Information Assurance/Information Security

John W. Lainhart IV

presentation for the

Computer System Security and Privacy Advisory Meeting

June 13, 2002
Agenda

- Information Assurance
- COBIT™ & the Management Guidelines
- IT Governance
- SysTrust℠ Assurance Service
- Managing Security of Information
- Board Briefing on IT Governance
- Information Security Governance
- Center for Internet Security Benchmarks
Information Assurance
Conducting those operations that protect and defend information and information systems by ensuring confidentiality, integrity, availability and accountability. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities.

NIAP Definition
Strategic Vision: Holistic Understanding

Security is a Function of Business


Implement Control Protective Measures to Mitigate Exploitable Risks and Minimize Operational Impacts Caused by Physical And IT Vulnerabilities… Threats Will Continue to Exist…

Traditional Security Must be Integrated And Active for OPSEC and Business Continuity to be Effective
IA Program Objectives: *Moving Beyond Information Security*
Integrity, Confidentiality, Availability, Accountability

<table>
<thead>
<tr>
<th>Proactive Measures</th>
<th>Event</th>
<th>Reactive Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Protect</strong></td>
<td><strong>Detect</strong></td>
<td><strong>React</strong></td>
</tr>
<tr>
<td>Policies</td>
<td>Procedures</td>
<td>CIRT (CERT)</td>
</tr>
<tr>
<td>Intrusion Detection</td>
<td>Firewall Management</td>
<td>COOP</td>
</tr>
<tr>
<td>Password Management</td>
<td>Configuration</td>
<td>Disaster Recovery</td>
</tr>
<tr>
<td>Biometrics</td>
<td>Management</td>
<td>Continuity of Government</td>
</tr>
<tr>
<td>Encryption</td>
<td>Threat Analysis</td>
<td>Incident Reporting Process</td>
</tr>
<tr>
<td>Vulnerability Assessment</td>
<td>Risk Analysis</td>
<td>Business Environment Monitoring</td>
</tr>
<tr>
<td>Training &amp; Education</td>
<td>Document Control</td>
<td>Managed Security Services</td>
</tr>
<tr>
<td>Classification</td>
<td>Smart Cards</td>
<td>Business Continuity</td>
</tr>
<tr>
<td>Management</td>
<td>C&amp;A (NIACAP, DITSCAP)</td>
<td>Computer Forensics</td>
</tr>
<tr>
<td>SW Patches</td>
<td>Anti-Virus</td>
<td>Business Continuity</td>
</tr>
<tr>
<td>Data Storage</td>
<td>Contingency Plans</td>
<td>Network Security Intelligence</td>
</tr>
<tr>
<td>Personnel Security</td>
<td>Physical Security</td>
<td></td>
</tr>
<tr>
<td>Counter Competitor Intelligence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Penetration Testing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Networks</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Social Engineering</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open Source Exploitation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Successful programs contain both proactive and reactive functions to be effective.
Concentric Barriers: Rings of Security

Protecting Critical Assets in the Virtual World Mirrors the Physical

Proactive Measures
- Protect
  - Deter e.g. Warning Banner
  - Detect e.g. Intrusion Detection
  - Delay e.g. Firewall
  - Defend e.g. Encryption
  - Deny e.g. Honey Pots
  - Defeat e.g. Arrest

Event
- Detect

Reactive Functions
- React
  - Monitoring
  - CIRT
  - Forensics
  - BCP/COOP

Defense in Depth

Escalation by Severity
PDD 63 responds to the **Interdependence** of Infrastructures and Technologies

- Telecommunications
- Power
- Gas/Oil
- Finance/Banking
- Transportation
- Water
- Government Services
- Emergency Services

**What We Can Do:**

- Threat Analysis
- Vulnerability Studies
- Protective Measures
- Impact Analysis

*What the Public Sees/Reads Determines their Confidence*

*What the Public Does Not See Involves Detailed Integration Of the Infrastructure: Plans/Compliance/Actions*
Information Assurance Program

Develop a cross functional (technical, physical, personnel and environmental) matrix team consisting of empowered management and staff who are tasked to develop and manage long-term strategic direction for the organization Information Assurance Program incorporating:

- Security Vision & Strategy
- Senior Management Commitment
- Training & Awareness Programs
- Information Assurance Management Structure
Information Assurance Program

