Industry Perspective: What are the Risks to be Faced by Organisations?

Jong Ki Yoo
Consultant, CISA, CISSP, CFJP
IBM Business Resilience & Continuity Services

06 September 2005

Agenda

- Security is the top priority (by IBM Market Intelligence, Banking Report, Sep 2004)
- Pain Points
  - Security Triggers
  - Understanding the Pain
  - Key Security Trends
  - Countermeasures
- IBM Security & Privacy Research

> Unauthorized use of computer systems is on the decline, as is the reported dollar amount of annual financial losses resulting from security breaches.

> In a shift from previous years, both virus attacks and denial of service outpaced the former top cost, theft of proprietary information. Virus costs jumped to $55 million.

> The percentage of organizations reporting computer intrusions to law enforcement over the last year is on the decline. The key reason cited for not reporting intrusions to law enforcement is the concern for negative publicity.

> Most organizations conduct some form of economic evaluation of their security expenditures, with 55 percent using Return on Investment (ROI), 28 percent using Internal Rate of Return (IRR), and 25 percent using Net Present Value (NPV).

> Over 80 percent of the organizations conduct security audits.

> The majority of organizations do not outsource computer security activities. Among those organizations that do outsource some computer security activities, the percentage of security activities outsourced is quite low.

> The Sarbanes-Oxley Act is beginning to have an impact on information security in some industries.

> The vast majority of the organizations view security awareness training as important, although (on average) respondents from all sectors do not believe their organization invests enough in this area.
Information Security Maturity: 1996

<table>
<thead>
<tr>
<th>Blissful Ignorance</th>
<th>Awareness Phase</th>
<th>Corrective Phase</th>
<th>Operations Excellence Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review Status Quo</td>
<td>18% Develop New Policy Set</td>
<td>Conclude Catch-Up Projects</td>
<td>0% Track Technology and Business Change</td>
</tr>
<tr>
<td>80%</td>
<td></td>
<td>Design Architecture</td>
<td>Continuous Process Improvement</td>
</tr>
<tr>
<td></td>
<td>(Re) Establish Security Team</td>
<td>Institute Processes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Initiate Strategic Program</td>
<td></td>
</tr>
</tbody>
</table>

Quoted from [Meta Group] Security Programs, Trends and Markets - Security & Risk Strategies March 10, 2005

Information Security Maturity: 2000

<table>
<thead>
<tr>
<th>Blissful Ignorance</th>
<th>Awareness Phase</th>
<th>Corrective Phase</th>
<th>Operations Excellence Phase</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review Status Quo</td>
<td>28% Develop New Policy Set</td>
<td>Conclude Catch-Up Projects</td>
<td>2% Track Technology and Business Change</td>
</tr>
<tr>
<td>60%</td>
<td></td>
<td>Design Architecture</td>
<td>Continuous Process Improvement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Institute Processes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Initiate Strategic Program</td>
<td></td>
</tr>
</tbody>
</table>

Quoted from [Meta Group] Security Programs, Trends and Markets - Security & Risk Strategies March 10, 2005
Information Security Maturity: 2004

Quoted from [Meta Group] Security Programs, Trends and Markets - Security & Risk Strategies March 10, 2005

Information Security Maturity: 2008 (expected)

Quoted from [Meta Group] Security Programs, Trends and Markets - Security & Risk Strategies March 10, 2005
Security is the top priority

Solution Priorities and Spending for 2005: Banking

<table>
<thead>
<tr>
<th>Industry-Specific Solution</th>
<th>Total '05 Spending¹ (% of IT Spending)</th>
<th>% Top Priority Solution²</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Solutions</td>
<td>Total '05 Spending¹ (% of IT Spending)</td>
<td>% Top Priority Solution²</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure Solutions</td>
<td>Total '05 Spending¹ (% of IT Spending)</td>
<td>% Top Priority Solution²</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Quoted from IBM Market Intelligence, Solutions Market Monitor, Sep 2004
Countries: US, UK, France, Germany, and Japan / Industries: Automotive, Electronics, Financial Markets, Banking, Consumer Products, Wholesale Distribution & Services, and Retail

Pain Points – Security Triggers

Where do threats to your organization originate from?

