APEC-OECD Workshop - Parallel Session 3

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

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

06 September 2005

Agenda

- Hard Facts & Figures about Security (by 2004 CSI/FBI Computer Crime & Security Survey)
- Information Security Maturity (Year 1996, 2000, 2004, 2008 by Meta Group)
- 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

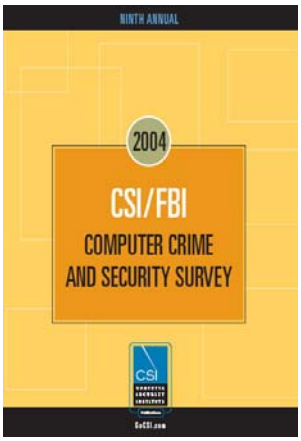
Hard Facts about Security - 2004 CSI/FBI Computer Crime & Security Survey

> 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).



Hard Facts about Security - 2004 CSI/FBI Computer Crime & Security Survey

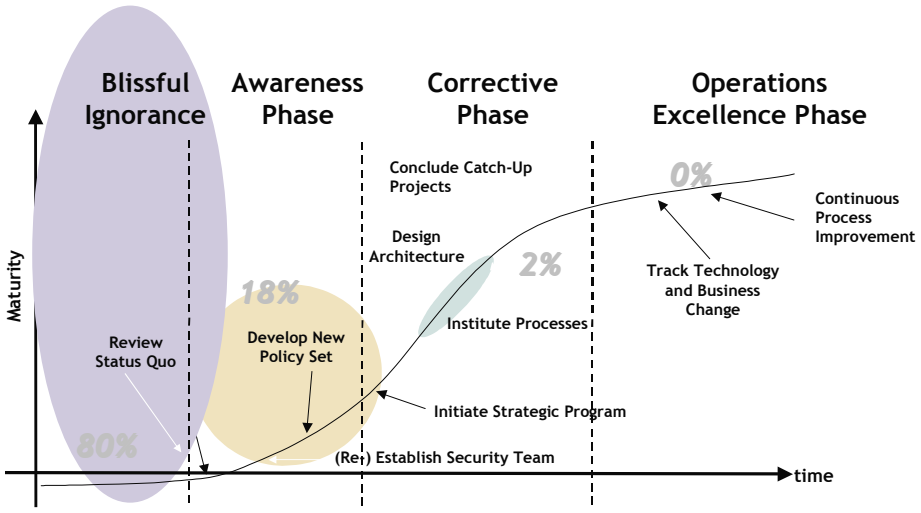
> Over **80 percent** of the organizations conduct security audits.

> 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.

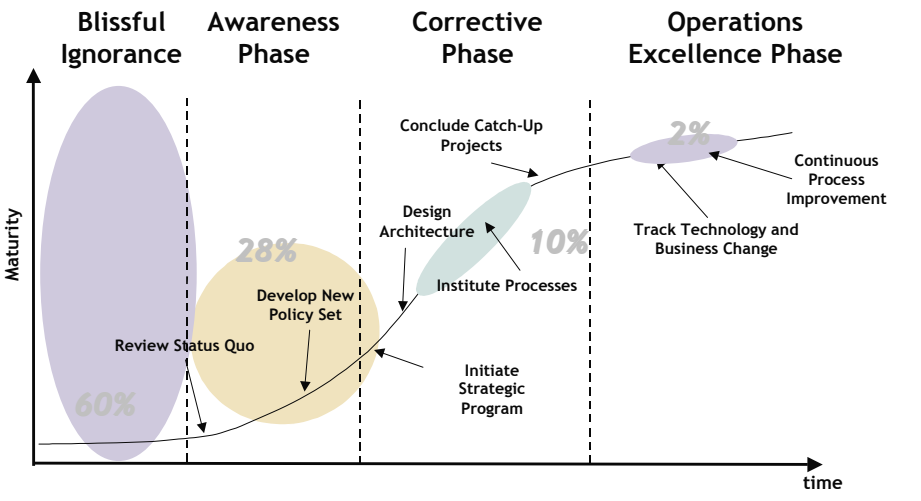
> The vast majority of the organizations view **security awareness training as important**, although (on average) respondents from all sectors **do not believe their organization invests enough** in this area.

