Center for Education and Research in Information Assurance and Security
Second Annual Research Symposium

April 2001

Information Security as a Business Decision: The Case of the Financial Services Industry

Mukul Gupta, Alok Chaturvedi and Shailendra Mehta
Krannert Graduate School of Management,
Purdue University
Lorenzo Valeri
International Center for Security Analysis,
King's College, London

Contact: mehta@mgmt.purdue.edu
765 494 5703

http://www.cerias.purdue.edu

Outline

- **Security Threats**
- Environment
- Model
- Preliminary Results

E-commerce Security Breaches

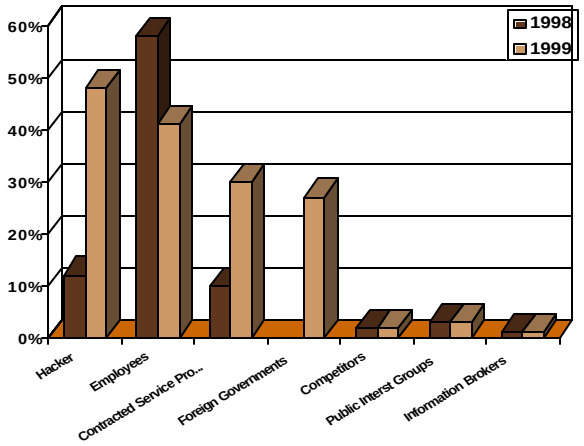
	Employee Access Abuse	Proprietary Information Leak	Destruction of Computer Resources	External Unauthorized Access	Malicious Code
Aerospace	55%	44%	33%	22%	55%
Banking and Financial	60%	30%	21%	17%	35%
Communication and High Tech	45%	32%	19%	34%	70%
Consulting	38%	22%	18%	18%	67%
Government	47%	16%	18%	18%	84%
Manufacturing	68%	18%	25%	25%	86%
Medical	70%	30%	20%	12%	80%
Military	50%	13%	13%	25%	88%

Source: Information Security Magazine, July 1999, http://www.icsa.net

Malicious Threats

- Outsiders
  - Crackers/Script Writers
  - Terrorists
  - Organized Crime
  - Competitors
  - Foreign Governments
- Insiders
  - Employees
  - Former Employees
  - Contractors
  - Outsourcing
  - Customers

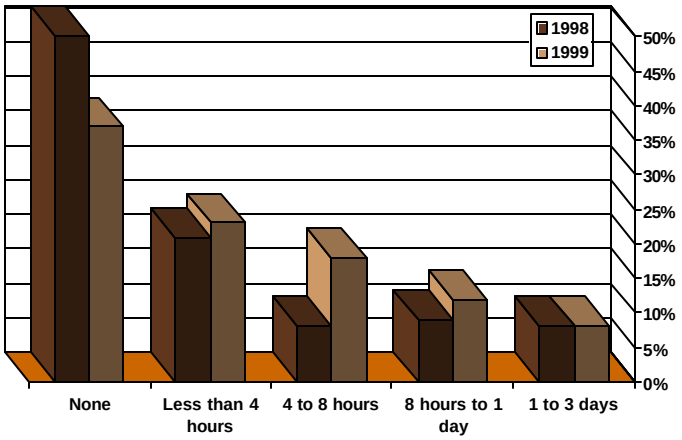
Malicious Threats



Non-Malicious Threats

- Malfunctions
- Loss of services, equipment or facilities
- Unforeseen effects of change
- Overloads
- Human errors

