Building Effective, Tailored Information Security Policy

John Pescatore
Trusted Information Systems
301-947-7153         johnp@tis.com
Changing Business Model

**PAST**

- Traditional structure: (Sectors, wholly owned businesses, *stability*)

**FUTURE**

- Modern structure: (SBUs, JVs, IPOs, Divestitures, Acquisitions, Partnerships, Strategic Alliances...*constant change*)

**Need for flexibility will increase**
Electronic Business Relationships

- To be successful businesses need the ability to create rapid setup/teardown electronic business relationships with customers, suppliers, and partners. Security will need to be distributed throughout the computing enterprise.
Enterprise-wide Security

- One Time Passwords
- Strong Authentication
- Data Encryption

- Multilevel O/S
- Secure WWW
- Virus Protection
- Audit/Backup
- Data Encryption

Data

- Firewalls
- Host Security
- Messaging Security
- Integrity
- Availability

Firewalls

- Single Sign On
- Data Encryption
- Workplace Privacy

Producers

Secure RDBMS
- Object Oriented Security

Consumers

- Electronic Commerce
- Digital Signatures
- Windows NT
- Non-repudiation

Encryption
- Firewalls
- VAN Costs

Encryption
Infrastructure Impacts

- Changing business model leads to:
  - Growth by acquisition
  - Strategic alliances
  - Constant change

- Infrastructure needs to support:
  - Virtual Offices
  - Virtual Enterprises
  - Virtual Workgroups

- Security enables business to use the Internet to keep up with pace of change
  - Encryption
  - Authentication
  - Access Control
Growth by Acquisition

◆ Security Impacts:
  - Security Policy inconsistencies
  - Interoperability of Security Controls
  - Level of security sinks to lowest common denominator

◆ Policy Demands:
  - Frequent, often unplanned, updates needed
  - Must address multiple cultures
  - Drive to select best-of-breed approach
Strategic Alliances

Security Impacts:
- Team today, compete tomorrow
- Need for international secure connectivity
- Varying levels of trust

Policy Impacts:
- Focus on business-critical data
- Need to address export issues
- “One size fits all” no longer works
Constant Change

- **Security Impacts:**
  - Vulnerabilities follow transitions
  - Breakdown of informal policies
  - High administrative load for access control

- **Policy Impacts:**
  - Need for intrusion detection, updates, audits
  - Need to accessible formal policy
  - Policy needs to drive affordable solutions
Integrated Security Planning

- Treat security like an investment
  - Strategic planning
  - Business-driven
  - ROI or Cost/Benefit Analysis
- Legal and regulatory issues

<table>
<thead>
<tr>
<th>Strategize</th>
<th>Implement</th>
<th>Measure/Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business/ Mission Needs</td>
<td>Information Technology Needs</td>
<td>Security Services Required</td>
</tr>
<tr>
<td></td>
<td>Needs</td>
<td>Develop Security Architecture</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deploy Security Controls</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Perform Intrusion Detection</td>
</tr>
<tr>
<td>Policy Development and Refinement</td>
<td>Procurement/Development</td>
<td>Update Policies and Controls</td>
</tr>
<tr>
<td></td>
<td>Awareness/Education</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Compliance Enforcement</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Upgrade/Enhancement</td>
<td></td>
</tr>
</tbody>
</table>
Tailored Security Policy

- Goal is to influence behavior
- Need to enable, not just to deny
  - Users can route around controls all too easily
  - Become cost of sales, not just overhead
- Focus on the business needs
  - What data will be handled?
  - How can that data be accessed?
  - What is your organization’s paranoia level?
  - What controls are required on that data?
Data Categorization

- Define broad classes of information created, stored and/or delivered by your business
- Logical groupings based on impact to business
  - Customer data - financial records, medical records, orders
  - Business data - financial, competitive, intellectual property
  - Employee data - salary, benefits, home phone
# Data Categorization

- **Assign sensitivity levels, eg:**
  - **Unrestricted**
  - **Restricted**
  - **Controlled Distribution**

<table>
<thead>
<tr>
<th>Unrestricted</th>
<th>Restricted</th>
<th>Controlled Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meeting notes</td>
<td>Memos for the record</td>
<td>Salary data, personnel files</td>
</tr>
<tr>
<td>Internal telephone directory</td>
<td>Organizational directories with home addresses and/or phone numbers</td>
<td>Customer databases, privacy or medical-related information</td>
</tr>
<tr>
<td>Corporate publicity</td>
<td>Financial reports</td>
<td>Data on mergers or potential acquisitions</td>
</tr>
<tr>
<td>User IDs</td>
<td></td>
<td>Passwords, encryption keys</td>
</tr>
<tr>
<td>Most internal policies and procedures</td>
<td>Incident response plans</td>
<td>Results of risk assessments</td>
</tr>
<tr>
<td>Functional information about a major application</td>
<td>Source code for a major application</td>
<td>Information that is the major product of a major application: loan approvals, flight plan data, public safety information, calculations, etc.</td>
</tr>
</tbody>
</table>
Data Access

- How could an attacker get to your data?
  - How is it created?
  - Where is it stored?
  - How is it transmitted?

