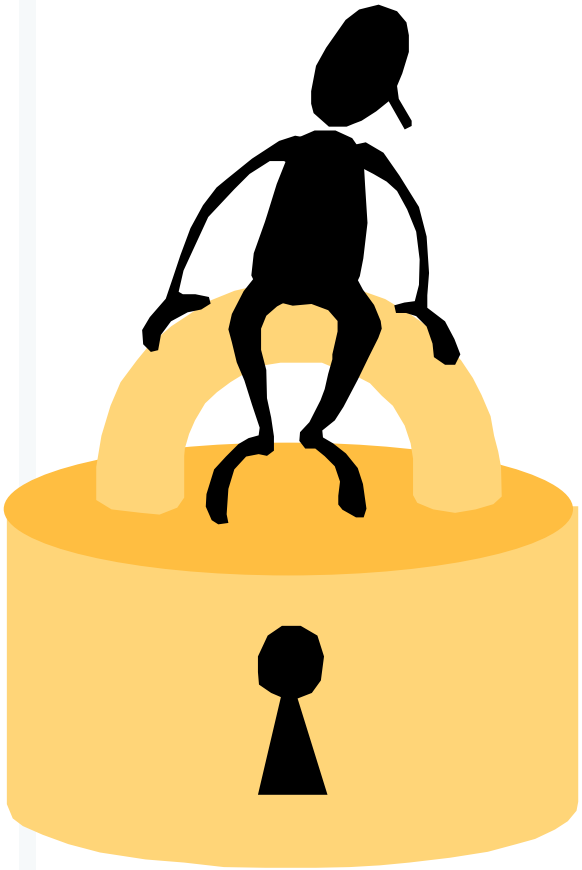
UTS:
IT Security Office



UNIVERSITY OF TECHNOLOGY SYDNEY

How Secure is the Network?

Ian Waters
Senior IT Programs Consultant
July 2005

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

Agenda

- Security Framework
- Security Program
- Network Risk Assessment
- Lessons Learnt

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

General George S Patton:

"Take calculated risks. That is quite different from being rash."

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

What is Security?

Dictionary: "The state or feeling of being safe or protected"

Definition from IT perspective: "The state of being free from unacceptable risk"

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

How Do We Reach this State?

By using a formal risk assessment methodology

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

UTS Environment

- 3 campuses
- 27000 students and 2500 staff
- 6300 network-connected devices
- Challenging, somewhat hostile, with users and intruders prone to experimentation, mischief and worse

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

IT Security Framework at UTS

- IT Security Policy
  - Principles
  - A high-level statement of measures and controls to protect corporate UTS information
  - Endorsed by University Council in 2000

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

IT Security Framework at UTS

- IT Security Policy
- IT Security Standards and Guidelines
  - Derived from principles of Security Policy
  - Provide the detail of best practice
  - Based on international standard for information security management (ISO 17799:2001)
  - Tailored for environment at UTS

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

IT Security Framework at UTS

- IT Security Policy
- IT Security Standards and Guidelines
- High Level Risk Assessment

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

IT Security Framework at UTS

- IT Security Policy
- IT Security Standards and Guidelines
- High Level Risk Assessment
- Analysis and Prioritisation

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

IT Security Framework at UTS

- IT Security Policy
- IT Security Standards and Guidelines
- High Level Risk Assessment
- Analysis and Prioritisation
- Detailed Risk Assessments

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

IT Security Framework at UTS

- IT Security Policy
- IT Security Standards and Guidelines
- High Level Risk Assessment
- Analysis and Prioritisation
- Detailed Risk Assessments
- Risk Management Plans

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

IT Security Framework at UTS

- IT Security Policy
- IT Security Standards and Guidelines
- High Level Risk Assessment
- Analysis and Prioritisation
- Detailed Risk Assessments
- Risk Management Plans
- System Security Plans

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

Risk Assessment Process

- Identify assets eg hardware, data, people plus intangibles like reputation
- Enumerate vulnerabilities and threats
- Determine likelihood of these occurring
- Determine impact if they do
- Identify current risk level
- Specify required risk level
- Use gap to determine priorities for risk mitigation action

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

UTS Risk Assessment Methodology

- Based on framework used by Commonwealth Government
- Conforms to international standard ISO 13335-2 Managing and Planning IT Security

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

UTS Risk Assessment Methodology

- Standardised definition of likelihood:

Negligible	Unlikely to occur
Very Low	Likely to occur two/three times every five years
Low	Likely to occur once every year or less
Medium	Likely to occur once every six months or less
High	Likely to occur once per month or less
Very High	Likely to occur multiple times per month or less
Extreme	Likely to occur multiple times per day

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

UTS Risk Assessment Methodology

- Standardised definition of likelihood
- Standardised definition of consequence:

Insignificant	Will have almost no impact if threat is realised
Minor	Will have some minor effect on the asset value, but will not require any extra effort to repair or reconfigure the system
Significant	Will result in some tangible harm, albeit only small and perhaps only noted by a few individuals
Damaging	May cause damage to the reputation of system management, and/or notable loss of confidence in the system's resources or services
Serious	May cause extended system outage, and/or loss of connected customers or business confidence
Grave	May cause system to be permanently closed, and/or be subsumed by another (secure) environment

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

UTS Risk Assessment Methodology

- Standardised definition of likelihood
- Standardised definition of consequence
- Standardised measure for risk:

