Information Availability -
Industry Trends, Emerging Concerns & Executive Metrics
Changing World of IT Risk Management

Overview: Types of IT Security Disasters (& stories)

Information Availability – What is it? How do you measure it?

Compliance & Information Availability
How many squares do you see?
Answer?

A. 16
B. 34
C. 30
D. 29
Answer?

A. 16
B. 34
C. 30*
D. 29
How many squares do you see?

4x4 = 1
3x3 = 4
2x2 = 9
1x1 = 16
Changing Nature of Information Availability

In The Beginning Was Y2K…..Then Came:

September 11th –
Enron Accounting Scandal
– Investor Confidence

August 03 Blackout –
Aging Infrastructure
Risk Management

Natural Disasters → External
- Hurricanes

Internal
- Fires

Non-Physical
- Viral Outbreaks

Man-Made Disasters → Terrorist Detonations

Disgruntled Employees

Hackers
Risk Management

Risk Identification Process

Risk Mitigation Stage

Active Controls

Administrative Controls
Process Controls
Technical Controls
Financial Controls

Passive Controls

Plan on Doing Nothing
Contingency Plans
Measure acceptable risk?

Internet Security Alliance July 2002/Data from Dr. William M. Hancock, Exodus, A Cable and Wireless Service
A Word on IT Security Disasters & Internet Disruptions
### Network Disruption

*prey upon an organization’s lack of security or detection capability. Examples are DOS attacks or p/w guessing.*

**Considerations:** Operational disruption testing  
**Vignette:** Attack on world’s root DNS infrastructure
Network-Based IT Security Disaster Considerations: VOIP?
Standard Firewall Security Rule Set

Secure DMZ-to-Internal Network Nomenclature

- Block any incoming packet of any type that has an internal IP address as its source address. (protects against spoofing)
- Allow in any TCP packet that’s part of an established connection. (maintains corporate internet use policy)
- Allow in any TCP packet that’s explicitly addressed to 012.34.56.79 on port 80. (protects against spoofing)
- Block any other incoming TCP packets and log them to the router’s display. (protects opportunistic reconnaissance / entry)

How does this look for VOIP / Extranet Service Providers w/o VPN?
The difference between DOS and DDOS

A DOS (denial of service) attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include attempts to:

- "Flood" a network to slow or halt network traffic
- Disrupt connections between two machines to prevent access to a service
- Prevent a particular individual from accessing a service
- Disrupt service to a specific system or person

A DDOS (distributed denial of service) is merely a larger-scale, coordinated effort that shows no single point of origin and seeks to inflict greater damage by attacking more and related targets simultaneously.
Key Questions for VOIP Availability?

- Have you conducted a single-point-of-failure analysis prior to adopting VoIP?
- Because some VoIP services do not work during power outages, do you have a continuity plan in place to provide back-up power in the event of an outage?
- Do you have a way to connect with emergency services?
- Have you considered the dangers of leveraging a single technology—the Internet—and thereby creating problems with a single point of failure?
- Have you installed adequate controls to mitigate the availability risks associated with VoIP?
- Are you protecting yourself against eavesdropping, spoofed IP addresses, and inauthentic data packets flooding your server?
- Have you considered the dangers of replay attacks?
- Are you monitoring traffic and restricting it to a select group of IP addresses?
- Do you require VoIP devices to authenticate each other before communication starts?
- Do you use TLS to provide a secure communication channel?
- Do you encrypt communications using SRTP?
- What is your level of redundancy for web connectivity?
Types of IT Security Disaster Planning

**Network Disruption:** prey upon an organization’s lack of security or detection capability. Examples are DOS attacks or p/w guessing.

Considerations: Operational disruption testing

Vignette: Large retail store

---

**Malicious Code** characterized by the insertion of malicious code into an organization’s infrastructure. Examples are worms and viruses.

Considerations: Alternate Site Anti-Virus, Filtering

Vignette: Large national bank in leveraging HA
Malicious-Code IT Security Disaster Considerations: XML?

XML document wrapped in IP package enters corporate network via the Internet.

Network inspects the package, but not the document.

Document is not identified as potential security threat and enters enterprise.

Your enterprise security is potentially compromised by an XML document which could contain malicious code.
Key Questions for XML Availability?

