Communications of the Association for Information Systems

Volume 20 Article 50

December 2007

Global Sourcing of IT Services and Information Security: Prudence before Playing

Seymour E. Goodman
Georgia Institute of Technology, goodman@cc.gatech.edu

Rob Ramer
Aeritae Consulting Group

Communications of the Association for Information Systems

GLOBAL SOURCING OF IT SERVICES AND INFORMATION SECURITY: PRUDENCE BEFORE PLAYING

Seymour E. Goodman
Georgia Institute of Technology
goodman@cc.gatech.edu

Rob Ramer
Aeritae Consulting Group

ABSTRACT

This paper calls for awareness of the risks in global sourcing of IT and IT-enabled services. It calls for appropriate assessment and mitigation of these risks. The authors identify ways in which global sourcing (often called offshoring) increases information security exposures and recommends strategies for managing such risks.

Keywords: Outsourcing risk, offshoring, global information risk, risk management, information security, privacy, law

I. INTRODUCTION

Global sourcing of IT services expands the potential number of system vulnerabilities by lengthening communication channels and increasing the number of organizations and computer networks that touch the data. Global sourcing, often called offshoring, increases the number of risks and exposures[1] to a procuring company through intimate connections with network systems and legal and political jurisdictions where foreign governments and a larger number of illicit organizations have a greater presence.

This paper examines how offshoring exacerbates information security risks. While these risks exist in other contexts, e.g., within a single organization or domestic outsourcing, offshoring introduces new forms of risk by opening more opportunities for incursion, accident, or exposure. For example, offshoring may expose an organization's computer systems to a larger population of criminals who are not likely to be held accountable for harm done to citizens of another country. Another example is that offshoring often occurs across channels of communication that are not under the effective control of either the procuring or providing companies (respectively the buyers and vendors of outsourced IT services) or their parent countries.

We raise these concerns, not to condemn offshoring but rather to show how these risks can be better managed. Any risk that is identified and properly assessed can be managed to some

[1] In this paper *risk* is the potential for a security breach and *exposure* is an asset that is put at risk.

extent. We hope that the problems presented here will lead to greater prudence and more cautious, thoughtful, and effective practices in risk prevention. The goal of this paper is to raise awareness and thus contribute to the appropriate assessment and mitigation of these risks.[2]

This paper and the two large studies, which underpin it [Beaumont et al. 2005; Goodman et al. 2006] do sound alarms and encourage caution because of the rapidly growing number of security and privacy violations experienced with information systems, This paper is written from the perspective of U.S.-based procuring companies and does not examine the risks that service providers also face. The perspective is reinforced by the greater availability of reports on violations in the U.S. and in the English language, and the greater familiarity the authors have with U.S. laws and regulations than those for any other country. Nevertheless, we believe that many of the concerns and the prudence advocated in this paper also apply more generally for non-U.S. procurers and domestic outsourcing as well.

In this paper we examine the drivers behind the increased prominence of Information Security (InfoSec) and then examine how global sourcing or offshoring exacerbate InfoSec risks and exposures. We use the classic vulnerability, threat, and risk model[3] to show how offshoring risks are indeed greater than in-country outsourcing. The paper then examines the actual targets of the threats, that is, who and what are impacted by the increased risks and exposures. We conclude with a section that examines ways to mitigate the risks.

WHO CARES ABOUT SECURITY?

Information security used to keep security professionals up at night while IT leaders and their business counterparts slept soundly. In 2007 security became a more serious concern of U.S. business leaders and their legal departments because of at least three drivers:

1) Regulatory concerns in financial services and other industries (See Appendix I for key laws & regulations);
2) The Payment Card Industry Data Security Standard (commonly known as PCI); and
3) Changes to court rules requiring availability and proof of integrity of electronically stored information (ESI) submitted as evidence.

There has been a continuing string of major security breaches. One of the most alarming breaches was the theft of millions of credit card records from TJX, which owns retailers such as T.J. Maxx, Marshalls, and HomeGoods [Greenemeier 2007]. And the breaches have coincided with a steep rise in identity theft. A Gartner study noted that 15 million Americans were victims of identity theft during the 12 months ending in August 2006, and that the average identity theft fraud loss more than doubled from $1,408 in 2005 to $3,257 in 2006 [Keizer 2007]. In response, the Federal Trade Commission and other federal regulatory agencies are beginning to clamp down hard. Federal banking regulators are now conducting information security audits of small and mid-sized banks that used to escape with a lighter review. And the FTC conducted a number of enforcement actions under the Safeguards Rule of the Gramm-Leach-Bliley Act.