Assessment and Diagnostic Service

- Risk Assessment (incorporating Asset Inventory, Mission Requirements Driven Policy, Threats, Vulnerabilities, associated Risk, Countermeasures, ROI, and strategic action implementation plan)
- Penetration Testing and Analysis
- Financial (budget) Assessment
- Diagnostics Security Reviews of specific platforms
- Asset Inventory Analysis
- Security Readiness Reviews
- Security Testing and Evaluation (documentation, testing and Evaluation)
- Government Information Security Reform Act (GISRA) Review
- Critical Infrastructure Protection Analysis
- Certification and Accreditation (System Security Authorization Agreement)
- Data/Information Integrity Assessment
- Site Surveys and Analysis
- Tools (i.e., EMM@, ESAS, Buddy System)
Information Assurance Program

Management Services

- Policy Development
- Technical Writing
- Standards
- Management Infrastructure
- Education Training and Awareness
- Business & Technical Disaster Recovery (documentation, training and testing)
- Management Training
- Continuity Of Operations (COOP) Development
- Capacity Management
- Configuration Management
- IAP Metrics
- Knowledge Management
- Distance Learning
- Strategic Management Consulting
- Economic Security
Information Assurance Program

Architecture Services

- Enterprise-Wide Architecture
- Network Security architecture and Specialized Architectures
- Security Product Review & Analysis
- Security Program Review & Analysis
- Life Cycle Methodology Development
- Configuration
- Security Architecture and Design
Information Assurance Program

Implementation Services
- Commercial security products (COTS)
- Encryption
- Single Sign On
- Firewalls
- Servers
- Routers
- Web/Internet Services
- VPNs
- Public Key Infrastructure (PKI)
- Secured Electronic Transaction (SET)
- Digital Certificates
- Certificate Authority Design
- Authentication
- Directory Services
- Smart Cards
- Biometrics
- Wireless
Information Assurance Program

Incident Investigation and Assurance Services

- Investigation and recovery from computer security incidents
- Data Forensics
- Incident Reporting and response services
- CERT/NOC capabilities
- Vulnerability Alerts
- Virus Alerts
- Unauthorized intrusion detection
Building on the strengths of your current Y2K Infrastructure, the next step is to move to a world class Information Assurance Program.
COBIT™

Information Technology Governance Institute

Control Objectives for Information and related Technology
COBIT: An IT control framework

- Starts from the premise that IT needs to deliver the information that the enterprise needs to achieve its objectives
- Promotes process focus and process ownership
- Divides IT into 34 processes belonging to four domains
- Looks at fiduciary, quality and security needs of enterprises and provides for seven information criteria that can be used to generically define what the business requires from IT

- Planning
- Acquiring & Implementing
- Delivery & Support
- Monitoring

- Effectiveness
- Efficiency
- Availability
- Integrity
- Confidentiality
- Reliability
- Compliance
COBIT: An IT control framework

- A high-level control objective for each process
  - identifying which information criteria are most important in that IT process
  - stating which resources will usually be leveraged
  - providing considerations on what is important for controlling that IT process
- 318 detailed control objectives for management and IT practitioners
- Extensive audit guidelines building on these objectives
COBIT Management Guidelines

Answers Key Management Questions
Through the use of:

- Maturity Models
- Critical Success Factors
- Key Goal Indicators
- Key Performance Indicators
<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 Non-Existent</td>
<td>Complete lack of any recognizable processes. The organization has not even recognized that there is an issue to be addressed.</td>
</tr>
<tr>
<td>1 Initial</td>
<td>There is evidence that the organization has recognized that the issues exist and need to be addressed. There are however no standardized processes but instead there are ad hoc approaches that tend to be applied on an individual or case by case basis. The overall approach to management is disorganised.</td>
</tr>
<tr>
<td>2 Repeatable</td>
<td>Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and therefore errors are likely.</td>
</tr>
<tr>
<td>3 Defined</td>
<td>Procedures have been standardized and documented, and communicated through training. It is however left to the individual to follow these processes, and it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalization of existing practices.</td>
</tr>
<tr>
<td>4 Managed</td>
<td>It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.</td>
</tr>
<tr>
<td>5 Optimized</td>
<td>Processes have been refined to a level of best practice, based on the results of continuous improvement and maturity modeling with other organizations. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.</td>
</tr>
</tbody>
</table>
COBIT Management Guidelines

