IMS3110
INFORMATION SYSTEMS SECURITY

Managing Security in the organisation
Impact of E-commerce on the organisation
Lecturer: Sue Foster
Week 6

Learning Objectives

- Review the lecture outcomes from Week 5
- Describe risk mitigation in relation to issues surrounding organisations conducting e-business
- Understand the business risks of conducting e-commerce in organisations
- Discuss the security risks facing organisations conducting e-commerce

Weekly IS Security topics

<table>
<thead>
<tr>
<th>Week</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Assignment 1 due in tutorials = 5%</td>
</tr>
<tr>
<td>6</td>
<td>Security design</td>
</tr>
<tr>
<td>7</td>
<td>E-commerce – Internet security</td>
</tr>
<tr>
<td>8</td>
<td>Risk Management: Step 1: Risk analysis and assessment</td>
</tr>
<tr>
<td>9</td>
<td>Business continuity plans (BCP) and disaster recovery</td>
</tr>
<tr>
<td>10</td>
<td>Security policies etc</td>
</tr>
<tr>
<td>11</td>
<td>Security design</td>
</tr>
<tr>
<td>12</td>
<td>BCP and disaster recovery</td>
</tr>
</tbody>
</table>

*Extract from: Managing Security of Information
By: Robert G. Parker, Deloitte & Touche LLP
Deepak Sarup, ALLTEL International Resource
Patrick Stachtchenko, Deloitte Touche Tohmatsu, January 1998 (p.4)

The concept of security applies to all information.

Security relates to the protection of valuable assets against loss, disclosure, or damage. In this context, valuable assets are the data or information recorded, processed, stored, shared, transmitted, or retrieved from an electronic medium. The data or information must be protected against harm from threats that will lead to its loss, inaccessibility, alteration or wrongful disclosure.

The protection is through a layered series of technological and non-technological safeguards such as physical security measures, background checks, user identifiers, passwords, smart cards, biometrics, firewalls, etc. Security applies to all information. The security concept is summarized in the security objective.

Security Objective: The objective of information security is "the protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality, and integrity."
Holistic approach to IS security

Risk management

- Risk analysis/assessment
  - Determine critical assets
  - Analyse threats
  - Statistics
  - Current/future trends
  - Establish vulnerabilities
  - Perform gap analysis

RISK MANAGEMENT

Security Framework – goals of IS security
- Confidentiality
- Availability
- Integrity
- Authentication
- Accountability

Security Controls

PROVIDE:
- Protection for vulnerabilities
- Countermeasures against access breaches

Step 2 – Risk Mitigation

The outcome from the risk assessment is used to identify the optimum set of mitigation (control) measures.

Security Controls

- Controls are policies, procedures, techniques, devices, systems, and other measures, which may be taken to reduce the opportunity for unauthorised access to a system
  - Examples?
    - Control relational model
  - Defence in depth
    - Refers to a variety of security overlays implemented to prevent unauthorised access
Controls

Four types:
- Deterrent controls
  - reduce the likelihood of a deliberate attack
  - Example?
- Preventative controls
  - protect vulnerabilities and make an attack unsuccessful or reduce its impact
- Corrective controls
  - reduce the effect of an attack
- Detective controls
  - discover attacks and trigger preventative or corrective controls


Control Relational Model

Preventative Control

Detective Control

Corrective Control

Deterrent Controls

What Else Can You Do??

Put in place sophisticated SECURITY CONTROLS
- Intrusion detection systems
- Firewalls
- Anti virus software - updates
- Vulnerability Scanning and analysis tools
  - Provide automatic patching and updates
- Security policies and procedures
- Security logs = audits

Defence In Depth solution – A Layered Strategy

Physical defence
- Security policies and procedures
- Access controls

Network defence
- Intrusion detection systems
- Firewalls

Application protection
- Encryption
- Policy definition and management
- OCTAVE/CRAMM/COBRA

Rule management
Learning outcomes:

- Define e-commerce and describe the numerous terms that reflect an e-commerce perspective
- Discuss the implications to organisations that enter into an e-commerce initiative
- Describe the numerous risks to organisations and customers in relation to E-Commerce

E-COMMERCE

E-Commerce refers to all commercial activity conducted with the aid of electronic devices or via computers connected to each other using some medium – internet

Computers also include:
- hand held devices (PDAs)
- M-commerce
  - Mobile phones

Further definitions

Often referred to as simply e-commerce, business that is conducted over the Internet using any of the applications that rely on the Internet, such as e-mail, instant messaging, shopping carts, Web services, and EDI, among others.

