Securing Information System: Facebook (Chap. 8)

1031CSIM4C08
TLMXB4C (M1824)
Tue 2, 3, 4 (9:10-12:00) B425

Min-Yuh Day
Assistant Professor
Dept. of Information Management, Tamkang University

http://mail.tku.edu.tw/myday/
2014-11-04
<table>
<thead>
<tr>
<th>Week</th>
<th>Date</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>103/09/16</td>
<td>Introduction to Case Study for Information Management</td>
</tr>
<tr>
<td>2</td>
<td>103/09/23</td>
<td>Information Systems in Global Business: UPS (Chap. 1)</td>
</tr>
<tr>
<td>3</td>
<td>103/09/30</td>
<td>Global E-Business and Collaboration: NTUC Income (Chap. 2)</td>
</tr>
<tr>
<td>4</td>
<td>103/10/07</td>
<td>Information Systems, Organization, and Strategy: iPad and Apple (Chap. 3)</td>
</tr>
<tr>
<td>5</td>
<td>103/10/14</td>
<td>IT Infrastructure and Emerging Technologies: Salesforce.com (Chap. 5)</td>
</tr>
<tr>
<td>6</td>
<td>103/10/21</td>
<td>Foundations of Business Intelligence: Lego (Chap. 6)</td>
</tr>
</tbody>
</table>
課程大綱 (Syllabus)

週次 (Week)  日期 (Date)  內容 (Subject/Topics)
7  103/10/28  Telecommunications, the Internet, and Wireless Technology: Google, Apple, and Microsoft (Chap. 7)
8  103/11/04  Securing Information System: Facebook (Chap. 8)
9  103/11/11  Midterm Report (期中報告)
10  103/11/18  期中考試週
11  103/11/25  Enterprise Application: Border States Industries Inc. (BSE) (Chap. 9)
12  103/12/02  E-commerce: Amazon vs. Walmart (Chap. 10)
<table>
<thead>
<tr>
<th>週次</th>
<th>日期</th>
<th>內容（Subject/Topics）</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>103/12/09</td>
<td>Knowledge Management: Tata Consulting Services (Chap. 11)</td>
</tr>
<tr>
<td>14</td>
<td>103/12/16</td>
<td>Enhancing Decision Making: CompStat (Chap. 12)</td>
</tr>
<tr>
<td>15</td>
<td>103/12/23</td>
<td>Building Information Systems: Electronic Medical Records (Chap. 13)</td>
</tr>
<tr>
<td>16</td>
<td>103/12/30</td>
<td>Managing Projects: JetBlue and WestJet (Chap. 14)</td>
</tr>
<tr>
<td>17</td>
<td>104/01/06</td>
<td>Final Report (期末報告)</td>
</tr>
<tr>
<td>18</td>
<td>104/01/13</td>
<td>期末考試週</td>
</tr>
</tbody>
</table>
Chap. 8
Securing Information System:
Facebook:
You’re on Facebook? Watch out!

Case Study: Facebook (Chap. 8) (pp.319-320)

You’re on Facebook? Watch out!

1. What are the key security issues of the Facebook?
2. Why is social-media malware hurting small business?
3. How to manage your Facebook security and privacy?
4. What are the components of an organizational framework for security and control?
5. Security isn’t simply a technology issue, it’s a business issue. Discuss.

Overview of Fundamental MIS Concepts

Overview of fundamental MIS Concepts
using an Integrated framework for
describing and analyzing information systems

- Develop security policies and plan
- Deploy security team
- Implement Web site security system
- Implement authentication technology
- Implement individual security technology

Business Challenges
- “Social” nature of Web site
- Gigantic user base

Management

Organization

Information System
- Launch malicious software
- Launch spam
- Steal passwords and sensitive financial data
- Hijack computers for botnets

Business Solutions
- Disable computers
- Invade privacy
- Increase operating cost

You’re on Facebook? Watch Out!

• Facebook – world’s largest social network

• Problem – Identity theft and malicious software

  – Examples:
    • 2009 18-month hacker scam for passwords, resulted in Trojan horse download that stole financial data
    • Dec 2008 Koobface worm
    • May 2010 Spam campaigned aimed at stealing logins

• Illustrates: Types of security attacks facing consumers

• Demonstrates: Ubiquity of hacking, malicious software

SYSTEM VULNERABILITY AND ABUSE

• Why Systems are Vulnerable
• Malicious Software: Viruses, Worms, Trojan Horses, and Spyware
• Hackers and Computer Crime
• Internal Threats: Employees
• Software Vulnerability

CONTEMPORARY SECURITY CHALLENGES AND VULNERABILITIES

- Unauthorized access
- Errors
- Tapping
- Sniffing
- Message alteration
- Theft and fraud
- Radiation

- Hacking
- Viruses and worms
- Theft and fraud
- Vandalism
- Denial-of-service attacks

WI-FI SECURITY CHALLENGES

Hackers and Computer Crime

• Spoofing and Sniffing
• Denial-of-Service Attacks
• Computer Crime
• Identity Theft
• Click Fraud
• Global Threats: Cyberterrorism and Cyberwarfare