Maturity Models for Self-Assessment

Non-Existent  Initial  Repeatable  Defined  Managed  Optimised

0  1  2  3  4  5

LEGEND FOR SYMBOLS USED

Enterprise Current Status
International Standard Guidelines
Industry Best Practice
Enterprise Strategy

LEGEND FOR RANKINGS USED

0 Non-Existent  – Management processes are not applied at all
1 Initial  – Processes are ad hoc and disorganised
2 Repeatable  – Processes follow a regular pattern
3 Defined  – Processes are documented and communicated
4 Managed  – Processes are monitored and measured
5 Optimised  – Best practices are followed and automated
IT Governance

Objectives

- IT is aligned with the business, enables the business and maximises benefits
- IT resources are used responsibly
- IT related risks are managed appropriately

IT Activities

<table>
<thead>
<tr>
<th>Manage risks</th>
<th>Realise Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>security</td>
<td>Increase</td>
</tr>
<tr>
<td>reliability</td>
<td>Automation - be effective</td>
</tr>
<tr>
<td>compliance</td>
<td>Decrease Costs - be efficient</td>
</tr>
</tbody>
</table>

PO
AI
DS
MO
SysTrust\textsuperscript{SM}

American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants

Systems Reliability Assurance Service
Opinion on controls

- Based on a framework of principles & criteria
- Identify and assess the operating effectiveness of controls that support the criteria

A system must meet all principles & all criteria to be considered “Reliable”

- Reporting on less than 4 principles is permitted
- All criteria related to the principle must be met
SysTrust

SysTrust as an Assurance Service

SysTrust used to manage internal risk
- New applications being developed and/or implemented
- Applications already in use

SysTrust use to manage 3rd party risk

Partner systems
- 3rd party service-bureau systems
- Online marketplaces/exchanges
SysTrust as Consulting Engagement

SysTrust is a benchmark on controls

Opportunity to identify control weaknesses

Current engagements started as consulting

Greater market for Consulting or Assurance?
System reliability is defined as:

“A system that operates without material error, fault or failure during a specified time in a specified environment.”

Four Principles:

- Availability
- Security
- Integrity
- Maintainability
Managing Security of Information

International Federation of Accountants
International Information Technology Guideline
Managing Security of Information

Core Principles

**Accountability** - Responsibility and accountability must be explicit

**Awareness** - Awareness of risks and security initiatives must be disseminated

**Multidisciplinary** - Security must be addressed taking into consideration both technological and non-technological issues

**Cost Effectiveness** - Security must be cost-effective
Managing Security of Information

Core Principles

Integration - Security must be coordinated and integrated

Reassessment - Security must be reassessed periodically

Timeliness - Security procedures must provide for monitoring and timely response

Societal Factors - Ethics must be promoted by respecting the rights and interests of others
Managing Security of Information

Implementation Approach

Policy Development
Roles and Responsibilities
Design
Implementation
Monitoring
Awareness, Training, and Education

INFORMATION SECURITY POLICY STATEMENT EXAMPLE
Board Briefing on Information Technology Governance

Information Security Governance

Co-Badged by a Number of Leading Organizations
“IT governance is the term used to describe how those persons entrusted with governance of an entity will consider IT in their supervision, monitoring, control and direction of the entity. How IT is applied within the entity will have an immense impact on whether the entity will attain its vision, mission or strategic goals.”

ITGI document: Board Briefing on Information Technology Governance
“Executive management has a responsibility to ensure that the organization provides all users with a secure information systems environment. Furthermore, organizations need to protect themselves against the risks inherent in the use of information systems while simultaneously recognising the benefits that can accrue from having secure information systems.”

ITGI document: Information Security Governance
Center for Internet Security
Center for Internet Security

is developing:

• best-practice benchmarks that define the specific technical settings that will provide increased security for Internet-connected systems

• a security ruler that defines which of those specific settings will increase the relative security of your systems

• automated tools to continuously monitor the security status of your systems
Web Sites

• COBIT™ -- www.itgi.org
• SysTrust™ -- www.aicpa.org
• Managing Security of Information -- www.ifac.org
• Board Briefing on Information Technology Governance -- www.itgi.org
• Information Security Governance – www.itgi.org
• Center for Internet Security – www.cisecurity.org
QUESTIONS?
Contact Information:

John W. Lainhart IV
703/741-1647
john.w.lainhart@us.pwccglobal.com