OUTSOURCING

CSH6 Chapter 68
"Outsourcing & Security"
Kip Boyle, Michael Buglewicz,
& Steven Lovaas

Topics

➢ Introduction
➢ Why Outsource?
➢ Can Outsourcing Fail?
➢ Controlling the Risks
➢ Outsourcing Security Functions
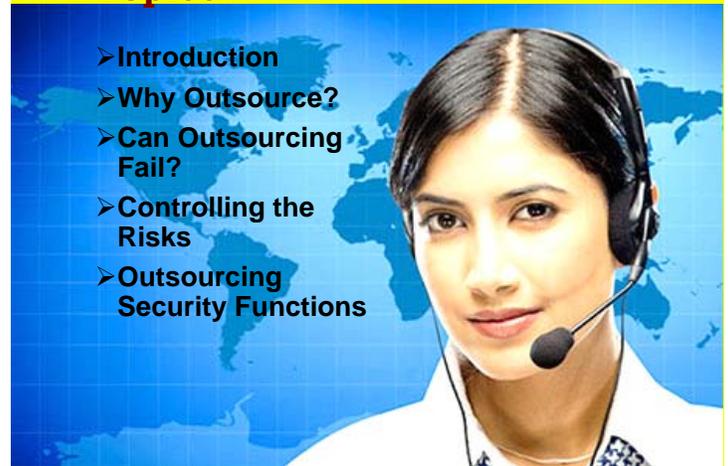
Introduction

➢ Opening Remarks
➢ Definitions
➢ Distinctions
➢ Insourcing
➢ Nearshoring
➢ Offshoring
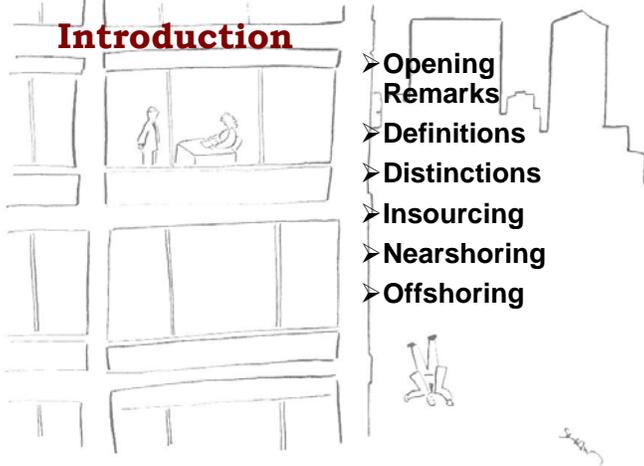
"Outsourcing? First door on your right."

Opening Remarks (1)

➢ "Outsourcing" encompasses different concepts
➢ Need different risk-management strategies
➢ Outsource for efficiencies & effectiveness
➢ Consequences: environment can change fast
➢ Key issues for early 21st century for outsourcing:
  ❑ Security problems
  ❑ China's rise
  ❑ India's growth & turmoil
  ❑ Blunders
  ❑ H-1B visa problems
  ❑ Small business outsourcing
  ❑ Managed services

Opening Remarks (2)

Benefits possible:
➢ Self-knowledge improves when forced to articulate needs, mission
➢ Clarify/institutionalize roles, goals, metrics
➢ Risk identification & mitigation
➢ Focus on core competencies
  ❑ Effectiveness
  ❑ Efficiencies
  ❑ Focus
  ❑ Discipline
➢ Cost savings

Definitions

➢ Vendor / contractor:
  ❑ Arm's-length entity
  ❑ Provides specific outsourced service(s)
➢ Organization / business:
  ❑ Entity contracting for products / services with vendor
➢ Outsourcing:
  ❑ Fulfillment of specific business function(s)
  ❑ By contracting with vendor
  ❑ To perform in vendor's facilities
➢ Insourcing:
  ❑ Use of contract / noncompany employees for specific in-house functions

Distinctions

- Many applications of out/insourcing possible
  - Call center
  - Corporate IT
  - Corporate finance
  - Corporate security
- Must not impose one rigid framework
- Different needs imply different priorities & methods
- Identify core business missions
  - Consider moving non-core functions outside
  - Or hiring contractors