E-commerce Downtime



Source: Information Week July 1999

Outline

Security Threats
Environment
Model
Preliminary Results

Business Wargame

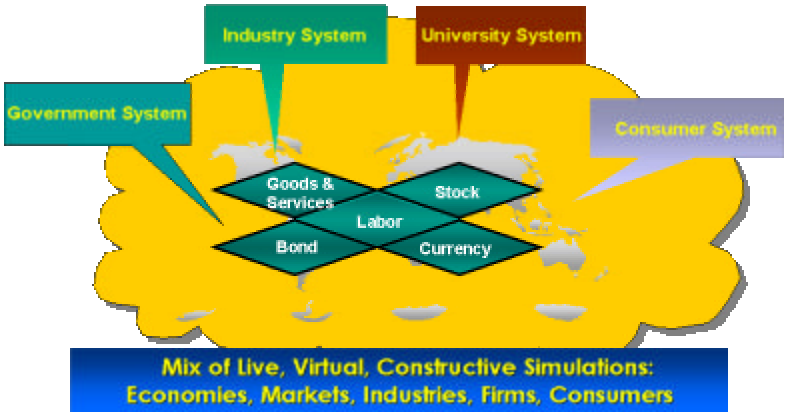
- Business counterpart of combat simulation, where battles are fought in marketplace rather than battlefields
- Main players are people and programs (manufacturers, distributors, resellers, and business customers)
- Allows experimentation of alternative management decision-making policies under pre-specified scenarios

Synthetic Environments for Analysis and Simulation

- A synthetically created economy with configurable goods and services, stock, bond, labor, and currency markets
- In these markets two kinds of agents interact
  - Live: people acting as firms, regulators and intermediaries
  - Virtual: artificially intelligent software agents behaving like human agents in a narrow domain

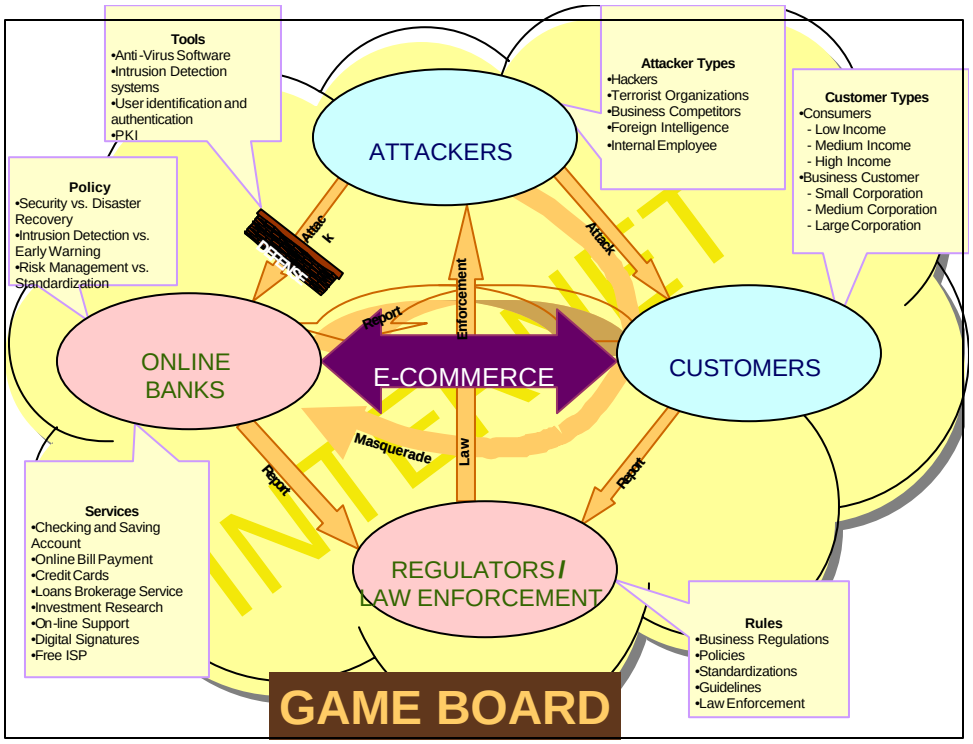
DoD's Synthetic Terrain

And Synthetic Terrain for Business War Gaming ..



