Outline of today’s lecture

1. Why a security policy?
2. Approaches to security

1. Why a security policy?

According to Higgins (1999: 217),

‘Without a policy, security practices will be developed without clear demarcation of objectives and responsibility, leading to increased weakness.’
1. The impetus of legislation?

As we saw last week, much of the push for information policy within organisations has come from outside, in the form of new laws regulating matters such as the privacy of personal data.

1. What is a security policy?

Weise & Martin (2001: 3) put it this way:

A formal statement of the rules through which people are given access to an organization’s technology, system and information assets. The security policy defines what business and security goals and objectives management desires, but not how these solutions are engineered and implemented.

They add that ‘the characteristics of good security policies’ must:

– ‘be implementable through system administration procedures, publishing of acceptable use guidelines, or other appropriate methods’
– ‘be enforceable with security tools, where appropriate, and with sanctions, where actual prevention is not technically feasible’
1. What is a security policy?

They add that ‘the characteristics of good security policies’ must:
– ‘clearly define the areas of responsibility for the users, administrators, and management’
– ‘be documented, distributed, and communicated’

1. Role of the Chief Information Officer (CIO)

• Key responsibility for IT policy
• Consulting with whom?
• How is policy realised?

1. Selling policy to management

May (1998: 127) says the role of the CIO can be overstated:
– ‘The CIO is not in charge of anything’
– ‘high-priced machines, not information, are the things being managed’
– ‘in most cases, the CIO is not an officer of the company’
1. Selling policy to management

According to Dutton & Ashford (1993), policy success in organisations often depends more on sales pitch and individual credibility, and less on a case’s intrinsic merits.

2. Approaches to security

- Where do threats lie?
- Shifting notions of information security
- PC security or information security?
- Relations with other organisations
- Appropriate policy responses

2. Where do threats lie?

What do we commonly understand as information security?

- Often equated with IT security
- Threats often seen as primarily external
- Physical security? / electronic security? / both?
- Meaning and parameters of information security have shifted over the years
2. Shifting notions of information security

Gerber et al. (2001: 33) argue that established approaches to security that seek to address:
- risks to organisation
- legal and other requirements (e.g., to trading partner)
- the organisation’s approach to information processing
are better suited to the protection of physical assets than of information.

2. Information security = IT security?

No more than information policy always means simply IT policy ...

‘the issue is not just about protecting the technology, it’s about protecting business or personal information wherever it resides’

(Wills, quoted in Gerber et al. 2001: 32)

2. Threats - primarily external?

- Denial of service attacks on the increase in recent years?
- Hackers popularly portrayed as a key threat
- Hard to quantify information security losses, for a range of reasons
2. Threats - primarily external?

According to Meyer et al. 1995 (cited in Loukis & Spinellis 2001), threats to security are posed by:

– malicious authorised users
– negligent authorised users
– outsiders

2. Consequences of security breaches

According to Meyer et al. 1995 (cited in Loukis & Spinellis 2001), breach of electronic data security can lead to:

– Disclosure
– Modification
– Fabrication
– Repudiation

2. Shifting notion of information security

We can see this especially in the narrow sense of IT security, which has changed over the years as systems have become more intricate and dispersed

(Thomson & von Solms 1998)
2. Mainframe security

- Number of users at a given time: one (at least in the early days)
- Major security consideration: physical access
- Major threat: environmental
- Policy implications: simple, limited in scope

2. Multi-user network security

Central computer became connected to a network of dumb terminals distributed within other sections of the organisation

- Major security consideration: physical & electronic access
- Number of users at a given time: many
- Major threat: password disclosure
- Policy implications: largely technical (managed by OS)
2. PCs connected through the Internet

The situation today, with networked stand-alone PCs within the organisation, and connectivity to the outside world via the Internet

- Major security consideration: network access
- Number of users at a given time: many
- Major threat: ???
- Policy implications: both technical & personnel issues

2. What prompts security-threatening behaviour?

Many writers turn to social psychology, seeing the source of the ‘problem’ in human behaviour:

- People are ‘naturally inclined’ towards crime
- Probability of criminal acts as often a consequence of friendship circles
2. PC security or information security?