7

Insourcing

- Commonplace to hire contractors
- Risks
  - Workplace for outside employees is inside security perimeter
  - High potential for abuse if contractor dishonest
  - May not have same trust in contractors as in employees
  - Plan for coping with errors by contractors
- May need specific / separate security classifications for employees, contractors
- Contractors may fail to comply with regulatory / legal requirements if policies unclear

8

Nearshoring

- Outsourcing specific discrete business function to
  - Same geographical region
  - Nearby region
  - Bordering region
- E.g.,
  - US nearshoring could include contracting out to US firm
  - Or Canadian or Mexican firms
- Many large companies nearshore services
  - EDS Agile, HP SMB Services, IBM Express Advantage

9

Offshoring

- Outsourcing specific, discrete business functions to vendor on another continent
  - E.g., EU company outsources a function to Indian company
- Considerable emotion in discussions
- Important to evaluate possibilities carefully
  - Understand your business
  - Articulate outsourcing / nearshoring / insourcing goals
  - Clear analysis of risks & management issues

Why Outsource?

- **Effectiveness vs Efficiency**
- **Being Effective**
- **Being Efficient**

"You'll be a perfect addition to our expendable workforce."

P.C.VEY

Effectiveness vs Efficiency

- Efficiency: using optimal resources for specific task
- Effectiveness: getting the work done as intended

12

Being Effective (1)

- Optimizing processes outside core competency is wasteful
- Core competencies
  - Mission-critical tasks / functions
    - ✓ Directly related to strategic goals
    - ✓ E.g., hospital / restaurant considers cleanliness mission-critical
  - That organization good at _____
  - E.g., for specific firms,
    - ✓ Brand management
    - ✓ Continuous improvement
    - ✓ Superior retail service
    - ✓ Supply chain management
    - ✓ Look / feel of products

Being Effective (2)

- Core competency requirements
  - Can be used to develop entirely new products / services
  - Provides significant customer benefits
  - Difficult for customers to duplicate
    - ✓ At least for a time
- Core competency can provide competitive advantage(s)
  - Therefore all other functions candidates for outsourcing
  - Focus resources on what counts

14
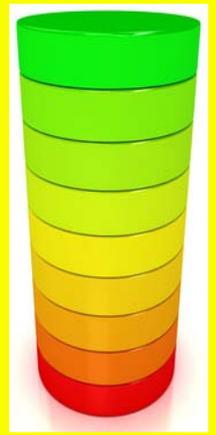
Being Efficient

- Measuring efficiency
  - Direct cost minimization
    - ✓ E.g., UK companies save ~40% costs by using labor in India
    - ✓ Save £10M for every 1,000 jobs outsourced
- Benefits of outsourcing
  - Decreased capital investment
  - Decreased fixed costs
  - Increased variable costs vs fixed costs
    - ✓ Pay by volume of service / products
  - Increased speed / reduction work cycle time
  - Management focus – emphasize competitiveness

15

Can Outsourcing Fail?

- Yes, Outsourcing Can Fail
- Why Does Outsourcing Fail?
- Universal Nature of Risk
- Clarity of Purpose & Intent
- Price
- Social Culture
- International Economics
- Political Issues
- Environmental Factors
- Travel
- Labor
- Additional Risks

16

Yes, Outsourcing Can Fail

- JP Morgan Chase (2004)
  - Terminated U$5B contract with IBM
- EDS (Electronic Data Systems)
  - Terminated U%1B contract to run Dow Chemical phone / computer networks

17

Kathleen Sebelius Admits Obamacare Website Was Not Ready

http://www.inquisitr.com/1211143/kathleen-sebelius-admits-obamacare-website-was-not-ready/

Kathleen Sebelius is now saying the Obamacare website HealthCare.gov was not ready, months after the critical piece of the Affordable Care Act has already set sail.

HealthCare.gov Failure (2)

The Inquisitr previously spoke to anonymous computer experts who gave their analysis of why the Obamacare website glitches were so noticeable:

"The Obamacare website problems are most likely caused by the design of HealthCare.gov. It requires people to register for an account, confirm email, validate identity, and validate eligibility before they can see insurance plan information, which creates an unnecessary up-front bottleneck. This means all these processes were hitting the server databases as soon as someone attempted to create a HealthCare.gov user account. Creating that bottleneck up-front puts all users down the same funnel — even those who are only curious and have little intention to buy insurance. The other issue is that many people are choosing to try the Federal Obamacare website instead of using one of the sites for the state exchanges."

