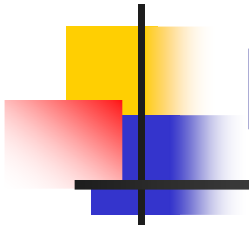
# Globalization and Offshoring of Software: Risks and Exposures

Sy Goodman
Georgia Institute of Technology
June 26, 2006

ACM Subcommittee: Jean Camp, Chuck House,
Bill Jack, Rob Ramer, Marie Stella



# Primary Categories of Risk

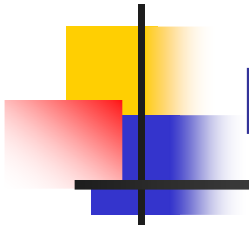
- Business risks (ref: Deloitte, 2005)
  - Structural
  - Cost
  - Organizational complexity
  - Legal
- Security (ACM “Globalization…” 2006)
  - Malicious exploitation of vulnerabilities
  - Accidental and natural disasters

# Primary Sources of Additional Risk and Exposure

- Longer supply chain and lines of communication
- Organizational and systems “intimacy” and complexity
- Multiple jurisdictions

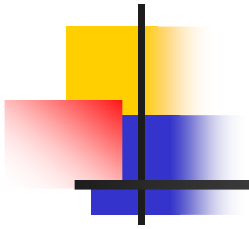
# Risks and Exposures By Victim

- Procuring or providing organization
- Individual
- National capabilities and security



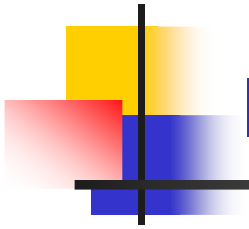
# Procuring or Providing Organization

- Systems intimacy - relationships can make one or both systems less secure
- Compounded insider problems
- Risks to intellectual property
- Third party attacks



# Individuals (you and me)

- Little (mostly no) say in business decisions
- Little we can do to protect ourselves
- Lots to lose:
  - Privacy
  - Jobs
  - Property (e.g., via identity theft, fraud)
  - Other security risks (e.g., other forms of crime)



# Individuals: Compromise of Personal Data

- Many (ChoicePoint counts in hundreds) recent (and probably past, before recent attention and reporting laws) instances of losses of sensitive personal data
- Risks potentially greatly increased if information is spread over multiple national jurisdictions
- Economic/market incentives and competition do not afford much protection

# Protecting the Sensitive Data of Individuals 1: Some Possible Requirements for Provider Companies

- Providers should have security and data protection plans. They should be required by contract and work should not be allowed to begin without them. There should be requirements for reporting incidents. Breach should be grounds for termination and redress.
- Providers might be certified,perhaps through adherence to prescribed standards. Who would certify the providers and stand behind the certifications?
- Providers should agree to no indirect third-party outsourcing arrangements without explicit approval from the procurer. This should be contractual, with heavy sanctions, e.g., termination.

# Protecting the Sensitive Data of Individuals 2: Some Possible Requirements for Provider Countries

- Provider countries should enact data privacy laws that applies to foreign citizens whose sensitive data is offshored to their country, or agree to recognize and enforce the laws of the procuring countries. Procuring companies should not do business in providing countries if the data is not protected at least as well there as in the procuring countries (e.g., a generalization of the Safe Harbor certifications of the EU).
- These laws should be backed by either demonstrated capacity to enforce them (e.g., by a good record of enforcement) or by secured assets in order to ensure penalty.

# Protecting the Sensitive Data of Individuals 3: Some Possible Requirements for Procurer Companies

- There should be reporting requirements and stiff penalties for failing to protect sensitive information - just like failing health inspections. While a procurer may be theoretically subject to privacy regulations, experience shows that practice is woefully lacking (recent examples for ChoicePoint and the VA notwithstanding).

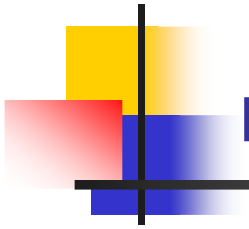
# Protecting the Sensitive Data of Individuals 4: Some Possible Requirements for Procurer Countries

- Procurer countries should consider legislation or other strong forms of regulation requiring any of the measures listed here.
- Certain information about a nation's citizens or business may be considered particularly sensitive and vulnerable and might be forbidden from being hosted (or even sent as a transaction) outside the originating country.

# Protecting the Sensitive Data of Individuals 5: Some Possible Technical Means

- There should be no mass export of databases or transactions.

  Databases should be kept on servers in the procuring countries. This would also make it easier to cut off a derelict of abusive provider.
- Data should be used in transactions on a one-record-at-a-time and as-needed basis. After one transaction is completed, another should not be initiated until the record for the first is effectively removed from further access.
- Databases should be encrypted to help protect data at rest and in transit, and to help prevent unauthorized data mining for purposes not intended by the procuring organization or contrary to relevant laws.
- Systems should be instrumented to facilitate discovery, reporting, and forensics.



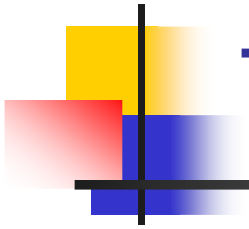
# Protecting the Sensitive Data of Individuals 6:

- More generally, I suspect that the R&E subcommittee would endorse the spirit and content of the just completed (literally last week) USACM Policy Brief on “Policy Recommendations on Privacy”

- (www.acm.org/usacm/Issues/Privacy)

# National Capabilities and Security

- Loss or atrophy of critical skills
- Means to enable attacks against critical infrastructures
- Compromise of providing organizations by organized crime, terrorist organizations, or national intelligence services.



# Two Final Notes

- Our analysis is not intended to be a blanket condemnation of outsourcing (domestic or offshore). We are advocating risk mitigation.
- The Privacy and Computer Crime Committee of the ABA just launched a book-length study of managing outsourcing risk. Our ACM study will be a major starting input to their effort. We expect it to provide more precise attention to matters of law and regulation than we could.