Information Security Maturity: 1996



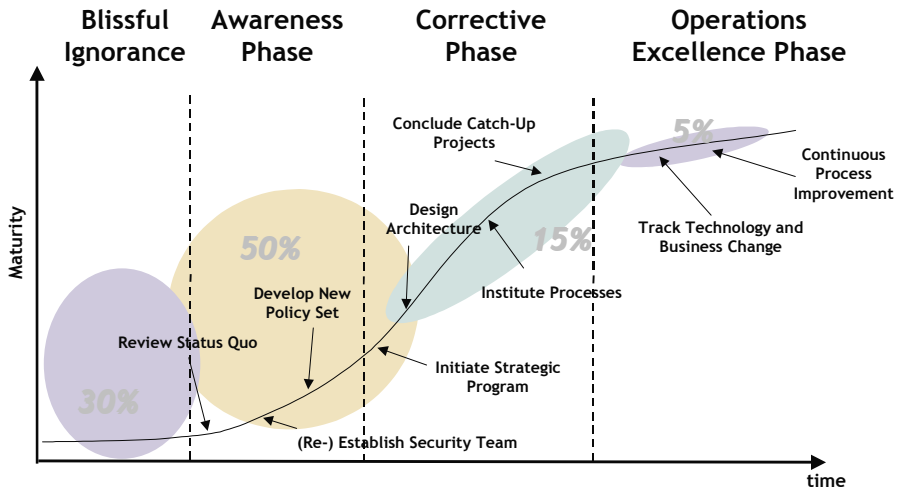
Quoted from [Meta Group] Security Programs, Trends and Markets - Security & Risk Strategies March 10, 2005

Information Security Maturity: 2000



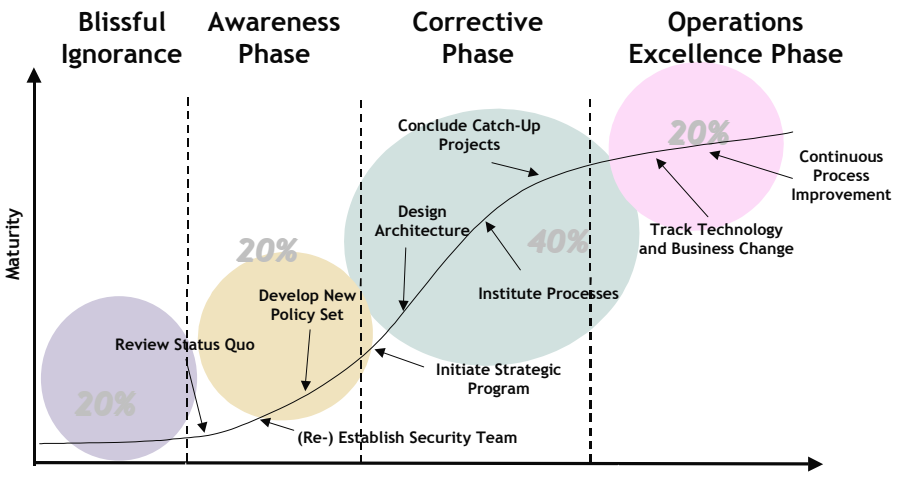
Quoted from [Meta Group] Security Programs, Trends and Markets - Security & Risk Strategies March 10, 2005

Information Security Maturity: 2004



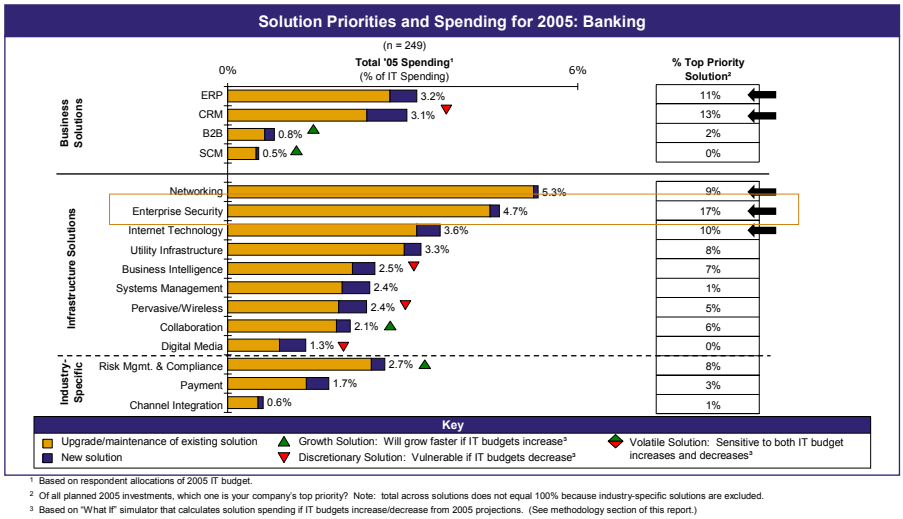
Quoted from [Meta Group] Security Programs, Trends and Markets - Security & Risk Strategies March 10, 2005

Information Security Maturity: 2008 (expected)



