The state-of-the-art in security governance

Stephen Wilson
Lockstep Consulting
CA Expo, Sydney 16 Feb 2004

This is the modern world

San Francisco Chronicle

22 October 2003

A tough lesson on medical privacy
Pakistani transcriber threatens UCSF over back pay

See www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2003/10/22/MNGCO2FN8G1.DTL

Corporate Governance

Duty to customers & staff

versus

Duty to shareholders

Corporate Governance

"The business" *versus* "Technology"

Is security *really* "good for business"?

The compliance landscape

- Privacy Act (Cth) 1988
- Privacy Amendment (Private Sector) Act 2000
- Stock Exchange Listing Rules
- Sarbanes Oxley Act (Federal US)
- Cyber insurance policy conditions
- Europay MasterCard Visa EMV directive
- Basel II

Today's security drivers

- Identity Theft
  - Annual cost to community
  - Annual cost to banks
- Critical Infrastructure Protection
- Show adherence to 'best practice'
  - AS/NZS 17799
- Reduce cost of adverse events
- Reduce cost of remediation

Mapping governance onto IT

- "[A virus] is not a technology issue"
  Microsoft spokesman to BBC 5 May 00
- "Privacy is not a technology issue"
  Lou Gerstner, Chair IBM, 30 Nov 2000
- "Risk assessment … is not a technology issue"
  Robert Ferguson, Check Point to Senate Joint Committee 2 April 2003

Sloganeering!

Google

Searched the web for "is not a technology issue". Results 1 - 10 of about 586.

11 February 2004

Impact of Privacy on IT

NPP 1 - Collection
NPP 2 - Use and disclosure
NPP 3 - Data quality
NPP 4 - Data security
NPP 5 - Openness
NPP 6 - Access and correction
NPP 7 - Identifiers
NPP 8 - Anonymity
NPP 9 - Transborder data flows
NPP 10 - Sensitive information

Privacy Management Strategy

1. The Nature of the Business
2. Information to support the Business
3. Organisational responses to Privacy
4. Information Sharing
5. Architectural Considerations
6. Special Issues

Security management tools

- Privacy Impact Assessment
- Threat & Risk Assessment
- Quantifying Security ROI

Reckoning security ROI

Severity	Description / *Interpretation*	Cost
Insignificant	*Will have almost no impact if threat is realised.* No extra financial impact at all.	$0
Minor	*Will have some minor effect on the asset value. **Will not require any extra effort to repair or reconfigure.*** No financial impact from incident itself but let us assume that a few hours effort may be required to confirm the nature of what has happened.	$1,000
Significant	*Will result in some tangible harm, albeit only small and perhaps only noted by a few individuals or agencies. **Will require some expenditure of resources to repair** (e.g. "political embarrassment").* The approximate cost of a press release to redress "political embarrassment".	$10,000

Ref: www.oict.nsw.gov.au/ pdf/4.4.37.ROSI.pdf

Reckoning security ROI (cont).

Damaging	*May cause damage to the reputation of management, and/or notable loss of confidence in the system's resources or services.* ***Will require expenditure of significant resources to repair.*** Corresponding to the cost of several weeks consultancy to restore resources and services, recover data from backups, conduct investigatiions and so on.	$100,000
Serious	*May cause extended system outage, and/or loss of connected customers or business confidence.* ***May result in compromise of large amounts of Government information or services.*** Corresponding to the cost to totally recover a large set of data, including reverting to original paper files, client interviews and other labor intensive methods.	$1,000,000
Grave	*May cause system to be permanently closed, and/or be subsumed by another (secure) environment.* ***May result in complete compromise of Government agencies.*** Corresponding to a typical agency's annual budget.	$10,000,000

Aims of management tools

- **Privacy Impact Assessment**
- **Threat & Risk Assessment**
- **Quantifying Security ROI**

- ***Pro-activity***
- ***Transparency, What-If modeling***
- ***Engagement of management***

Conclusions

Thank you

Stephen Wilson
Lockstep Consulting
0414 488 851
swilson@lockstep.com.au

