Implementing Information Security Policies and Standards

A Real Life Example

Bruce W. Edwards
Manager – Audit and Assurance - TAS
What we will review

1. Understand – InfoSec, why should we?

2. Assess – Your organisation’s situation

3. Act – Address your organisation’s situation

4. Maintain – Appropriate Information Security which supports privacy
Understand

InfoSec, why should we?

- Recent events – check the media!
- Example - The GCIO security review was prompted by a specific security breach involving MSD kiosks
- The GCIO security review identified wide-ranging and systemic IT security and privacy issues
- Subsequent security and privacy breaches (ACC…) in the public sector heightened the need for attention

The day to day BAU environment!

Is this a surprise?

Understand the situation at your organisation

Security Education Day
‘Keep it safe, keep it simple, keep out of the media’
1 November 2012 - PWC
Why InfoSec Policies and Standards?
Understanding the Challenges

Information Security Requirements, Responsibilities and Expectations

1. Human & Social Vulnerabilities
2. Technological Vulnerabilities

Fast Pace of Change

Regulatory Climate

UofL
Research
Clinical
Athletics
Administration
Donor Fund Raising

Academics

Security
Why InfoSec Policies and Standards?

Understanding the Challenges

Regulatory Climate

- Government
- Suppliers and business partners
- Competitors (Opportunists)
- Employees
- Senior Management
- Clients, Consumers, the Public

Your organisation

Information Security

Human & Social Vulnerabilities

Fast Pace of Change

Requirements, Responsibilities and Expectations
A common foundation to address and/or support…

• Regulations, laws, requirements

• Expectations
  Stakeholders, customers, clients, sponsors, partners/collaborators, shareholders, our constituents, media, the public…

• Efficiency
  Unified approach is more effective, less confusing, easier to understand
  Well designed polices and standards are ultimately an enabler

Numerous areas, similar requirements and expectations
Understand

Why Policies and Standards?

What is a policy? (from http://www.m-w.com/
1 a : prudence or wisdom in the management of affairs b : management or procedure based primarily on material interest
2 a : a definite course or method of action selected from among alternatives and in light of given conditions to guide and determine present and future decisions b : a high-level overall plan embracing the general goals and acceptable procedures especially of a governmental body

UofL InfoSec:
High level requirement statement or paragraph about a type of technology or behavior in the IS/IT/ICT environment.
Understand

Why Policies and Standards?

What are standards?

A required approach for conducting an activity or task, utilizing a product, etc. Many times a standard is a best practice that must be followed to have a better chance of overall success. From: www.tensteppb.com/90.1Glossary.htm

-and/or-

What about good enough?

Descriptive requirements for a behavior based policy.
Procedures:

Clear steps to follow to accomplish specific tasks or behave in certain ways. Procedures should support organization, contractual, regulatory and/or statutory obligations and requirements.

Examples:
- Set-up a software firewall
- Encrypting sensitive email
Why Policies and Standards?

What good are policies?

What would an organisation look like without any policies and standards?

Policies and Standards:

*Set the foundation for compliance expectations* of constituents (employees, senior management, faculty, staff, students, partners, collaborators, vendors, etc.)
UofL’s objectives were:

An organisation with consistent, common-sense policies that:

1. “Pass muster” in the event of a regulatory review or audit

and

2. Allow flexibility for academic, research and operational requirements

3. while supporting the required CIA (confidentiality, integrity and availability) of sensitive information.
Establish InfoSec policies and standards for the organization

What should be included?