Electronic commerce can be between two businesses transmitting funds, goods, services and/or data or between a business and a customer.

The Terms!!

Electronic Commerce

- E-banking: organising accounts and paying bills
- E-shopping: purchasing goods from a website
- E-tailing: selling goods to shoppers from a website
- B2B: Sending and receiving orders to and from business partners
- E-govt: lodging tax returns, business activity statement (BAS), conducting other transactions with other government agencies
- E-marketplace
- E-globalisation

---

E-business Reality

Customer perspective:
But I Ordered It on the Web Months Ago...

Problems Shipping Online

- 28% Experienced problems with order
  (order not delivered)
- 18% Ordered goods that never arrived
- 9% Ordered goods that never arrived but were billed
- 4% Ordered goods that were never billed
- 1% Tried to contact supplier via e-mail without success
- 7% Ordered goods that did not arrive by specified date or time
- 5% Ordered goods that did not meet specifications
- 1% Order was processed more than once

Source: Gartner Group, January 2000
Boston Group, Forrester Research
and Yankee Group, 1999

---

Projected growth in E-commerce

- Yankee Group
- Boston Cons. Group
- Forrester Research
- Gartner Group

Source: Gartner Group, January 2000
Boston Group, Forrester Research
and Yankee Group, 1999
The B2B market in the US is projected to grow to approximately $1.5 trillion in 2004.

- B2B is still in the early adopter phase.
- By 2004 20% of B2B sales in the chemical industry will be internet based.
- Asia is embracing eCommerce sooner than anticipated.
  - IDC predict B2B in Asia (excluding Japan) will grow to $32.6 billion in 2003.
  - B2B sales in Japan will reach $62 billion in same period
So is eCommerce Real?

- Commercial use of the internet is only 5 years old
- Over half of Schwab’s transactions come over the Net
- In just 4 years Amazon became the USA’s 3rd largest bookseller
- Cisco takes 99%+ of their orders over the Net
- Over 50% of ALL new/secondhand car buyers do their research over the Net
- Australian Wine Society
  - http://www.wine-searcher.com/
- Sony Playstation

Who is using it?

- 40,000,000+ businesses worldwide
  - <10% have “active” websites
- The Fortune 1000
  - Most have websites
  - >80% have functional intranets (beyond email)
  - <25% conduct REAL eCommerce (trading partners)
- < 10% Conducting Ecommerce
- Have Commerce Sites Integrated To Back Office Fulfillment Systems

WHY???

- 50% reduction in processing time
  - Fisher Scientific, 3M
- Reduction in purchasing costs from $45 to $1.50 per order
  - GE and 3Com
- 50% reduction in the time taken to order parts and therefore a saving of $2 mil. In stored value
  - Alaska Airlines
The 2000 Executive View: Drivers of E-Business

- Improved accessibility
- New business partners
- Worldwide presence 24x7
- New sales channels

Opportunities
- New Business Models
- Improved accessibility
- New business partners
- Worldwide presence 24x7
- New sales channels
- Saving Potential

- Employees
  - More responsibility
  - Less administration
  - Less training

Opportunities and Challenges

- Employees
  - More responsibility
  - Less administration
  - Less training

Challenges
- Increasing Global Competition
  - Greater price transparency
  - Better product comparability

Success factors
- 1 to 1 marketing
- Logistics organisation

Consequences for existing logistical processes and partnerships
Economic implications of e-commerce

- Stakeholder Protection (security of transactions and issues of availability)
- Business Ethics and Compliance (issues of privacy)
- Technology Neutrality
- Information Transparency
- Cost Effectiveness