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

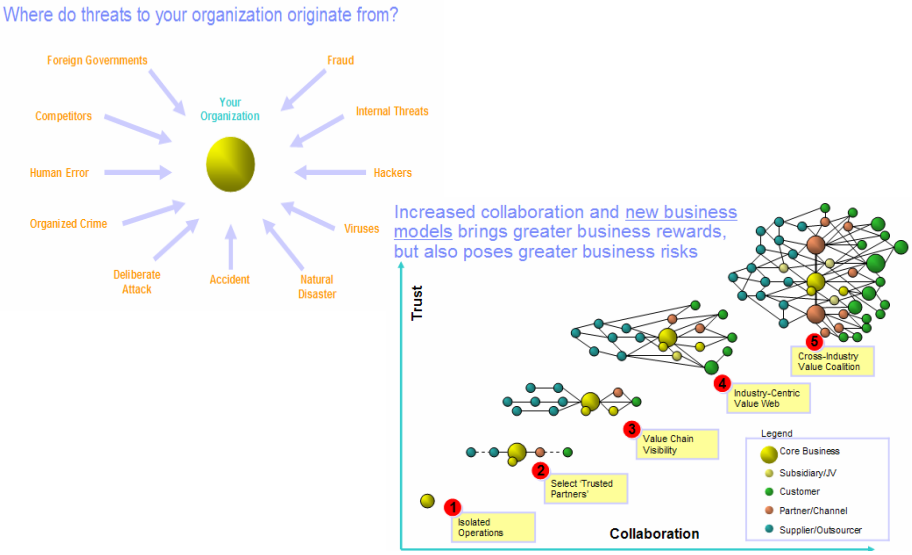
Security is the top priority



¹ Based on respondent allocations of 2005 IT budget.
² Of all planned 2005 investments, which one is your company's top priority? Note: total across solutions does not equal 100% because industry-specific solutions are excluded.
³ Based on "What If" simulator that calculates solution spending if IT budgets increase/decrease from 2005 projections. (See methodology section of this report.)

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



Pain Points – Security Breaches (Media Titles)

Pain Points – Understanding the pain

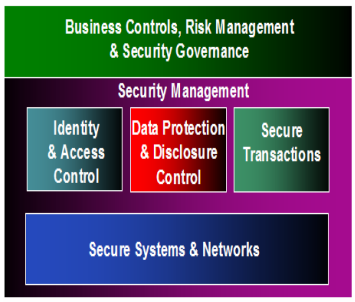
- Protecting privacy and security of customer and employee information
- Securing exchange of business critical information
- Manage identity within and across enterprise(s)
- Ensure integrity of the environment
- Manage security policies to mitigate risks

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 an 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



[Key Security Themes]

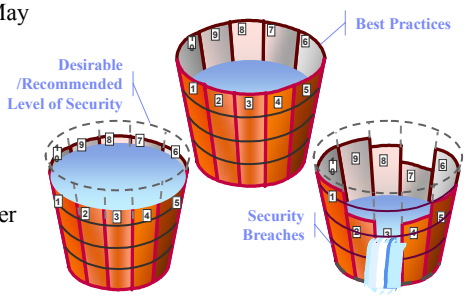
Pain Points – Countermeasures

- 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

[Information Security – Three Properties]



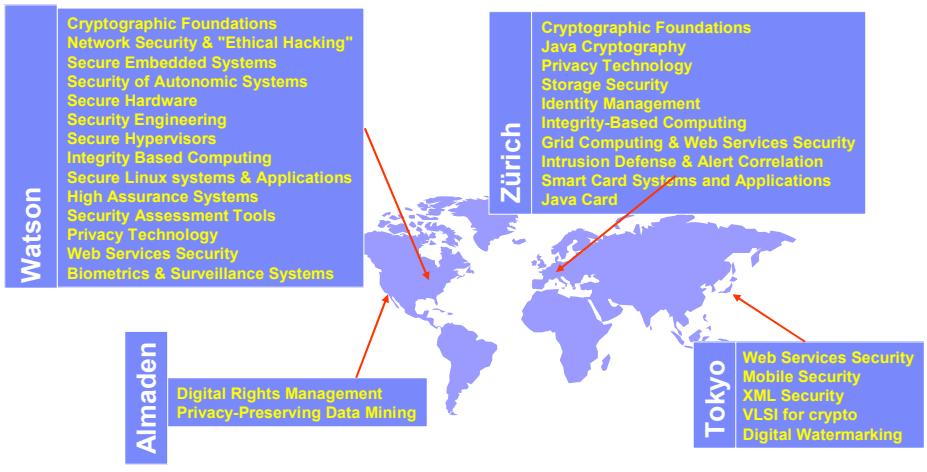
[How much security is enough? – Wooden Tub Model]

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

Quoted from Security & Privacy Research Capabilities, IBM Report 2004

Security & Privacy Research at IBM – Global Research Centers



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/offerings 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