			Consequence			
		Insignificant	**Minor**	**Significant**	**Damaging**	**Serious**
	Negligible	Nil	Nil	Nil	Nil	Nil
	Very Low	Nil	Low	Low	Low	Medium
Likelihood	**Low**	Nil	Low	Medium	Medium	High
	Medium	Nil	Low	Medium	High	High
	High	Nil	Medium	High	High	Critical
	Very High	Nil	Medium	High	Critical	Extreme
	Extreme	Nil	Medium	High	Critical	Extreme

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

Risk Management

- Identify safeguards required to mitigate risk
- Develop action plan with timetable and responsibilities
- For a particular system or resource, this risk management plan forms the basis of its IT Security Plan

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

Compliance and Review

- Report on progress in treating risk
- Review for new or changed threats and vulnerabilities at regular intervals
- Repeat - process enables high priority risks to be addressed first

UTS: IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

IT Risk Assessment Program at UTS

- Trial within IT Division - 33 corporate systems underwent a high-level assessment
- Identification of assets across University - 211 major IT systems and resources
- High-level risk assessment of all major systems - 48 at highest priority
- Pilot detailed risk assessment
- Review of effectiveness of methodology
- Detailed risk assessment of other systems in order of high-level risk

UTS: IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

Network Risk Assessment (1)

- Identify assets by breakdown into major components
  - Infrastructure
  - Data
  - Voice
  - Audio Visual
- Further breakdown major components into sub-components
  - eg cabling, VPN, switchboard, video conferencing

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

Network Risk Assessment (2)

- Conduct a risk assessment workshop for each major component, involving key stakeholders, to identify threats and vulnerabilities
  - Commence with brainstorming session
  - Brings to light other threats
  - Use institutional standards and external checklists to identify further threats

Network Risk Assessment (3)

- Identify the current and required risk associated with each of the threats and vulnerabilities
  - Use tables for standard definitions of likelihood, consequence and risk level

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

Network Risk Assessment (4)

- Document results of risk assessment following the workshop and confirm with participants

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

Network Risk Assessment (5)

- Conduct a further workshop on each component with the same participants to identify risk mitigation actions
- Agree responsibility and timeframe for each risk mitigation action
- Document the results in a risk management plan

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

Results

- Identification of 37 sub-components for the 4 major network components
- Identification of 86 threats
- Determination of 105 treatments to be included in the risk management plan

UNIVERSITY OF TECHNOLOGY SYDNEY

Example

Threat	Power surge
Description	Power fluctuation damages equipment
Assets Affected	Equipment not connected to an uninterruptible power supply
Impact	Partial or total network failure
Threat Source	Power utility
Existing Controls	Some uninterruptible power supplies installed
Likelihood Rating	Medium
Consequence Rating	Significant
Current Risk Rating	Medium
Required Risk Rating	Low
Treatment Option	Reduce
Treatment Detail	Install further UPS's
Priority	B
Treatment Action	Connect all network equipment to UPS
Responsibility	CW
Timeframe	Ongoing

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

Resources Required

- Identification of components: 4 senior managers for one hour
- Risk assessment workshops: 3-5 technical personnel and managers for 2.5 hours
- Risk management workshops: 3-5 technical personnel and managers for 2 hours
- Facilitator: 50 hours
- Total: Approximately 126 person-hours or 18 person-days

UNIVERSITY OF TECHNOLOGY SYDNEY

Lessons Learnt

Time Constraints

- Especially difficult to get key technical staff together for a lengthy period
- Preferable to perform risk identification in one workshop, as it is not easy to restart and invariably will involve time lost while revisiting threats previously discussed
- One solution is to start people thinking before the workshop, to tailor the depth and detail of the threat identification to the time available, and to use checklists to uncover any major omissions

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

Lessons Learnt (cont)

Mixed Motivations

- Participants may not want to be there at a workshop and not contribute willingly, may have a vested outcome that they are determined to achieve by exaggerating risks, or preferably may be enthusiastic about the process and participate fully
- There is a need for the facilitator to be impartial and a diplomat

UTS: IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

Lessons Learnt (cont)

Accountability Required

- It is desirable for the system custodian to take responsibility for documentation of results, implementation of risk mitigation actions, and followup and updating of plans
- Sometimes at UTS this has not been achievable, and the facilitator has had to perform some of the above

UTS: IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

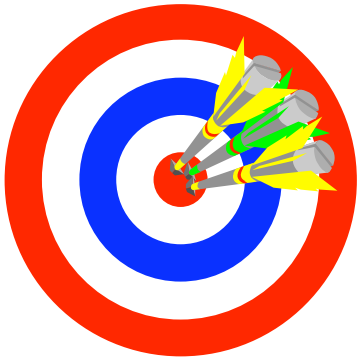
Lessons Learnt (cont)

Documentation Procrastination

- A System Security Plan is often not produced in a timely fashion
- It should be, but as the last step in the process it is often postponed

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY



Conclusions

- Risk assessment does work and does produce a more secure outcome
- Complexity abounds, in particular for the network, making risk assessments time-consuming
- Attention must be given to defining the scope of what is to be assessed and understanding its underlying architecture, to permit risks to be assessed for all logical components
- Process permits prioritisation of a potentially very large number of actions that could be taken to improve security
- Process gives management (and the auditors) some confidence that the risks associated with introduction of a new system have been considered and addressed before the system goes live

UTS:
IT Security Office

UNIVERSITY OF TECHNOLOGY SYDNEY

Questions