

## A Model of Information Assurance Benefits

J. Ezingeard, E. McFadzean, & D. Birchall, *Information Systems Management*, Spring 2005, Vol. 22, No.2, pp.20-29.

---

---

---

---

---

---

---

---

## Good Information

- Basis of
  - Good decisions
  - Customer trust
  - Business continuity (sometimes phrased “resilient” systems)
  - Good governance

---

---

---

---

---

---

---

---

## Why the Increase in Information Assurance Interest?

- High level executives have greater interest in security – more so in US than in other countries
- Incidents that have appeared in media – particularly failure of security or the misunderstanding of what information meant
- Publicized cases where executives have distorted information

---

---

---

---

---

---

---

---

Who Is Leading The Charge To Make Executives More Aware of Information Assurance?

- Note the Deloitte as well as the Ernst & Young references
- Many senior executives are of a mindset that information security is a technology issue – it is also a policy and governance issue
- In the end, senior executives must understand the return on investment for information assurance

---

---

---

---

---

---

---

---

Information Assurance ROI

- Direct versus indirect
- Tangible vs intangible
- Recurring vs non-recurring

---

---

---

---

---

---

---

---

Define Information Assurance

- Information security is one aspect of information assurance, but it is not the whole definition
- 3 properties
  - Confidentiality
  - Integrity – not corrupted or unintentionally deleted
  - Availability – remember that information is needed close to the time that a decision is required
    - also **identification** and **authentication**
    - (buried in the paragraph) **non-repudiation** which means the organization can assure the information is accurate

---

---

---

---

---

---

---

---

### U.K. Information Assurance

- "... the certainty that the information in the organization is reliable, secure, and private. IA encompasses both the accuracy of information and its protection."
- Business continuity is part of the mindset for information assurance, how should this be reflected in an organization's disaster plan?

---

---

---

---

---

---

---

---

### Threats to Information Assurance

- Many (but not all) can be identified
- Knowing that they will occur is not the same as **knowing when** they will occur
- Believing the organization has a plan to react to a threat is not the same as **knowing** the plan will work

Just because you have driven a car for years does not mean you are capable of driving in a NASCAR race

---

---

---

---

---

---

---

---

### The "Problem Prevention" Attitude

- Can lull an organization into a false sense of security
- Prevention can lead to fixed responses when an agile approach to responses is the essence of preparedness
- A metric to measure information assurance can be in opposition to the organization's goals
  - Remember, an organization that collects no data will not risk a lapse in IA but it will go out of business

---

---

---

---

---

---

---

---

### The Inevitability of Risk

- Organizations profit from risk
- Organizations better able to manage risk will show higher profits
- Risk management is superior to risk prevention

---

---

---

---

---

---

---

---

### Enabling Approach

- How can an organization achieve competitive advantage with information assurance?
- Forces an organization to take a “forward thinking” approach to the information asset

---

---

---

---

---

---

---

---

### Avoiding Negative Strategic Consequences of Poor Information Assurance

- Information system breaches can cause irreparable harm to an organization
- Information assurance should be part of the corporate strategy, not vice versa
- “Good faith” is no longer sufficient, an organization's stakeholders require that an organization actually deliver on the promise of information assurance

---

---

---

---

---

---

---

---

### Information Assurance Benefits

- Article gives four
  - Operational (e.g. supply chain management)
  - Tactical (e.g. better control and business intelligence)
  - Strategic (e.g. alignment to stakeholders' expectations)
  - Organizational (i.e. those sought by organization stakeholders)
- What about societal benefits?

---

---

---

---

---

---

---

---

### Implications of Information Assurance

- Article focuses on
  - Holistic picture of the controls and processes
  - Compliance
  - Alignment of IA to corporate strategy
  - Trickle-down to lower level employees
  - Ability of the IA plan to make adjustments
- What implications can you envision?

---

---

---

---

---

---

---

---

### Operational Benefits from Information Assurance

- Makes information systems "resilient"
- Improves access in that assurance empowers easy-to-use systems (e.g. less error-checking is required)
- When decision makers trust the information system, more use of the system follows

---

---

---

---

---

---

---

---

### Tactical Benefits from Information Assurance

#### Assurance

- Easier to comply with outside demands for compliance (such as Sarbanes- Oxley)
- Reduced complexity (redundant systems and data are frequently found when information assurance principles are not applied)
- Applying assurance forces managers to deal with tactical issues – such as consistency across functional areas
- In general, managers better understand a system when they are forced to examine and defend it; they must do this for information assurance

---

---

---

---

---

---

---

---

### Strategic Benefits from Information Assurance

#### Assurance

- This is the weakest part of the authors' case
  - Better governance
  - Cheaper equity
  - More sales
  - Lower costs

---

---

---

---

---

---

---

---

### Implications

- Actually, there are far reaching implications
  - Senior corporate managers must understand information assurance if it is to be implemented
  - Requires a broad study of information systems in the firm as opposed to looking at each separately
  - Requires that information assurance principles (applied to the organization's information systems) is well communicated to all employees

---

---

---

---

---

---

---

---