---

[2] In the information security industry it is assumed that there is no such thing as absolute security. Therefore the goal is to mitigate rather than eliminate a risk. For example, there is no way to guarantee that a networked computer cannot be hacked into without disconnecting it from the network.

[3] A *vulnerability* is security flaw that could potentially lead to a breach, e.g. an unlocked door to the computer room or a weak password. A *threat* is an agent that could exploit a vulnerability. *Risk* is the likelihood that an agent will exploit a vulnerability. For example, in a small town with no crime leaving the door to your home unlocked is still a vulnerability, but it may be a low risk since there is a lack of criminal threats.

The leading payment card companies changed their policies so that large companies that fail audits based on the PCI Data Security Standard will be charged a higher rate for transactions. This change could cost retailers tens of millions a year.

And in December of 2006, the courts changed the Federal Rules of Criminal Procedure (FRCP). Companies are now required to promptly submit ESI evidence in a suit or face stiff penalties, including having the case being decided in favor of the other party. In addition, the FRCP requires that companies show proof of security controls to ensure the integrity of the evidence.

What do these three drivers have to do with outsourcing and in particular offshoring? First, Federal regulators and the courts have taken the position that outsourcing of a business process does not absolve the procuring company of responsibility for the confidentiality and integrity of the data processed. Sarbanes Oxley, PCI, and other audits must examine the storage and processing of appropriate data wherever it is.

OFFSHORING AND THE INTERNATIONALIZATION OF RISK

Risk can be defined as the likelihood of potential harm being realized. For information security risk, the likelihood is a function of vulnerabilities or weaknesses in computer systems and processes and the threat-actors who can maliciously exploit the vulnerabilities. By identifying risks and exposures (R&E), we are not suggesting a company avoid offshoring. Risk avoidance is only one way of managing risk. The more common approach is risk management. To this end we will examine some high-level strategies for mitigating the risks and exposures that we identify.

II. EXACERBATION OF VULNERABILITIES

Almost every modern organization relies on information processing systems to operate. These systems include the computers and network devices that form the infrastructure but also the information processing applications and the people and processes that operate the whole system. Therefore, a holistic examination of system vulnerabilities must include technology, infrastructure, business applications, people, and processes.

The IT technologies in place and their specific uses within the procuring and providing organizations are the immediate primary sources of additional vulnerabilities, here defined to be weaknesses that can be exploited. It is now well established that hardware and especially software for large, complex, distributed, and networked systems suffer from extensive vulnerabilities. New vulnerabilities are continuously discovered, fixed by the manufacturer, and then these patches to device software must be implemented. Vulnerability and patch management are extremely difficult problems within one organization. Outsourcing further complicates the picture by integrating trusted computer networks with unknown levels of patches. In particular, offshoring further exacerbates the problem by lengthening supply chains and lines of communication over unknown networks and thus creating additional exposure.

The same problem exists for people and processes as well as technology. Take, for example, change management of a business application. Any change introduces the risk of system failure or compromise. Organizations have introduced strict change control procedures and software to manage this risk. Then they have trained their programmers and operators on these change control systems, which include controls during the coding and testing phases of development. When software development is outsourced, the change management system is radically altered. Vulnerabilities could be introduced by different coding or testing methods.

Offshoring arrangements require two or more organizations to work more or less closely with each other, thereby necessitating greater trust, dependency, and intimacy than would otherwise be the case. These arrangements require that both people and systems get mixed across the organizations. This mixing exposes one to the other, and perhaps to unfriendly third parties, and likely makes each system and organization less secure than it was when they were separated. In offshoring, the possible consequences of these exposures may be made more severe because of

cultural, language, ethical, legal, and other differences that may not exist in purely domestic outsourcing.

A sample of organizational mixing problems includes creating a new group of "insiders," clashing security strategies and cultures, drastically diminished ability to know about and respond to security breaches, and exposure to intellectual property theft. To some extent, these problems may be mitigated by subsidiary arrangements, i.e., where the procuring company owns the offshore provider, as is the case with several major multinationals like GE, Target, IBM or Microsoft.

Organizational mixing makes the problem of enterprise risk assessment and mitigation even more difficult than it was without any offshoring arrangements. But "more difficult" does not have to translate into "impossible." This subject is treated more extensively in "Offshoring Risks and Exposures" [Goodman et al. 2006] and will receive little additional attention here.

III. INTERNATIONALIZATION OF THREATS

The globalization of IT processing itself creates additional threats. Instead of the home network being exposed to external threats or threat-actors that exist on the global network, offshoring opens an organization's systems by conducting internal processes over the global network. To some extent, these threats are a factor of the WWW, but offshore outsourcing magnifies the problem by incorporating people who are subject to different legal jurisdictions and different and often competing nation states and political systems.