- Typical client/server/Internet scenario
  - Created on a Windows 95 PC
  - Stored locally, on a file server, on an internal Web server, in a database, external Web server
  - Sent over LANs, WANs, over Internet via http, ftp and email
Data Access

- Identify Data Owners and Data Maintainers
- Identify business needs to provide access to the data
  - Internal employees
  - External employees
  - Business partners
  - Customers
  - Other third parties
- Identify exposure points and threats
Paranoia Level

- Getting to “good enough security”
- Security policy needs to match the risk acceptance profile of an organization
  - What are the realistic threats?
  - How visible is your organization?
  - What are the consequences of an incident?
  - How sensitive is your organization to the intangible costs of an incident?
- Regulatory and legal issues
## Risk Profiling Matrix

<table>
<thead>
<tr>
<th>Threats:</th>
<th>Rating</th>
<th>Visibility</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>None identified as active; exposure is limited</td>
<td>1</td>
<td>Very low profile, no active publicity</td>
<td>1</td>
</tr>
<tr>
<td>Unknown state or multiple exposures</td>
<td>3</td>
<td>Middle of the pack, periodic publicity</td>
<td>3</td>
</tr>
<tr>
<td>Active threats, multiple exposures</td>
<td>5</td>
<td>Lightning rod, active publicity</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Consequences</th>
<th>Rating</th>
<th>Sensitivity</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>No cost impact; well within planned budget; risk transferred</td>
<td>1</td>
<td>Accepted as cost of doing business; no organization issues</td>
<td>1</td>
</tr>
<tr>
<td>Internal functions impacted; budget overrun; opportunity costs</td>
<td>3</td>
<td>Unacceptable Business Unit management impact; good will costs</td>
<td>3</td>
</tr>
<tr>
<td>External functions impacted; direct revenue hit</td>
<td>5</td>
<td>Unacceptable Corporate Management impact; business relationships affected</td>
<td>5</td>
</tr>
</tbody>
</table>

**Total Score:**

---

Copyright © 1997 Trusted Information Systems - 6/23/97
Security Controls

◆ Match the required controls to the organizational value of the data, the risk tolerance of the organization, and the investment required to meet the policy
  • Sounds easy, huh?

◆ Security policy can have wide ranging impact
  • Business-wide review
  • End result will be a compromise between security goals and business realities
## Security Controls

<table>
<thead>
<tr>
<th>Protection Required</th>
<th>Information Category</th>
<th>Restricted</th>
<th>Unrestricted</th>
<th>Controlled Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification</td>
<td>Identify as Organization Property</td>
<td>Identify as Organization Property, with category shown on initial page of record</td>
<td>Identify as Organization Property, with category shown on each page of record</td>
<td></td>
</tr>
<tr>
<td>Disclosure Restrictions</td>
<td>None inside the Organization</td>
<td>Based on need to know</td>
<td>Only when approved by the information owner</td>
<td></td>
</tr>
<tr>
<td>Access Controls</td>
<td>Access limited to within the organization</td>
<td>Access limited to those authorized by the information owner</td>
<td>Access limited to those authorized by the information owner. All access must be logged</td>
<td></td>
</tr>
<tr>
<td>Transmission over networks</td>
<td>No restriction</td>
<td>Internal networks only</td>
<td>Must be encrypted before transmission over any network</td>
<td></td>
</tr>
<tr>
<td>Storage</td>
<td>No restriction</td>
<td>Locked storage, physical secure computer area.</td>
<td>Locked storage, encrypted when stored on computer connected to network</td>
<td></td>
</tr>
</tbody>
</table>
Writing the Policy

- Match your organization’s culture
- Use the “real” information channels
- Several sources for templates
  - Outside consultants
- Involve Legal, HR, Public Affairs
- Policy should be issued from as high in the organization as possible
Awareness and Education

Standard approaches:
- Part of new hire training
- Yearly signed awareness statement
- System banners
- Internal newsletters

Direct Marketing approach
- Pay stub messages
- Online quizzes with awards
- Self assessment tools
Trusted Information Systems

• Since 1983, computer, network, and information security
• Customers in industry and federal, state, and local governments, worldwide
• Security products, security consulting, and world-respected research and development
• RecoverKey encryption technology
• TIS offices in Maryland, Virginia, California, UK, Germany
• TIS Business Partners in North America, South America, Europe, Asia, Africa, and Australia