Deloitte Consulting 2005 Study

- "Calling a Change in the Outsourcing Market"
  - Interviews with 25 large organizations in 8 sectors
- 70% respondents looking more cautiously at outsourcing due to bad experiences
- 25% canceled outsourcing when promised savings / higher efficiency failed
- 44% saw no cost savings

Deloitte Consulting

Why Does Outsourcing Fail?

- Danger when focusing primarily on *cost reduction*
  - But in 2004-2006, rate of cost-savings as primary driver rose from 70% to 80% respondents
- But including *effectiveness* can change evaluation
- Problems
  - Measuring performance difficult
  - Failure to create win/win situation
  - Difficult to align goals of organization & vendor
  - Must master new / more complicated communications
  - Maintaining sufficient knowledge / skill in outside workforce
  - Insecurity perceived by internal employees & unions
 - Contract termination can be disruptive to clients (lower QoS)

BENCHMARKING

Universal Nature of Risk

- Greatest cost: ignorance
- Greatest price: failure
  - Poorly defined expectations / poor planning = doom
- Planning
  - IA team should assess entire outsourcing project
  - IA not only team involved
  - But must not restrict IA merely to technical details
  - Liability remains with firm, not outsourcing provider

"You're what we call 'high risk.'"

IA Review of Proposals

- What information assets at risk?
- Value / sensitivity of assets
- Current / future "risk shadow" due to outsourcing?

Clarity of Purpose

- Must articulate tasks
  - Rely on employees to define specifics
  - Conflict of interest: often those defining tasks are ones to be fired after outsourcing!
- Phases
  - Analysis – define/document work
  - RFI (request for information)
  - RFP (request for proposal)
  - Vendor selection
  - Training
- Focus on mutually beneficial vendor relations

Risks Related to Clarity of Purpose

> - Poor identification / definition of task(s)
> - Employees defining tasks may be training their replacements
> - Workforce reduction traumatic
>   - Uncertainty
>   - Unrest
>   - Resentment
> - Lowered morale may have consequences
>   - Lost productivity (water-cooler discussions)
>   - Insider sabotage
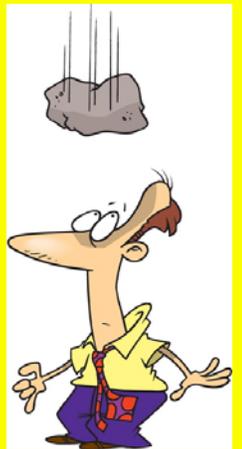
Price

> - Beware paper-thin profit margins
>   - Vendor must also survive and profit
>   - Otherwise see constant corner-cutting
> - Beware short-term profit evaluations
>   - Take long-term view
>   - Client must see significant long-term profit

-10% -20% -30%
-40% -50% -60%
-70% -80% -90%

Social Culture

> - Vendor must cope with client culture
>   - Be conscious of social norms across international boundaries
> - Client must evaluate differences in beliefs / attitudes / behaviors
>   - Especially important for outsourced client contacts such as technical support
>   - Parkerian Hexad
>   - Particularly timeliness
>   - Some hostility developing in USA towards foreign accents (e.g., Indian) in support

International Economics

> - Keep long-term economic developments in mind
>   - Collapsing economy may terminate contracts
>   - ✓ Vendor may go out of business
>   - ✓ Social disruption may stop all business
>   - Once functions outsourced, business continuity affected if supplier fails
> - Changes in exchange rate may affect costs if contract fails to stipulate *client's* currency for charges
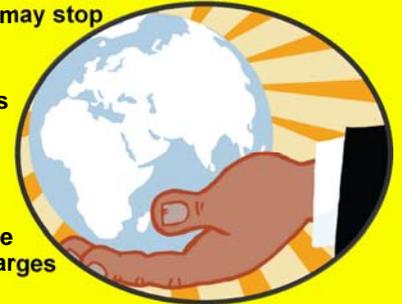
Political Issues

> - Graft / bribery vs national laws (e.g., US legal restrictions on such payments)
>   - Foreign Corrupt Practices Act of 1977 (FCPA) (15 U.S.C. §§ 78dd-1, *et seq.*)
> - Opposing political forces' attitudes to outsourcing vendors
> - Terrorism causing increasing concerns for vendors & clients
>   - E.g., Taliban defines anyone doing business with US / Intl armed forces as targets
> - Rule of law: is there any (e.g., China, Burma)?