Information Security

• Preservation of **confidentiality, integrity and availability** of information; in addition, other properties such as **authenticity, accountability, non-repudiation and reliability** can also be involved

[ISO/IEC 17799:2005]
Information Security Management System (ISMS)

• that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security

– NOTE: The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

Source: ISO/IEC 27001:2005
PDCA model applied to ISMS processes

Source: ISO/IEC 27001:2005
INTERNATIONAL STANDARD ISO/IEC 27001
Information technology — Security techniques — Information security management systems — Requirements

Contents
Foreword
0 Introduction
1 Scope
2 Normative references
3 Terms and definitions

4 Information security management system

5 Management responsibility
6 Internal ISMS audits
7 Management review of the ISMS
8 ISMS improvement

Annex A (normative) Control objectives and controls
Annex B (informative) OECD principles and this International Standard
Bibliography

Source: ISO/IEC 27001:2005
INTERNATIONAL STANDARD ISO/IEC 27001
Information technology — Security techniques — Information security management systems — Requirements

Contents
Foreword
0 Introduction
  0.1 General
  0.2 Process approach
  0.3 Compatibility with other management systems
1 Scope
  1.1 General
  1.2 Application
2 Normative references
3 Terms and definitions

Source: ISO/IEC 27001:2005
4 Information security management system

4.1 General requirements

4.2 Establishing and managing the ISMS

   4.2.1 Establish the ISMS

   4.2.2 Implement and operate the ISMS

   4.2.3 Monitor and review the ISMS

   4.2.4 Maintain and improve the ISMS

4.3 Documentation requirements

   4.3.1 General

   4.3.2 Control of documents

   4.3.3 Control of records

Source: ISO/IEC 27001:2005
5 Management responsibility

5.1 Management commitment
5.2 Resource management
  5.2.1 Provision of resources
  5.2.2 Training, awareness and competence
6 Internal ISMS audits

7 Management review of the ISMS
   7.1 General
   7.2 Review input
   7.3 Review output

8 ISMS improvement
   8.1 Continual improvement
   8.2 Corrective action
   8.3 Preventive action

Source: ISO/IEC 27001:2005
INTERNATIONAL STANDARD ISO/IEC 27001
Information technology — Security techniques — Information security management systems — Requirements

Annex A (normative) Control objectives and controls
Annex B (informative) OECD principles and this International Standard
Bibliography
PDCA Improvement Cycle

1. Plan
   - Establish ISMS

2. Do
   - Implement and Operate the ISMS

3. Check
   - Monitor and review the ISMS

4. Act
   - Maintain and Improve the ISMS
BUSINESS VALUE OF SECURITY AND CONTROL

- Legal and Regulatory Requirements for Electronic Records Management
- Electronic Evidence and Computer Forensics

ESTABLISHING A FRAMEWORK FOR SECURITY AND CONTROL

• Information Systems Controls
• Risk Assessment
• Security Policy
• Disaster Recovery Planning and Business Continuity Planning
• The Role of Auditing

General Controls

- Software controls
- Hardware controls
- Computer operations controls
- Data security controls
- Implementation controls
- Administrative controls

TECHNOLOGIES AND TOOLS FOR PROTECTING INFORMATION RESOURCES

• Identity Management and Authentication
• Firewalls, Intrusion Detection Systems, and Antivirus Software
• Securing Wireless Networks
• Encryption and Public Key Infrastructure
• Ensuring System Availability
• Security Issues for Cloud Computing and the Mobile Digital Platform
• Ensuring Software Quality

PUBLIC KEY ENCRYPTION

DIGITAL CERTIFICATES

Institution/individual subject

Request certificate

Internet

Certificate received

Digital Certificate Serial Number
Version
Issuer Name
Issuance/Expiration Date
Subject Name
Subject Public Key
CA Signature
Other Information

Certification Authorities (CAs)

Transaction partner: online merchant or customer

Case Study: BSE (Chap. 9) (pp.392-394)

Border States Industries (BSE) Fuels Rapid Growth with ERP

1. What problems was Border States Industries encountering as it expanded? What management, organization, and technology factors were responsible for these problems?

2. How easy was it to develop a solution using SAP ERP software? Explain your answer.

3. List and describe the benefits from the SAP software.

4. How much did the new system solution transform the business? Explain your answer.

5. How successful was this solution for BSE? Identify and describe the metrics used to measure the success of the solution.

6. If you had been in charge of SAP’s ERP implementations, what would you have done differently?
資訊管理個案
(Case Study for Information Management)

1. 請同學於資訊管理個案討論前
   應詳細研讀個案，並思考個案研究問題。

2. 請同學於上課前複習相關資訊管理相關理論，以作為個案分析及擬定管理對策的依據。

3. 請同學於上課前
   先繳交個案研究問題書面報告。
References


– 周宣光 譯 (2011)，資訊管理系統－管理數位化公司，第12版，東華書局