Helms et al. (2000) argue that one of the easiest ways for external agents to obtain security-related information is through human contact ("social engineering"), not electronic data incursion/interception.

2. Relations with other organisations

- The emergence of the Internet has facilitated (and encouraged) growing exchanges of information between organisations.
- Information security breaches can threaten important relations with others.
- Then again, some writers advise wariness when appraising "seemingly friendly rapports with outside entities" (Helms et al. 2000: 121).

2. Appropriate policy responses

- Internal measures
- Recourse to the law?
- Retaliation?
- A case study
2. Internal measures

- Wood (1997) suggests the separation of duties as one key to security policy - but this may be hard to realise in small organisations

- Many other writers focus on securing staff compliance, arguing that:

  ‘Employees put information at risk the moment they open their mouth’

  (Helms et al. 2000: 120)

What will motivate staff to comply?

Can use be made of ‘other means than punishment’?

(Siponen 2000b: 197)

2. Internal measures – selling policies to staff?

‘Selling means persuading people to do something that they would not do knowing all the facts’

(Siponen 2000a: 35)

– Therefore, ‘guidelines should always be justified’

(Siponen 2000a: 36)
2. Internal measures

Overzealous security policies can create problems of their own:

- ‘Oppressive work environment’
- ‘Compartmentalization of information’
- ‘Duplication of effort’
- ‘Falsely generated paranoia’

(Helms et al. 2000: 127, 118)

2. Recourse to the law?

What are the risks here?

- Disclosure
- Loss of competitive edge
- Loss of face

2. Retaliation?

Cybervigilantism:

‘the proactive process of responding to information attacks by hackers (from whatever source) with corresponding attacks on them’

(Hutchinson & Warren 2001: 106)
2. Retaliation?

**Cybervigilantism:**

‘the proactive process of responding to information attacks by hackers (from whatever source) with corresponding attacks on them’

(Hutchinson & Warren 2001: 106)

2. Cybervigilantism - (Hutchinson & Warren 2001: 108)

Survey of 111 IT managers in Western Australia and Victoria:

- Pentagon right in striking back against hackers: 73%
- Your organisation has been attacked: 14%
- Your organisation has a right to retaliate: 65%
- Better left to authorities: 60%
- People have a right to attack controversial web sites: 64%
- Your organisation has a right to expect others will respect integrity of its site: 98%
- Your organisation has a policy re hackers etc: 33%
- Attack from a competitor organisation is a real threat: 30%

2. Case study - the Greek public sector

Loukis & Spinellis (2001) surveyed 53 organisations, many of them with small IT systems (and some problems gathering data)

- Most common procedure was backup
- More than half had logical and physical security zones
- Less than a quarter had an IS security plan or policy
- ‘Critical organisations’ (eg hospitals, banks, soc security) were most likely to have advanced measures
### 3. Further reading

<table>
<thead>
<tr>
<th>Author(s)</th>
<th>Title</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>M. Garber et al. (2001)</td>
<td>'Formulating information security requirements',</td>
<td>IM&amp;S 9(1).</td>
</tr>
<tr>
<td>M. Helme et al. (2000)</td>
<td>'Shielding your company against information compromise',</td>
<td>IM&amp;S 8(3).</td>
</tr>
<tr>
<td>W. Hutchinson &amp; M. Warren (2001)</td>
<td>'Attitudes of Australian information system managers against online attackers',</td>
<td>IM&amp;S 9(3).</td>
</tr>
<tr>
<td>M. Siponen (2000a)</td>
<td>'Critical analysis of different approaches to minimizing user-related faults in information systems security: implications for research and practice',</td>
<td>IM&amp;S 8(5).</td>
</tr>
<tr>
<td>G. White &amp; S. Pearson (2001)</td>
<td>'Controlling corporate e-mail, PC use and computer security',</td>
<td>IM&amp;S 9(2).</td>
</tr>
</tbody>
</table>