Environmental Factors

> - How likely are natural disasters in remote location?
> - Could natural disaster trigger political collapse?
> - What is host country's capacity for recovery from environmental disaster?
> - Will regional infrastructure cope with disruptions to maintain QoS / SLA?

Travel

> Employees will have to visit vendor or client
> - Training
> - Quality control
> - Management coordination
> Keep in mind
> - Travel costs ($$, productivity, morale)
> - Employee safety / health (food, disease, war, insurrection, kidnapping)
> - Delays for travel documents (e.g., visas)
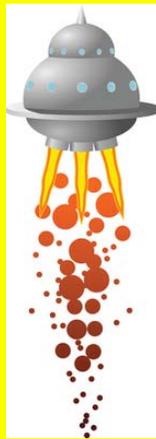
Labor

> Risks
> - Turnover (requiring more training)
> - Escalating wages
> - Work stoppages
> - Cost growth
> Examine history & forecasts
> - Supply of workers
> - Worker exploitation (may violate client country's laws & affect public image, employee morale – or lead to boycotts)

Additional Risks

> Loss of corporate expertise
> Loss of direct control
> Internal changes in corporate purpose
> - Moving from doers to managers of doers
> Overhead of ongoing contract management

Controlling the Risks

> Controls on What?
> Controlling Outsourcing Risk
> Availability Controls
> Utility Controls
> Integrity & Authenticity Controls
> Confidentiality & Possession Controls
> Making the Best of Outsourcing

Controls on What?

> Players
> - People
> - Corporations
> - Societies
> - Governments
> Focus primarily on organizational behavior
> - Policies, contracts, agreements, trust relations critical
> - Information security policy critical
> - Coordinate with legal dept: contracts / site selection / politics / economics / separation of duties

Controlling Outsourcing Risk

Use Parkerian Hexad as framework for analysis / remediation
> Confidentiality
> Control or Possession
> Integrity
> Authenticity
> Availability
> Utility
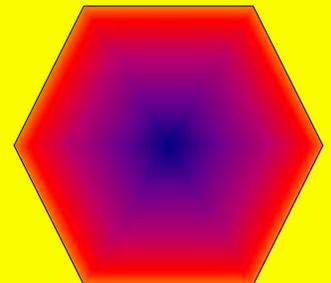
Availability Controls & Outsourcing

- Infrastructure can be determinant
  - E.g., trans-Pacific cable cut Feb 2007
  - Most of Asia inaccessible to North America via Internet
  - Distance increases risk of interruption
- Backup strategy critical
  - BCP essential for vendor & client sites
  - Consider backup *vendor* contracts
- SLA may be unenforceable if no rule of law
- Evaluate possible vendor(s) carefully
  - Site visits
  - News / government reports
- Monitor situation in vendor locale continuously

US Dept of State Country Reports

38

Utility Controls & Outsourcing

- Careful version control
- Encryption recovery (for forgotten keys)
  - Beware national/international restrictions on encryption technologies
- Beware incompatible formats
- Language issues
  - Accents
  - Word usage
  - Writing

39
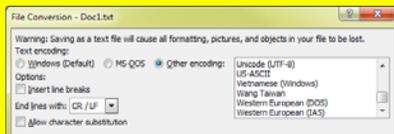
Integrity & Authenticity Controls & Outsourcing

- Prevent unauthorized or accidental modifications
- Analyze vendor's history / reputation
- But effective collaboration may required access to sensitive corporate data
- Trust infrastructure
  - Access control mechanisms
    - ✓ RBAC* / least privilege important
  - Division of labor
  - Delegation of responsibilities
  - Vendor must not be able to change structure
- Monitoring incorporated into contracts
  - Audits – preferably unannounced
  - Where are backups kept?
  - Change-tracking on servers