- Is XML affecting your network performance or application server performance?
- Do you have a plan in place to address a denial-of-service attack which could take down your network by flooding your server with XML messages?
- Do you have security measures in place to scan XML files for malicious code?
- Is your company depending on XML—creating a single point of failure?
- Is your proprietary corporate data being compromised by XML?
- Are you validating Web Services Description Language?
- Are you doing all you can to validate data between the sender and receiver?
- Do you know which applications currently installed or planned use XML?
- Have you considered cryptography or patch management solutions?
- Are you familiar with XML acceleration appliances?
- Are you familiar with binary XML and its potential benefits/risks?
- Can SML-migration be a consideration for your XML-based communications?
**Types of IT Security Disaster Planning**

**Network Disruption:** prey upon an organization’s lack of security or detection capability. Examples are DOS attacks or p/w guessing.
- Considerations: Operational disruption testing
- Vignette: Large retail store

---

**Malicious Code** characterized by the insertion of malicious code into an organization’s infrastructure. Examples are worms and viruses.
- Considerations: Alternate Site Anti-Virus, Filtering
- Vignette: Large national bank in leveraging HA

---

**Vulnerability Management:** exploit specific technical weaknesses inherent in the infrastructure itself. Worms, patch mgmt, etc
- Considerations: Patch Management (including Alt. Site)
- Vignette: Cisco Source Code, SNMP
Types of IT Security Disaster Planning

**Network Disruption**: prey upon an organization’s lack of security or detection capability. Examples are DOS attacks or p/w guessing.
- Considerations: Operational disruption testing
- Vignette: Large retail store

**Malicious Code**: characterized by the insertion of malicious code into an organization’s infrastructure. Examples are worms and viruses.
- Considerations: Alternate Site Anti-Virus, Filtering
- Vignette: Large national bank in leveraging HA

**Vulnerability Management**: exploit specific technical weaknesses inherent in the infrastructure itself. Worms, patch mgmt, etc.
- Considerations: Patch Management (including Alt. Site)
- Vignette: Small e-business wholesaler

**Criminal / Compliance**: finite, deliberate attacks that use a combination of exploits (i.e. administrative, process, financial) to achieve a highly desired goal. Also consider government enforcement actions.
- Considerations: Internal Penetration Testing / Forensics Provider
- Vignette: Small NY non-profit company
Regardless of the source of interruption, plans must address Internet disruptions with varying levels of tangible effect and geographical reach. It is important to note that the severity of end-user impact is correlated to specific interruption levels.
## Trends

<table>
<thead>
<tr>
<th>Traditional Disaster Recovery Site Considerations</th>
<th>Additional Security Considerations for Recovery Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Network Connectivity</td>
<td>- Anti-Virus Protection</td>
</tr>
<tr>
<td>- Hardware</td>
<td>- Firewalls and Access Control Rules</td>
</tr>
<tr>
<td>- Operating Systems</td>
<td>- Router Control List</td>
</tr>
<tr>
<td>- Mission-critical Applications</td>
<td>- IDS</td>
</tr>
<tr>
<td></td>
<td>- VPN and Authentication Tokens</td>
</tr>
<tr>
<td></td>
<td>- Content Filtering</td>
</tr>
<tr>
<td></td>
<td>- Forensics and Diagnostic Tools</td>
</tr>
<tr>
<td></td>
<td>- Operating System and Application Security Patches</td>
</tr>
</tbody>
</table>
Information Availability
Fierce competition drives lean programs
- Need to become more effective more efficiently
- Security, BC/DR, & IT programs are often disconnected & overlapping = Inefficient

Gartner Group 2004: Industry trends

- Need for information / guidance supporting IT governance, asking questions such as:
  - What should be defined in repeatable process?
  - What is an appropriate level of detail?
  - What should be measured? What should be automated?
  - What is Best Practice? Is there a certification available?

- Organizations more aware of service continuity & related risks

- Virtues of dependability, reliability & resilience as an integral part of an organization’s business culture and value proposition
  - Address continuity issues as standard operating policy, instead of addressing them as an added-cost item
  - Accepting the costs of fully tested continuity plans and rock-solid SLAs as the price of remaining viable within your industry
IAA: A holistic assessment of how an enterprise handles their Information Availability Program
## IAA Approach

- **3 Domains:** Info Security; Info Management; Info Architecture
- **5 Competencies within each domain**
- **150 Attributes**