Guidance adequate to meet the organisation’s risk tolerance relative to InfoSec risks (incidents, legal and regulatory exposure, lost business, PR…)

To be effective, must take into account:

1. Strategic Alignment
2. Risk Assessment and Management
3. Value Delivery
1. Strategic Alignment

- Align InfoSec with business strategy (support organisational objectives)

*We are in this together!*

- Account for culture, governance style, technology, organisational structure

- Tone from the top - executive support!
2. Risk Assessment and Management

- **Identify InfoSec risks** to the organization
- **Understand** exposure to **consequences** of adverse events
- **Risk mitigation** *only to* acceptable levels of residual risk
- **Educate** - **Risk acceptance** *(inaction is acceptance)*

*Establish InfoSec policies and standards for the organization*

---

*Security Education Day*

"Keep it safe, keep it simple, keep out of the media"

1 November 2012 - PWC

---

*ISACA®*
2. Risk Assessment and Management

**Sensitive Information?**

*Sensitive information* is information of a confidential or proprietary nature as well as other information that would not be routinely published for unrestricted public access or where disclosure is prohibited by laws, regulations, contractual agreements or company University policy.

Sensitive information includes but is not limited to information such as medical and health records, grades and other enrollment information, credit card, bank account and other financial information, social security numbers, personal addresses, phone numbers, etc.

**Note:** Sensitive information does not include personal information of a particular individual which that individual elects to reveal.

---

*Security Education Day*

'Keep it safe, keep it simple, keep out of the media’

1 November 2012 - PWC

[ISACA® logo]
Establish InfoSec policies and standards for the organization

3. Value Delivery

Standard security baseline

- InfoSec policies, standards, procedures now aligned with business objectives and risk tolerance
- Supports InfoSec investments congruent with business objectives and risk tolerance

Assess

Information Security Supports Privacy

Security Education Day
‘Keep it safe, keep it simple, keep out of the media’
1 November 2012 - PWC
3. Value Delivery

- Policy and Standard Adoption
  - Review
  - Buy-in
  - Official Adoption

Assess  Establish InfoSec policies and standards for the organization

BEWARE: Now we are done with that!

Security Education Day
‘Keep it safe, keep it simple, keep out of the media’
1 November 2012 - PWC
Establish InfoSec policies and standards for the organization

Policy Pitfalls to Beware!

* Sufficient mgt buy-in
* Legitimacy of policy source
* Adequacy of policies
* Mgt understanding of trade-offs (stringent vs increased risk)
* Motivation/incentive to follow policy
* Encompasses relevant laws, regs, accepted practice
* Adequate resources
* “One size fits all” approach

* Marketing, awareness, training (training attendance, user ability)
* Regular review and updating
* Policy compliance monitoring and auditing
* Policy and business goals alignment
* Underlying documentation (procedures)
* On-going risk assessment to foster continued examination
* Proactive vs reactive
Where was UofL?

Information Security Policies, Standards and Procedures:

- Disjointed

- Hap-hazard

- Delineation between Policy, Standard, Procedure not always clear, not consistent

- Each policy evolved “organically” to fit a perceived need at the time (not a structured approach)
Assess

Where was UofL?

Information Security Policies, Standards and Procedures:

- Not part of a cohesive, consistent and unified package
- Not organised, no clear cohesion to policies
- Hard to find
- Not effectively communicated to all constituents
- Policies written/implemented in a manner *not* conducive to academic constituent support

Can your users “get behind” the policies?

Security Education Day
‘Keep it safe, keep it simple, keep out of the media’
1 November 2012 - PWC
Where was UofL?

Information Security Policies, Standards and Procedures:

- Old policies DID NOT allow for the *possibility* of self-direction (with regards to technology) within a structured framework

- Unclear and/or inconsistent sanctions

- Sanction enforcement, what is that?

- Unclear Senior Management Support

- Highly variable support within the organization

Different InfoSec policy Approaches:
- General or specific
- Technology neutral or specific

Security Education Day
‘Keep it safe, keep it simple, keep out of the media’
1 November 2012 - PWC

Wellington Chapter
Where is UofL now?

- Support from Senior Management
- Received support for consistently enforced sanctions
- “Radical” approach (for UofL) for this cohesive whole:

* As **technology neutral** as possible
  Policy defines expectations for a technology but not the specific technology that must be used

* **Overall** Policies and Standards
  Not written for a specific regulation (example: HIPAA) but inclusive of regulatory requirements
Policy and Standards Adoption Process

Review and comments from representatives of the University...