*Role-based access control

40

Confidentiality & Possession Controls & Outsourcing (1)

- Outsourcing inherently compromises confidentiality & control
  - Decide if balance is positive
  - Laws *may* protect balance – if there is in fact rule of law on both sides
- HSBC call center – Bangalore, India – 2006
  - Employee arrested
  - Hacked into bank's computers
  - Stole £233,000
  - Hired because of forged high-school transcripts
  - Only criterion for hiring was English skills
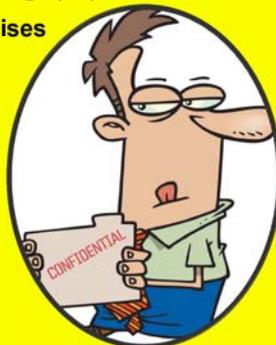
41

Confidentiality & Possession Controls & Outsourcing (2)

- Constant monitoring / audit
  - Clear terms of contract
  - Unannounced audits
  - Monitor log files, real-time security tools
- May replace absent laws by contract terms
  - Failure of security → termination of contract
  - May not help if legal process in vendor's country
  - But could help in client's country

42

Making the Best of Outsourcing

➢ **Careful planning**
➢ **Careful implementation**
➢ **Focus on trust & monitoring**
  ❑ **"Trust, but verify"**
➢ **Plan for threats to availability**
  ❑ **BCP / DRP**
➢ **Training, liason**
➢ **Integrate security into contract terms**

Outsourcing Security Functions

➢**Overview of Security Outsourcing**
➢**Who Outsources Security?**
➢**Why do Organizations Outsource Security?**
➢**Risks of Outsourcing Security**
➢**How to Outsource Security Functions**
➢**Controlling Risk of Security Outsourcing**

Overview of Security Outsourcing

➢ **Can improve overall security**
  ❑ **Take advantage of specialized security expertise / experience / perspective**
  ❑ **Depends on vendor's history / reputation**
➢ **Contracted security-guard force commonplace**
  ❑ **Example of insourcing**
➢ **Increasing use of security-service vendors**
  ❑ **Nearshoring**
  ❑ **Includes software testing for security vulnerabilities**

Outsourcing Security (1)

The following snapshots are from the document shown here.

Link (abbreviated) is:

http://tinyurl.com/opfemca

www.pwc.com/gsiss2015

Managing cyber risks in an interconnected world

Key findings from The Global State of Information Security® Survey 2015

30 September 2014

pwc

46

Outsourcing Security (2)

Cybersecurity services market is expanding

In the wake of increased incidents and heightened regulations, corporations and government agencies are scrambling to safeguard their data and networks— a push that is catalyzing growth in the market for cybersecurity solutions and technologies.

Research firm Gartner predicts that global IT security spending will increase 7.9% to $71.1 billion in 2014, and grow an additional 8.2% to reach $76.9 billion in 2015, according to *The Wall Street Journal.*[19]

The upsurge in security incidents and the resulting media coverage has helped unleash a flood of venture capital investment in companies that provide cybersecurity software, solutions, and services.

During the first six months of 2014, venture capital firms invested $894 million in US cybersecurity startups, almost the same amount invested in all of 2013.[20] That puts the sector on track to post the highest investments in more than a decade. At the same time, the market capitalizations of some security firms hit new highs in the past year.

47

Outsourcing Security (3)

At the height of the venture-funding boom, the valuation of some cybersecurity companies was five-to-ten times their annual revenues in 2013.