### Domains

<table>
<thead>
<tr>
<th>Domains</th>
<th>Information Security (A)</th>
<th>Information Management (B)</th>
<th>Information Architecture (C)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security (A)</td>
<td>Policies, Procedures, and Regulatory Compliance</td>
<td>Management Controls</td>
<td>Facility and Environmental Infrastructure</td>
</tr>
<tr>
<td>Information Management (B)</td>
<td>Architecture &amp; Project Management</td>
<td>Information Management</td>
<td>Network Design</td>
</tr>
<tr>
<td>Information Architecture (C)</td>
<td>Access Control / Organizational Skills</td>
<td>Continuity of Services</td>
<td>Systems Design</td>
</tr>
<tr>
<td></td>
<td>Awareness, Education, and Training</td>
<td>Maintainability</td>
<td>Component Architecture (Data/Voice)</td>
</tr>
<tr>
<td></td>
<td>Exposure Analysis and Reporting Metrics</td>
<td>Performance Measurements</td>
<td>Information Accessibility Documentation</td>
</tr>
</tbody>
</table>
Example Results

<table>
<thead>
<tr>
<th>Category</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall IAA Score</td>
<td>52.4%</td>
</tr>
<tr>
<td>Info. Architecture</td>
<td>79.7%</td>
</tr>
<tr>
<td>Info. Management</td>
<td>50.6%</td>
</tr>
<tr>
<td>Info. Security</td>
<td>27%</td>
</tr>
</tbody>
</table>

Very Good: 70%+
Good: 60% – 69%
Average: 50% - 59%
Fair: 45% - 49%
Poor: Below 45%
Information Security

Info Security Rating: 27%
- Policies, Procedures: 27%
- Architecture & PM: 40%
- Access Control: 12%
- Awareness/Education: 19%
- Exposure Analysis: 37%

Sample Strengths:
- A high-level Information Security Policy, along with some supporting Security-related policies and standards, exist at ABC Corporation.
- Firewalls, Intrusion Detection, Virus Detection, and internal Vulnerability Assessments software and/or services are in place. Additionally, anti-virus is deployed and used at the server, SMTP, and desktop levels. WAN and LAN design has included resiliency considerations.
- ABC Corporation contracts with external third parties for routine audits of the security environment.
# Roadmap: High Priority Actions

<table>
<thead>
<tr>
<th>Domain</th>
<th>Attribute</th>
<th>Recommendation Summary</th>
<th>Impact</th>
<th>Effort</th>
<th>Cost</th>
<th>Action Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS</td>
<td>A.1.1</td>
<td>Audit and Improve Information Security Policies</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>1</td>
</tr>
<tr>
<td>IS</td>
<td>A.1.1</td>
<td>Framework for Policy Administration, Review, and Enforcement</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>1</td>
</tr>
<tr>
<td>IS</td>
<td>A.2.1</td>
<td>Conduct an Enterprise Risk Assessment</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>1</td>
</tr>
<tr>
<td>IS</td>
<td>A.2.2</td>
<td>Improve and Implement Information Security Management Model</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>1</td>
</tr>
<tr>
<td>IS</td>
<td>A.3.4</td>
<td>Formalize Process for Status Changes and Terminations</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>1</td>
</tr>
<tr>
<td>IS</td>
<td>A.3.5</td>
<td>Improve Password Practices</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>1</td>
</tr>
<tr>
<td>IS</td>
<td>A.3.6</td>
<td>Improve Workstation Security Practices</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>1</td>
</tr>
<tr>
<td>IS</td>
<td>A.4.8</td>
<td>Encourage IT Security Professional Development</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>1</td>
</tr>
<tr>
<td>IM</td>
<td>B.1.3</td>
<td>Establish a formal Information Availability Awareness Training Program</td>
<td>High</td>
<td>Med</td>
<td>Low</td>
<td>1</td>
</tr>
<tr>
<td>IM</td>
<td>B.1.4</td>
<td>Where applicable, establish formal SLAs with supporting vendors</td>
<td>Med</td>
<td>Low</td>
<td>Low</td>
<td>1</td>
</tr>
<tr>
<td>IM</td>
<td>B.1.5</td>
<td>Establish formal procedures for responding to changes to existing policies, procedure and guidance and their subsequent distribution</td>
<td>Med</td>
<td>Low</td>
<td>Low</td>
<td>1</td>
</tr>
<tr>
<td>IM</td>
<td>B.2.4</td>
<td>Formally document Service Level Objectives (SLOs) with System Administrators and end users.</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>1</td>
</tr>
<tr>
<td>IM</td>
<td>B.3.6</td>
<td>Establish a formal communications plan for internal and external audiences during recovery operations.</td>
<td>High</td>
<td>Low</td>
<td>Low</td>
<td>1</td>
</tr>
</tbody>
</table>
Compliance & Information Availability