- Strategic Technology Executive Committee (Fall 2005)
- Audit Services (Winter 2005-2006)
- InfoSec Awareness Team (Spring 2006)
- InfoSec Policy Review Group (Spring 2006)
- ATC Policy Review Subcommittee (Summer 2006)
- Information and Data Security Task Force (Fall 2006)
- General Counsel (Fall 2006)
- Research Deans (January 9, 2007)
- Council of Academic Officers (March 21, 2007)
- Research Compliance Committee (April 2, 2007)
- HSC Compliance Oversight Committee (April 19, 2007)
- Tier 1 Personnel (all, via e-mail, May 9, 2007)
- Business Advisory Group (May 18, 2007)
- Strategic Technology Executive Committee (June 1, 2007)
- **Compliance Oversight Council (July 23, 2007)**
Where is UofL now?

Policy and Standard Framework

- General
- Accounts and Usage
- Computing Devices
- Network Services
- Data Centers and Facilities

Security Education Day
'Keep it safe, keep it simple, keep out of the media'
1 November 2012 - PWC
Policy and Standards Overview

Information Security and Technology Policy and Standards Map

General
- Information Security Responsibility IS PS001
- Business Continuity Planning and Disaster Recovery IS PS002
- Intellectual Property (IP) IS PS003
- Policy Exceptions IS PS004
- Sanction Policy IS PS005
- Security Incident Policy IS PS006

Accounts and Usage
- User Accounts and Acceptable Use IS PS007
- Passwords IS PS008

Network Services
- Network Service IS PS010
- Web Sites IS PS011

Computing Devices
- Workstation and Computing Devices IS PS012
- Server Computing Devices IS PS013
- Protection from Malicious Software IS PS014
- Backup and Retention of Data IS PS015
- Inventory, Tracking, Discarding or Redeploying Computing Devices or Media IS PS016

Encryption IS PS018

Base level expectations
1. Educate and Encourage Use
   - Training
   - Awareness
   - Consulting
2. Improve Compliance using
   - Consulting
   - Auditing and Monitoring, Assessment, Adjustment
   - Enforcement
3. Maintain Policy Relevance using
   - Self Assessment/audit
   - Feedback
   - Adjustment

'Security Education Day
'Keep it safe, keep it simple, keep out of the media'
1 November 2012 - PWC
Awareness Efforts include Annual Cyber-Security Awareness Week

Security Education Day

'Keep it safe, keep it simple, keep out of the media'

1 November 2012 - PWC
Maintain

Make it safe, keep it simple, keep out of the media

1 November 2012 - PWC

CSA

University of Louisville

security.louisville.edu

Thank you!

We hope you enjoy the Cyber-Security Awareness Week events!
UofL became…

An organisation with consistent, common-sense policies that:

1. “Pass muster” in the event of a regulatory review or audit and
2. Allow flexibility for academic, research and operational requirements
3. while supporting the required CIA (confidentiality, integrity and availability) of sensitive information.
Final points to ponder

1. On-going process of continuous improvement, no guarantees.
2. Diligence, education, awareness (at all levels) can provide a defensible position for compliance risk while supporting our organisations in doing their work effectively.
3. Policies and standards are a key part of this.

-----

4. Tone from the Top
   – Most important: Executive leadership by example
5. Training and Awareness!
   – More important than fancy technology
6. Technology
   – Use technology effectively, not as a substitute for #1 or #2!

Security Education Day
'Keep it safe, keep it simple, keep out of the media'
1 November 2012 - PWC
Questions?

Bruce W. Edwards
CIA, CISA, CISM, CRISC
Manager
Audit and Assurance
TAS/DHBSS
Bruce@BruceEdwards.net.nz
BEdwards@centraltas.co.nz