Outline

Security Threats
Environment
Model
Preliminary Results



Services

- Checking and Savings Account
- Online Bill Payment
- Credit Cards
- Loans Brokerage Services
- Investment Research
- On-line support
- Digital Signatures
- Free ISP

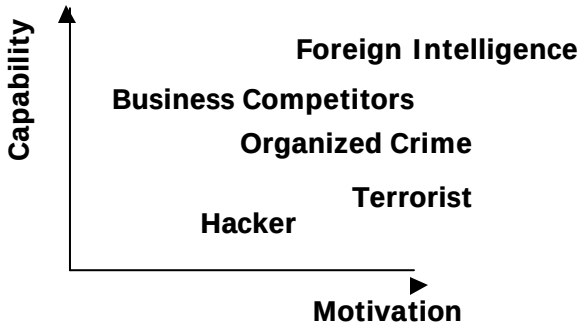
Human Agent Objectives

	Decision Category	Solutions	Choices	Key Performance Indicators
Business Decisions	Primary Services (Online Banking Report, 1999)	• Checking and savings account • Online Bill Payment • Credit Cards • Loans • Brokerage Services	• Product Bundle • Price • Quantity • Channel • Investments	• Revenues • Profits • Market Share
Business Decisions	Value Added Services	• Investment Research • On-line Support/Call Centers • Service Customization • Digital Signatures • Free ISP		
IT Decisions	IT Infrastructure	• Network • Operating System • Database • Application • Business Process	• Infrastructure • Investment Level	• Total cost of ownership • Quality of Service • Return of Investments
IT Decisions	Security Management (Financial Services Security Laboratory, 2000)	• Identification • Authentication • Authorization • Data Integrity • Audit • Data Disposal • System Integrity • Security Administration • Guidance • Non-Repudiation	• Security Feature • Investment level	• Security Index • Cost • Vulnerability

Behaviors

Agent	Behavior
Banks	Conservative Banks • invested in information security early and often and achieved higher revenue, profits, and customer satisfaction • banks were protected against attempted attack and were able to focus on core business activities Speculative banks • with little investments in information security did well early on, but once they suffered losses due to cyber attacks, they could not fully recover to compete effectively for several experiment periods • lost their customers trust and it was very difficult to win them back Belligerent banks • invested in offensive capabilities and resorted to espionage against their competitors • attracted the attention of the government and other competitive organizations and exposed them to retaliation from other banks and law enforcement
Perpetrators	• anti-social organizations that invested heavily in intelligence gathering capabilities showed a higher rate of successful attacks • those who did not gather intelligence often ended up wasting their offensive resources on banks that already had sufficient defensive resources • it was evident that artificial agents were better at terrorist activities than human agents
Law Enforcement	• when the law enforcement agents were very active and aggressive, the economy functioned very smoothly, and the cost of information security for the firms were much lower • when the government agents cooperated with firm agents on security and law enforcement, it benefited both the governments and the firms • although there was a tendency to not to disclose attacks, but when the victim banks made the attacks knowledge public, they generally performed better on the long run

Motivation and Capabilities



Defense

- Anti-Virus software
- User identification and authentication
- Intrusion Detection System
- PKI

Policy Decisions

- Security vs. Disaster Recovery
- Intrusion Detection vs. Early Warning
- Risk Management vs. Standardization

Outline

Security Threats
Environment
Model
Preliminary Results

Agents' Behaviors
Firms

- The conservative firms invested in security early and often and achieved higher cash balances
- These firms were protected against attempted attack and were able to focus on core business activities
- The speculative firms with no defense made money early, but once they suffered losses due to attacks could not fully recover to compete effectively for the duration of the game

Agents' Behaviors Perpetrators

- The terrorist organizations that invested heavily in intelligence gathering capabilities showed a higher rate of successful attacks
- Those who didn't gather intelligence often ended up wasting their offensive resources by wasting them on firms that already had sufficient defensive resources
- *Artificial agents proved to be better terrorists than humans*

Agents' Behaviors Government

- Governments that had security policies for their region attracted more firms and had higher GDP
- Governments that enforced law aggressively had higher GDP
- Governments that were unfair to foreign firms had declining GDP

Future Work

- Metrics for Valuation of Assets
  - Utility
  - Exclusive Possession
  - Cost of creation or recreation
  - Liability
  - Operational Impact
- Overall criteria
  - ROI
  - Reputation
  - Stock Market Value

From: Valuing Information Assets for Security Risk Management, *Information Systems Security*, September/October 2000 pp 17-23.

Summary

- Online banks are facing external and internal threats to their information systems
- The proposed simulation provides an artificial platform to design and test security policies
- Preliminary result provide some indication to successful strategies

Questions

?