BS 7799
Information Security Management

Reg Blake
VP Corporate Development
BSI America, Inc.
Reston, VA
Information - a most valuable asset in business

Information - increasingly vital:
  - For Competitive Success
  - To maintain a competitive advantage
  - In all sectors of the economy

Information - essential for economic survival

Information - takes many forms
  - written on paper
  - stored and/or transmitted electronically
  - mail
  - spoken
  - Audio-Visual
All *organisations* **depend** on information to survive

- Increasing **threats** - fraud, espionage, virus, hackers

- Increasing **exposure** - greater dependence on IT, less central control, new entry points for intruders

- Increasing **expectations** - managers, business partners, auditors and regulators demand protective measures
What is Information Security?

- Safeguarding the confidentiality, integrity and availability of written spoken and computer information
- To ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents
- Enabling mechanism for information sharing which ensures the protection of information and computing assets
- Confidentiality, Integrity, Availability and Accountability
Why is it important?

- Increasing dependence on computing and data networks
- Computer crime is on the increase (45%)
- $Billions is spent on information technology annually in the USA
- US Investments exceed this tremendously
- Introduction of paperless systems - e.g. on-line banking
• Internet - information retrieval, electronic commerce and commercial transactions, Intranet

• Requirement of Contracts and Tenders

• The need to comply with legislative requirements

• The need to formally control hacking, fraud, virus infection, sabotage etc.
• Employees
• Fraud, espionage, virus, hackers
• Growth of Networking - unauthorised access to computing systems
• Distributed computing - reduces central control within information systems
• Most information systems are not designed to be secure!
BS 7799

Standard for:
Information Security Management

1997 pilot certification scheme launched


1999 - BS 7799 Part One

1999 - BS 7799 Part Two

2000 - ISO 17799?
• 1999 - UKAS accredited scheme criteria published

• 1999 - BSI is awarded UKAS accreditation

• 1999 - First registrar to offer BS 7799 assessment and training services in the USA
Without a BS7799 based system, encryption and firewalls etc. will fail.....

Information Security is a Management Process, not a technological process
• Set of over **130 security controls**

• Organization selects controls that are applicable

• Organization must justify exclusion of non-applicable controls

• Organization must issue Information Security Policy and implement an Information Security Management System
The Requirements

- Information Security Policy Document
- Allocation of Information Security Responsibilities
- Provide all users with education and training in Information Security
- Develop a system for the reporting of Security Incidents
- Introduce virus controls
- Develop a business continuity plan
- Control the copying of proprietary software
- Safeguard Organizational Records
- Follow the requirements for data protection
- Establish procedures for complying with the security policy
The Ten Control Sections

- Security Policy
- Security Organisation
- Assets Classification and Control
- Personnel Security
- Physical and Environmental Control
The Ten Control Sections

- Computer Network and Management
- System Access Control
- Systems Development and Maintenance
- Business Continuity Planning
- Compliance
Those Most in Need

All organisations with a trading dependence on computing or data networks including:

- government departments, regulatory bodies and agencies
- internet service providers
- banks and electronic payment services
- retailers and suppliers trading electronically
- electronics and telecommunication
- State and local authorities
- internal IT departments
Cyberspace

- U.S.A. - largest user of the Internet
- Internet Activity - 70% occurs in the workplace
- Employee abuses
  - costly exposure
  - costly litigation
- Management
  - Must be proactive
  - Must address the problems
• Computer Crime Laws - federal government and across 50 states to manage computer misuse

• US Electronic Communications Privacy Act (fines $250K plus imprisonment)

• US Communications Decency Act 1996

• Fair Credit Reporting Act

• Freedom of Information Act
• Accreditation
  – UKAS
  – RAB?
• Registration & Certification
  – Registrars
The Assessment

- Two phased assessment process:
  - Phase 1 Desk Top Review - Risk Assessment, Statement of Applicability, IS Policies, Procedures and System
  - Phase 2 Implementation Audit - review of policies against working practice
Assessment Estimates & Dependencies

- ISO 9000
- Scope of system
- No. of users/sites
- Single/Multiple LAN/WAN
- Risk Level (e.g. Commercial, National)
- Remote Users
<table>
<thead>
<tr>
<th>Status</th>
<th>Size</th>
<th>Risk</th>
<th>Desk Top</th>
<th>Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 site with ISO</td>
<td>Single LAN</td>
<td>Commercial</td>
<td>1 day</td>
<td>2 days</td>
</tr>
<tr>
<td>Multi-site no ISO</td>
<td>Multiple LAN</td>
<td>National Security</td>
<td>4 days</td>
<td>6 days</td>
</tr>
</tbody>
</table>
Registered Companies

- Lifecare NHS Trust - Hospital
- Cabweb Ltd - Online Project Management
- Wright Publications - Electronic Publishing
- Midas Kapiti International - Banking software
- Volex Group - HQ of Manufacturing Co.
- LINK Interchange Network Limited - UK ATM Banking Network
- DBI Associates - Consulting
- American Society for Quality - QuEST Forum Administrator - Registration Repository System
- University of Texas at Dallas (UTD) - QuEST Forum Metrics Repository System
Contact:

Reg Blake
VP Corporate Development
Tel: 703-464-1908 (Voicemail)
Fax: 703-437-9001

E-Mail: reg.blake@bsiamericas.com