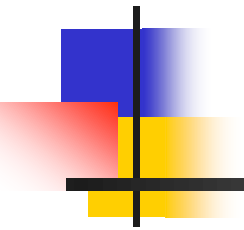

CSE 543
Information Assurance and Security

Information Assurance in Outsourcing

Professor Stephen S. Yau

Spring, 2014

What is Outsourcing?

- Outsourcing is an act of delegating or transferring some or all of the business process and services to external providers.
- External providers will develop, manage and/or administer these services in accordance with the contractual agreements on deliverables and QoS
- Examples of outsourcing
  - Using cloud computing services (software, platform and infrastructure services)
  - Outsourced software development
  - Using existing software from other organizations
  - Using Commercial Off-The-Shelf (COTS) items

Benefits of Outsourcing

- Low development cost
- Quicker development and deployment of timely services or products (accelerated time-to-market)
- Low cost for operations, maintenance and updates
- Accessing state-of-the-art expertise and skilled services
- Concentrating and investing more on core business

IA Challenges in Outsourcing

- ***Risk analysis and risk mitigation strategies*** are very difficult for outsourcing development
  - Difficult to identify risks of third party organization (e.g. risks of incomplete security requirements, insecure design, security vulnerabilities in implementation, incorrect testing, insecure deployment, various attacks)
  - Difficult to evaluate likelihoods and impacts of risks
  - Difficult to enforce risk mitigation strategies on third party organization

IA Challenges in Outsourcing (cont.)

- When a client uses ***outsourced software development***, the client may lose its control over the process of software development
  - The client does not know how the *development environments* of outsourcing providers are secure. (e.g. Are the environments safe from viruses, worms or other deliberate attacks?)
  - Are all the ***employees*** of the third party outsourcing providers trustworthy?
  - How to ensure ***security mechanisms*** are implemented properly?
  - How to ensure ***security tests*** are performed correctly?
  - How to ensure the developed software will be ***compatible*** with client's systems (ensure that outsourced software can run on client's systems without problems).

IA Challenges in Outsourcing (cont.)

- Client and outsourcing provider may have ***conflicting security policies and procedures***.
  - The client and the outsourcing provider may take different approaches to dealing with known vulnerabilities, intrusion detection, or perimeter defense.
  - These discrepancies may easily create vulnerabilities for the client.
    - For instance, a software developer made certain assumptions on firewalls and intrusion detection, which are not valid on the client's operating environments

IA Challenges in Outsourcing (cont.)

- Creating risks to client's ***intellectual property***
  - Litigation can take years of effort while the damage is immediate.
  - Trade secrets, customer data, and financial information often need to be made available to an outsourcing provider whose employees are not subject to U.S. laws.
    - The laws applying to protection of data are often non-existent in some offshore countries.

IA Challenges in Outsourcing (cont.)

- Ensure that outsourcing providers' facilities and all personnel ***adhere to the client's standards and laws*** regarding protection of data and intellectual property.
- Ensure that both client and outsourcing providers include ***security professionals*** in regular review meetings to ensure satisfaction of security requirements, and enforcement of security policies and procedures without conflict.
- Both clients and outsourcing providers document all the development process activities (including requirement, design, implementation, testing) in proper format and reviewed carefully.

COTS-Based Systems

- COTS: ***Commercial Off-The-Shelf***
- Companies, organizations and government agencies often use COTS items to build a system
  - Example: Use commercial database management software and web server software to build a web based system
- Benefits of COTS-based systems
  - Reduce development cost and time
  - COTS are proven to work
  - Technical supports from vendors

Risks for COTS-Based Systems

- ***Difficult to verify security*** of COTS products
  - COTS users often can review neither the source code, nor the software architecture.
  - COTS users have to rely on the reputation of the vendors, published security reports, and security forums.
- COTS software is generally a more ***attractive target for attackers*** than customized code
  - COTS software may be well known and widely available
  - More information on security vulnerabilities and viable attack patterns is shared
  - Attackers likely gain more benefits from attacking COTS products
- DoD agency: Defense Information Systems Agency (DISA), Joint Interoperability Test Command (JITC)

Risks for COTS-Based Systems (cont.)

- COTS vendors have very ***limited liability***
- COTS components are often ***generic***
  - Development of COTS items is primarily driven by vendors' perceptions of what will sell to the largest number of potential users
  - COTS components will ***likely lack specific security features*** needed by certain users.
  - COTS code does ***not address specific operating environment and business context.***

Mitigating Risks for COTS-Based Systems

- ***Identify all components*** to be integrated into COTS-based systems, including both COTS and customized components.
- ***Understand business goals and context*** of the system
  - What sensitive information is processed and stored in system?
  - What security mechanisms are required to protect the sensitive information in the system?
- ***Understand how COTS and customized components are connected***
  - Understanding these connections is critical to understanding how the vulnerability in one component may affect other components and how changes in one component can expose vulnerabilities in others.

Mitigating Risks for COTS-Based Systems (cont.)

- ***Control Access***
  - Developers of COTS components generally assume that access is controlled in appropriate ways by distributers and/or users
  - Implementing proper access control over each COTS component is critical
- ***Ask the Vendor***
  - Security-related problems over the history of COTS components
  - Security-related patches for the problems
- ***History***: Frequency of occurrences of security-related problems and vendor's diligence in addressing the security problems are important factors in selecting the COTS components.

Mitigating Risks for COTS-Based Systems (cont.)

- Engage with ***user community and security community***
  - Significant COTS items, especially software, are often addressed in online forums.
  - The information of these forums should be consulted before making purchase decisions as part of the design of the installation, and on a continuing basis during operations and maintenance phases.
  - Do not assume that all is said in these forums is accurate, but what is said there should be considered seriously.

Mitigating Risks for COTS-Based Systems (cont.)

- Engage with the ***experts***
  - Experienced security specialists, both individuals and companies can provide valuable advices for purchase, and assist with the design, implementation and verification.
- Look for ***certification***
  - Purchase COTS software from vendors who have demonstrated high quality of their software and development processes, such as ISO certification and CMMI appraisal

Mitigating Risks for COTS-Based Systems (cont.)

- Pay attention to ***updates***
  - Keep COTS software updated for latest security patches
- ***Monitoring***
  - Commonly used COTS software usually has logging capability to capture valuable information for anomalous behavior
- Prepare for ***failures***
  - Prepare how the organization should respond as failures might unfold