Risks within e-business

<table>
<thead>
<tr>
<th>E-business Risks and Snapshots</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic Direction</td>
</tr>
<tr>
<td>------------------------</td>
</tr>
<tr>
<td>Success of e-business initiative is directly linked to the company’s ability to develop and implement a strategic plan.</td>
</tr>
<tr>
<td>This plan can help in:</td>
</tr>
<tr>
<td>- Identifying major business growth initiatives</td>
</tr>
<tr>
<td>- Identifying gaps</td>
</tr>
<tr>
<td>- Reducing channel conflicts</td>
</tr>
<tr>
<td>- Benchmarking against best practices</td>
</tr>
</tbody>
</table>

- Channel Enhancement - Failure to realize strategic implications for sell side - Buy side risks are relatively low - Increased exposure to failure as partners involved.
- Industry Transformation - Risks associated with discarding traditional business models
- Convergence - Risks associated with investment and direction
Risks: Competitive Environment

- As more companies exploit e-business the competition in stable markets increases.
- Implementation delays pose risk to "first mover" advantage.
- Ability for companies to match other company’s offerings.
- Barriers for establishing business partnerships are reduced.
- Increasing global competition.
- Increase in customer expectations
- Price and product transparency.

<table>
<thead>
<tr>
<th>Competitive Environment</th>
<th>Value Chain Integration</th>
<th>Industry Transformation</th>
<th>Convergence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel Enhancement</td>
<td>Value Chain Integration</td>
<td>Industry Transformation</td>
<td>Convergence</td>
</tr>
</tbody>
</table>

Risks: Dependence on Others.

- New partnerships cause a shift in the balance of power.
- Previously guarded processes could be handled by outside partners.
- Which Processes and what Risks?
- Implies a level of trust — Proprietary information
- Joint problem solving and strategic development

<table>
<thead>
<tr>
<th>Dependence on Others</th>
<th>Value Chain Integration</th>
<th>Industry Transformation</th>
<th>Convergence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel Enhancement</td>
<td>Value Chain Integration</td>
<td>Industry Transformation</td>
<td>Convergence</td>
</tr>
</tbody>
</table>

Risks: Security

- Trust cannot be established without effective security
- Information Technology Infrastructure must support:
  - Confidentiality - Privacy
  - Integrity
  - Availability
  - Authentication — Identification, authorisation
  - Nonrepudiation
  - Accountability
- Automated channel connection to partners increases risk

<table>
<thead>
<tr>
<th>Security</th>
<th>Value Chain Integration</th>
<th>Industry Transformation</th>
<th>Convergence</th>
</tr>
</thead>
</table>

Security: The Core Issues

- THREATS
- INFORMATION SYSTEM SECURITY
  - Confidentiality, availability, integrity, authentication
- CONTROLS
- VULNERABILITIES
- BUSINESS RISKS FROM E-COMMERCE
Risks: Reputation
- Competitors without walls can quickly establish reputations.
- Managing customer expectations.
- Web page becomes the face of the company
  - Appearance
  - Navigation
  - Learning
  - Content
  - Speed
  - Errors

Risks: Culture
- E-business brings with it cultural change at the highest level.
- Employees maybe acting on behalf of other partners.
- Global languages and customs must be understood.
- Change management issues
- Executive leadership

Risks: Technology
- Solution selection
- Poor performance and lack of reliability
- User Training of new systems
- Speed at which the system becomes obsolete
  - Internally
  - Externally

Risks: Governance (management)
- Appropriate organisational structure to support e-business initiatives:
  - Central leadership Vs cross functional
- Auditing personnel need to understand e-business legal and security requirements
- Partners need to be involved in decisions.
- Thorough and open documentation required to prevent misinterpretation.
- Protection of intellectual property.
Risks: Project Management

- Top level commitment
- Change management risks
- E-business integration
- Data standards
- Lack of coordination across the company and partners

<table>
<thead>
<tr>
<th>Channel Enhancement</th>
<th>Value Chain Integration</th>
<th>Industry Transformation</th>
<th>Convergence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Management</td>
<td>1</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

Risks: Operations

- Lack of E-skills
  - Development
  - Maintenance
- Business Continuity Plans
- Scalability

<table>
<thead>
<tr>
<th>Channel Enhancement</th>
<th>Value Chain Integration</th>
<th>Industry Transformation</th>
<th>Convergence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operations</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

Risks: Legal and Regulatory

- Business practices must match latest legislation.
- Lack of clarity
- Clash of laws and culture
- Conflicting jurisdictions
- Intellectual property
- Piracy of web page content
  - Recourse?