SUNGARD® Availability Services
Keeping People and Information Connected™
Manage technology
Automate business processes
Enable new products and services
Participate in executive management role
Corporate Scandal: Continuing Pressure

- 5 Wall Street firms - $8+ Million fine
- Banc of America Securities - $10 Million penalty for Document Production Failures
- $37 Million fine Symbol Technologies accounting fraud (+ 11 executives)
- $25 Million penalty Lucent Technologies for accounting fraud
- $240 Million settlement for 5 specialist firms
New Categories of Risk

Interconnected Economy

Governance & Management

CIO

Privacy & Info Security

Liability for IT Failures
Emergence of Convergence

Regulatory

FFIEC & OCC Banking
Securities Act of 1934
Sarbanes Public Companies
Securities SEC 17a4

Reliability

Business Continuity
& Information Security
& Information Content Mgmt.

Privacy

GLB Financial
HIPAA

Accountability

SUNGARD® Keeping People and Information Connected™
Financial Services: Required Practices

✓ Identify critical back office activities and systems that support them. (business process, not just technology.)
✓ Drive planning and testing activities to meet appropriate RTOs
✓ Maintain sufficient geographically dispersed resources to meet recovery objectives (staff, equipment and data.)
✓ Routinely test recovery and resumption arrangements with emphasis on connectivity with major counter-parties and arrangements with third party providers.
## The Securities Market Value Chain

<table>
<thead>
<tr>
<th>Regulatory Agency</th>
<th>RTO Expectation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interagency White Paper</td>
<td>intraday: 2 – 4 hours</td>
</tr>
<tr>
<td>Clearing &amp; Settling</td>
<td></td>
</tr>
<tr>
<td>SEC Policy Statement</td>
<td>next business day</td>
</tr>
<tr>
<td>Trading Markets</td>
<td></td>
</tr>
<tr>
<td>SEC &amp; NASD/NYSE Policy</td>
<td>variable RTO’s permitted, but customer-notified SLAs</td>
</tr>
<tr>
<td>Securities Firms</td>
<td></td>
</tr>
</tbody>
</table>
Member firms must have documented business continuity plans. Annual review is required and senior officer is responsible.

Why? To bring self-regulated organizations into line with regulated financial sector. Goal is to enable members to meet existing obligations to customers, other broker dealers and counterparties.

NASD: 5600 members, 95000 branches
Effective Dates:

NASD Rule 3520 – Emergency Contacts
- All Firms June 14, 2004

NASD Rule 3510 – Business Continuity Plans
- Clearing Firms August 11, 2004
- Introducing Firms September 10, 2004

NYSE Rule 446 – Business Continuity Plans
- August 5, 2004
What are the Requirements?

Rule 3520
- 2 emergency contacts
  - Senior management & registered principal
  - Reviewed quarterly or when material change

Rule 3510
- Documented business continuity plan
- Senior management approval
- Outside repository
- Copy filed with NASD***
- Customer disclosure
10 Critical Elements for BCP:

1. Data back-up and recovery (hard copy & electronic)
2. All mission critical systems
3. Financial and operational assessments
4. Alternate communications between customers and the member
5. Alternate communications between the member and its employees
6. Alternate physical location of employees
7. Critical business constituents, banks, and counter-party impact
8. Regulatory reporting
9. Communications with regulators
10. How the member will assure customers’ prompt access to their funds and securities in the event that the member determines it is unable to continue its business

People, Processes and Technology
Newly Added Language:
Every NASD and NYSE member also will be required to disclose to its customers a summary of its business continuity plan that addresses how the member intends to respond to potential disruptions of varying scope.
Customer Disclosure:

- When?
  - At time of account opening
  - Available on request by mail
  - Posted on web site (if applicable)

Not yet widely known by business side or IT
Clear opportunity to open conversation with clients
Customer Disclosure:

Recovery Time Objectives (RTOs) for multiple scenarios

- Firm only
- Building only
- District only
- City only
- Regional

Planned Response

- Stated intention to continue business
- Back-up facilities and arrangements such as:
  - Voice response system
  - Online trading
  - Alternate call center/telephone contact
  - Access to accounts
- Significant 3rd Party relationships such as:
  - Clearing and settling
  - Outsourced front end/back office processing
Opportunity for Incident Management

- Crisis Control Team
  - Who has the authority to execute?
  - Emergency contact information
  - Alternate Command Center
  - Alternate means of communication

- Action Plan
  - Media control plan
  - Provisions for:
    - Legal
    - Human Resources
    - Finance
Why Sarbanes-Oxley?