Network security provider FireEye, after a $304 million initial public offering (IPO) in 2013, now has a market cap of approximately

$4.6 billion[21]

Enterprise firewall specialist Palo Alto Networks raised $260 million in a 2012 IPO and now has a market cap of approximately

$6.2 billion[21]

48

Why do Organizations Outsource Security? (1)

➢ Staffing Challenges
- ❑ Training & retention
- ❑ Key to success is deep understanding of specific business
- ❑ Should always look for ways of focusing employees on mission-critical functions
- ❑ Distribute less taxing, routine jobs to others
- ❑ Save on constant training costs by shifting to outsourcing firm

➢ Financial Savings
- ❑ Can be significant, esp for 24 hr monitoring
- ❑ Finding savings of 6x by outsourcing

49

Why do Organizations Outsource Security? (2)

➢ Threat intelligence / additional perspectives
- ❑ Enormous volume of threat info
- ❑ Difficult to keep up without full-time focus / team
- ❑ Smaller organizations cannot keep up

➢ Managed System Security Providers (MSSPs) can help
- ❑ Much larger staff dedicated to intelligence gathering / analysis
- ❑ May be able to negotiate training for in-house staff
  - ✓ But not always – vendors may consider info proprietary
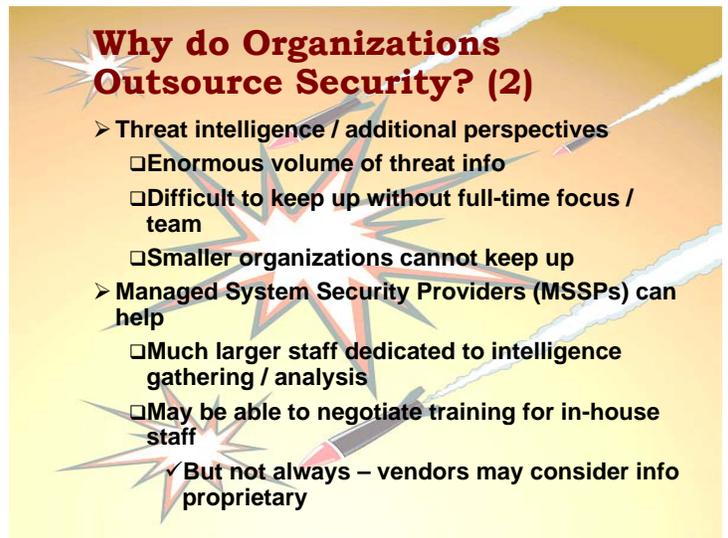
Risks of Outsourcing Security

➢ Conflict of interest: profit rises as detection decreases
➢ Where is your organization on vendor's priority list in emergency?
➢ Are costs determined by number of events? If so, how to monitor & prevent abuse?
➢ Where are vendor's employees? Offshore?
➢ Is theft of intellectual property & industrial espionage major issue? (e.g., China, India)
➢ How carefully does vendor verify employee backgrounds / qualifications?
➢ Who monitors vendor's employees when they are accessing your data?

51

How to Outsource Security Functions (1)

➢ SOW (Statement of Work)
- ❑ Consider work volume when partitioning responsibilities
- ❑ E.g., 1 case had administrative passwords stay under control of in-house staff
- ❑ Non-administrative passwords delegated to vendor

➢ Determine desired outcomes
- ❑ QoS: Quality of Service
- ❑ SLAs: Service Level Agreements
- ❑ E.g., reset password within 4 hours in 99% of cases

52

How to Outsource Security Functions (2)

➢ Choose reliable vendor
➢ Evaluate
- ❑ Financial health
- ❑ Reliable infrastructure
- ❑ Competent staff
- ❑ Satisfied customers
- ❑ Vendor independence
- ❑ Appropriate SLA
- ❑ Legal safeguards

53

How to Outsource Security Functions (3)

➢ SLA (Service Level Agreement)
- ❑ Outcomes desired
- ❑ Response times
- ❑ Roles & responsibilities
- ❑ Metrics
  - ✓ Statistical quality control

➢ Continuous process improvement
- ❑ Ensure that vendor is free to report mistakes
- ❑ Focus on improvement, not penalties

54

Controlling Risk of Security Outsourcing

➢ **Contract-management skills essential**
➢ **Ongoing monitoring by client**
➢ **Coordination with legal department**
  ❑ **Prepare for failure of SLAs or QoS**
➢ **Coordination with in-house security staff**
  ❑ **Continuity of operations part of BCP**
    ✓ **Be sure staff know what to do if service goes bad**
  ❑ **Immediate revocation of access to service-provider's copy of data & services if contract annulled**
  ❑ **Especially important for high-level administrative accounts**

55

DISCUSSION

"Well, that does it, Charlie—we've outsourced everything."