Operations Centre, DDoS protection, numerous security retainers etc.)

- Easily able to show the value of what would be a one-off activity towards an ongoing security program now
  - Easier to justify

OBSERVATIONS

Some observations on the Griffith Cybersecurity journey …..

- Significant evolution from two years ago (concerted and sustained effort)
- Level has been pitched right – balance between aiming high and what the culture and capability can grow to accommodate
- Approached in a highly proactive manner and with a mature perspective
- Focused on support of the business and being able to demonstrate value through transparent risk reduction
- Together with the institution's appetite for good governance – major wins have occurred (and there are more to go!)
- These wins have not be a walk in the park …. significant negotiation and collaboration required for buy in and acceptance.

OBSERVATIONS

- The approach and appetite have ultimately had to match – concerted effort facilitated by ….
  - University - large scale operating models (resources/governance)
  - Strong support and representation of cybersecurity from Senior Management (translates into decision making and $)
  - A strong culture of data governance headed up by IM Department
  - Lateral engagement with the IT Projects Office for embedding security
  - Rigour - Solutions Architecture Board (SAB) Change Advisory Board (CAB)
  - Digital transformation path - cloud, mobile and self serve, cybersecurity
  - Business based drivers such as PCI, PII and Medical Data
  - Improving security awareness and culture across the University,
  - Existing security technology based controls
  - More to go - 27001 gap analysis, controls, PMO, roadmap, awareness, etc.

THAT’S ALL FOLKS!

QUESTIONS?