Enron – 7\textsuperscript{th} largest company in US

- “record growth” through June 2001
- 1\textsuperscript{st} restatement October 2001
- Bankrupt by December 2001

Worldcom - $11Billion in restated “earnings”
Sarbanes-Oxley Purpose

• Ensure the integrity and transparency of US capital markets
• Restore checks and balances for corporate governance and ethical corporate behavior
• Restore reputation for rectitude of the SEC

Senator Paul Sarbanes, May 2004
Sarbanes – Applicable Sections

Section 302 - Certification
CEO and CFO must certify their financial statements
Deadline: in effect now

Section 404 – Internal Controls
Auditors must certify internal controls and processes in addition to financial numbers
Deadline: extended to Nov 15, 2004

Section 409- Disclosure
Companies must provide real time disclosure of material events that might effect performance, real time reporting (including changes/events relating to internal controls)
Deadline: August 2004 (NEW accelerated date)
## Which Regulations Apply?

<table>
<thead>
<tr>
<th>Industry: Buy Side Sell Side</th>
<th>Gramm-Leach-Bliley</th>
<th>Federal White Paper</th>
<th>SEC Trading Markets</th>
<th>NASD 3510 NYSE 446</th>
<th>SEC 17a4</th>
<th>Sarbanes Oxley</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clearing Bank (BONY e.g.)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>brokerage?</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Large Brokerage (Prudential/Wachvia Sec e.g.)</td>
<td>✓</td>
<td>If &gt; 5% share</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Market Data Feed (Reuters e.g.)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>?</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>3rd Party IT Business Services EDS e.g.</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Sample Analysis:

Bank of New York:

- IWP – 2 Hr RTO, business recovery (workgroup), network and connectivity to value chain
- GLB – info security & business continuity
- NASD 3510 – business continuity, customer SLAs
- SEC17a4 – electronic archiving incl. e-mail and IM relating to customer accounts if brokerage
- Sarbanes – info security, electronic archiving for workpapers/messages relating to financial statements
- FFIEC/OCC (retail) – business continuity, improved test results, info security, 3rd party supervision
### Industry: Healthcare

<table>
<thead>
<tr>
<th></th>
<th>Gramm-Leach-Bliley</th>
<th>HIPAA</th>
<th>Sarbanes Oxley</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insurance (Aetna e.g.)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Hospitals (Tenet Healthcare e.g.)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Large Group Practice</td>
<td>✓</td>
<td>✓</td>
<td>Not unless publicly held</td>
</tr>
</tbody>
</table>
Other industries

- Utility – FERC, NERC, Sarbanes if public
  - Physical and info security, business continuity, incident response
  - Annual certification
  - Electronic records retention
- Pharmaceutical – FDA Title 21, Sarbanes, HIPAA
  - Info security, business continuity, records retention
Changing World of IT Risk Management

Overview: Types of IT Security Disasters (& stories)

Information Availability – What is it? How do you measure it?

Compliance & Information Availability
Carl Herberger
SunGard Availability Services
Sr. Director, Information Security Professional Services
Wayne, PA
484-582-5739
Carl.Herberger@sungard.com
White Papers

SunGard has extensive experience in a variety of industries and technologies. We invite you to improve the effectiveness of your information Availability planning with complimentary access to white papers, executive briefs, etc.

We highlight industry trends and are always looking for new ideas. Contact Us to share your comments and suggestions.

- Stop Spoofing, Foil Phishing, Squelch Spamming: Protecting Email and Securing Production Availability
- Security, Continuity and Recovery for Internet Disruptions and Disasters
- Integrating Network Design With Continuity and Production Concerns to Ensure Information Availability
- IDC White Paper: Outsourcing Business Continuity Needs: Ensuring Information Availability While Ensuring ROI
- How Software Can Help You Protect the Availability of Your Business
- Integrating Business Continuity and Information Security