<table>
<thead>
<tr>
<th>Channel Enhancement</th>
<th>Value Chain Integration</th>
<th>Industry Transformation</th>
<th>Convergence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal and Regulatory</td>
<td>3</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

Risks: Business Process Controls

Typical risks

- Backup/recovery procedures.
- Problems affect the entire enterprise.
- New business rules
- Support

<table>
<thead>
<tr>
<th>Channel Enhancement</th>
<th>Value Chain Integration</th>
<th>Industry Transformation</th>
<th>Convergence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business process controls</td>
<td>2</td>
<td>4</td>
<td>3</td>
</tr>
</tbody>
</table>
Main Trends (1)

- The E-Conomy goes main street
  Online consumers with high expectations in terms of information quality, transaction usability and speed of delivery appear
- The wired workforce arises
  More information will be given to employees - direct involvement of nearly all employees in business processes through intranet technology and specific applications (virtual work community)
- Companies tear down information boundaries
  Joint business processes with partners are established by sharing information - B2B e-commerce takes off

Main Trends (2)

- Products become commodities
  The value of an offer (and the difference to others) will not be primarily the product itself - dynamic and individual presentation (incl. prices etc) will be key
- Behaviour & Interaction becomes valuable data
  Analysis of customer behaviour and dynamic reactions in real time lead to customer centric applications
- Virtual Communities are formed
  Specific knowledge / content will be exchanged in communities
- Networks allow new forms of learning
  Knowledge management and continuous learning on a self-service basis to "create" the empowered employee

Legally Speaking!!

- E-commerce is replacing a global marketplace tradition of signed writings as the ultimate best evidence of the law of contract to one of electronic intangible records
- There is little evidence that an electronic record will be considered conclusive legal proof
- The value of an electronic record often depends on the effectiveness of the security controls that have been instituted to protect the authenticity and integrity of the record
**E-commerce the issues**

- Vendor issues
- Stakeholder trust and confidence
- Legality
- Privacy
- Financial
- Risk
- Accountability
- Confidentiality
- Availability
- Integrity
- Non-repudiation
- Audibility
- Contractual obligations

**Non-Repudiation**

- To reject with denial
- Refuse to acknowledge and not pay

Particularly an issue in e-commerce where users may repudiate or deny transactions

**Trust And Confidence**

Factors that affect trust:

- Opportunities for fraud
- Electronic transactions are quick — lessening the opportunity to investigate trustworthiness
- Web sites constantly change — new URLs
- Here today — gone tomorrow

Issues: accountability, reliability, authentication

- Business is becoming more international entailing problems associated with cross border transactions
- Established relationships assume less importance — no personal service

**Non Repudiation**

- In business it is necessary to ensure the other party cannot later deny they are bound by the contract
  - The goal of non-repudiation
  - Forged signature
  - Signed under duress
- In a manual arrangement reduce the chance of this happening
  - All parties sign written documents
  - Use clear straightforward language
- In an ecommerce agreement?
The lecture today has only briefly touched on some of the many issues that impact on organisations that have developed or are thinking of developing an e-business initiative. Some of the organisations who jumped into e-business fairly early, without first considering the implications did not survive—simply because they were unprepared for the influx of online orders. Now organisations and customers have the added uncertainty of the security of transactions when conducting business online.

**References**

- Survivability protecting your critical systems located at: http://www.cert.org/archives/project/critical-systems.html
- Please look at this power point slide: [http://www.gsa.gov.hk/gov01/30/bullet02.pdf](http://www.gsa.gov.hk/gov01/30/bullet02.pdf)
- Please look at this power point slide: [http://www.sans.org/top20/top20paller03.pdf](http://www.sans.org/top20/top20paller03.pdf)

**Revision Questions**

- What are the main risks to organisations conducting e-commerce?
- What main types of security controls would you put in place to support an e-commerce initiative?
- Link those security controls to the control relational model and a defence in depth strategy.