- Foreign Intruders
- Cybercrime
- Natural Disasters
- Deliberate Attack
- Accidents
- Organised Crime
- Human Error
- Competition
- Fraud
- Internal Threats
- Niche

Increased collaboration and new business models brings greater business rewards, but also poses greater business risks
Pain Points – Security Breaches (Media Titles)

- The New York Times
- BusinessWeek
- Forbes
- The Economist

Pain Points – Understanding the pain

- Protecting privacy and security of customer and employee information
- Securing exchange of business critical information
- Managing identity within and across enterprise(s)
- Ensuring integrity of the environment
- Managing security policies to mitigate risks
Pain Points – Understanding the pain

- Protecting privacy of customer and employee information
  - Protect data and strategic assets
  - Consistently enforce security and privacy policies
  - Deploy solutions with appropriate security controls incl isolation
  - Simplify and strengthen user authentication and authorization

- Securing exchange of business critical information
  - Build and protect trust with customers and partners
  - Secure message exchanges that ensure integrity and confidentiality

- Managing identity across enterprise(s)
  - Managing user identity within and across enterprises
  - Managing security credentials and mapping

- Ensure integrity of the environment
  - Ensure security controls remain appropriate over time
  - Ensure end to end secure and trustworthy environment
  - Enable accountability through audit
  - Verify and adhere to security and compliance policies

- Manage security policies to mitigate risks
  - Mitigate and manage the security risk
  - Reduce cost of managing and administering security policies
  - Detect and manage intrusions

Pain Points – Key Security Trends

- Convergence of Physical and logical security
- Adoption of federated Identity management
- Drive toward greater interoperability
- Evolution of real-time threat management systems
- Movement from disaster recovery to business continuity and resiliency
- Enterprise wide security programs focusing on risk management and governance
Pain Points – Countermeasures

- Respond to changing business needs with agility
  - Support growth, change and consolidation initiatives
  - Accommodate applications as they change and facilities as they move
  - Integrate with business partners, customers and acquired companies—and rapidly determine which parties have access to which resources

- Protect your reputation and enhance trust in your brand
  - Safeguard data privacy and integrity to minimize intellectual property loss and damage to business relationships
  - Maximize secure transactions and continuity of business operations to earn the confidence of your customers and partners

- Optimize operational efficiency
  - Simplify and coordinate identity management to help end users collaborate and be highly productive
  - Leverage centralized views of security status, tools that facilitate administrative best practices and self-protecting, autonomic capabilities to enable skilled IT staff to focus on high-value tasks

- Gain a company-wide view of risks to contain costs
  - Identify the exposures to loss and liability that have the greatest potential business impact—dollar loss, downtime, contract penalties, compliance with regulations or other business policies—and address them first
  - Sense when internal and external changes impact enterprise-wide risks and respond accordingly
  - Protect your systems and networks from threats, not only by sensing threats before they happen, but also through integrated, closed-loop responses across your IT infrastructure

- Identify and maintain security compliance
  - Facilitate comprehensive, simplified management of risk, regulatory compliance and business controls
  - Provide a centralized policy auditing mechanism while helping to minimize staff and compliance costs

Ten Items to Consider for Minimizing Security Risks

- Conduct a Risk Assessment of Your Business
- Develop Security Standards
- Test Your Defenses
- Develop Procedures for Prevention and use Independent Third-Parties to Test Them
- Limit the Number of Individuals Who May Access Controls to Your Business
- Utilize Firewalls
- Utilize Surveillance Tools
- Monitor Your Networks for Unusual Activity
- Contact Your Internet Service Provider
- Report Computer Violations to the Proper Law Enforcement Authorities

[How much security is enough? – Wooden Tub Model]

[Information Security – Three Properties]
Security & Privacy Research at IBM – Global Research Centers

IBM Research Division has a worldwide presence through its eight locations with a total population of more than 3000 Researchers

- **Almaden**, Established: 1986, Employees: 500
- **Austin**, Established: 1995, Employees: 40
- **Beijing**, Established: 1995, Employees: 90
- **Delhi**, Established: 1998, Employees: 60
- **Haifa**, Established: 1972, Employees: 400
- **Tokyo**, Established: 1952, Employees: 300
- **Zürich**, Established: 1955, Employees: 300
- **Watson**, Established: 1961, Employees: 1750

Quoted from Security & Privacy Research Capabilities, IBM Report 2004
Security & Privacy Research at IBM - Solution Technologies

- New technologies that are implemented in current commercial solutions/offers to solve specific business issues

- IBM Secure CoProcessor Family
- JCOP Smart Card Technology
- Trusted Platforms
- Internet Banking Security Framework (IBSF)
- GILFAM – Advanced Electronic Signatures
- Biometrics and Surveillance Technologies
- Zurich Correlation Engine (ZCE)
- CLARAty: Clustering Alarms for Root Cause Analysis
- Intelligent Device Discovery (IDD)
- Early Detection of Network Service Worms (Billy Goat)
- Workstation Security Tool (WST)
- Auditing of Wireless Networks
- Software Tamper Resistance and Trusted JVM
- Broadcast encryption based key management
- Traitor Tracing
- Enterprise Privacy Architecture

Quoted from Security & Privacy Research Capabilities, IBM Report 2004

Wrap Up / End of Presentation

Please Remember...

- Security is a continuous process
- Security is everyone's responsibility