System vulnerabilities discussed in the previous section do not become operative without threat-actors. Here we distinguish between threat-actors with malicious intent and everything else. The latter includes business misunderstanding, incompetence, acts of God, and so on. Consequences might include defective products and services, failure to raise promised capital or capabilities, failure to meet specified contract obligations, and other similar consequences. Domestically, these are typically business risks that may get settled in civil law. They exist in greater variety in offshoring arrangements for reasons already alluded to [Deloitte 2005]. They should be anticipated, not taken lightly, and the procuring organization might well be advised to consider crafting business "pre-nuptial agreements" to protect themselves. [Hoffman 2006] At this point, we will be concerned only with R&E that involves malicious actors trying to exploit vulnerabilities, but we note that nonmalicious accidents or Mother Nature may also exploit vulnerabilities with similar consequences.

A broad potential risk, one that could be greatly exacerbated by offshoring, is that the providing organization, or at least significant parts of its ownership or management, could be compromised and used by organized crime or foreign governments to the detriment of the procuring country. (About half of the remainder of this section, including all specific examples not otherwise cited, is taken from a more extensive discussion in [Goodman et al. 2006]). This could serve as a means for, among other things, attacking critical national infrastructures and other targets of national and homeland security concern. There are instances of businesses becoming beholden to organized crime interests or fronts for government agencies in nations around the world. Offshoring provides potential for new reach and threats in this regard.

It is not difficult to imagine the providing organization gaining control over data assets and management (e.g., databases, network operations) that would give it a powerful platform, perhaps as managers of a significant part of a critical national infrastructure, to engage in such activities as:

- Unauthorized data mining, particularly across the data of multiple customers
- Intelligence and counterintelligence operations
- Planting focused malware
- Attack probing and planning

- Control of network operations
- Fronting for extensive criminal activities, e.g., money laundering
- Attack(s) preparation over an extended period against national security and emergency preparedness and response organizations and assets

Given several imaginable positions as a provider, one might be set up to continue such activities for a long period of time without detection, enabling it to do a great deal of damage in a relatively protected way. Attacks and other operations, such as those listed in the previous paragraph, could harm critical national infrastructure, such as transportation, power, and financial systems. Although such devastating attacks have not yet been realized, accidents and other considerations indicate that they are feasible and that greater protection would be prudent. We note that the variety and extent of malicious activity in cyberspace was underestimated in the past and, unfortunately, many of the forecasted risks were realized to a greater extent than almost anyone thought likely.

There are a number of countries, including but not limited to Russia, parts of Eastern Europe, and China, where there is a lack of a well-established rule of law that effectively protects individuals or commercial enterprises, and it may be difficult or impossible for provider organizations to resist overtures by organized crime or government security agencies. They have very little physical or legal means to defend themselves against such overtures.

IV. TARGETS OF RISKS AND EXPOSURES (R&E)

We have three subcategories of the targets or victims of R&E: the business partners, i.e., both the procuring and providing organizations; individuals (primarily the customers or clients of the procuring organizations); and national security, the latter being interpreted broadly to include economic capabilities.

Business partners, the service provider (e.g., an offshore development center or ODC) and service procuring organization (e.g., a life insurance company that contracted with the ODC for applications software development) face R&E from an offshoring relationship. Procuring businesses increase their regulatory risk because organizations such as the ODC have repeatedly stated that a company can outsource a function but not the regulatory responsibility. As explained earlier, the increased vulnerabilities and threats magnify the normal R&E that businesses face, such as loss of intellectual property, damage to brand or reputation, stock price drops in case of a reported security breach, or legal liabilities.

The increased risks cut both ways. Poor controls at a procuring company can undercut the provider's security. Take, for example, the following case, based on an actual experience, of a life insurance company and its software provider which operated an ODC in India. The two companies established a trusted network. Due to regulatory requirements, the procuring company forced the ODC to implement strong encryption and perimeter controls. Based on these security controls, the ODC was able to obtain a number of U.S. and European banking clients. However, a disgruntled employee at the insurance company was able to penetrate the ODC's network and collect bank account information from the ODC's banking clients. When this situation was discovered, the ODC lost its banking clients [Ramer 2003].

In today's stiff regulatory environment, compliance risk is one of the leading risks a company faces. With offshoring, complying with regulatory audits becomes an expensive proposition. With the new court rules, efficient retrieval of offshored records is a requirement for legal success. A penalty from a regulatory agency often causes far greater financial damage then the actual dollar value of the fine, and these have been growing larger. Many companies rely on their reputation for certain expertise or for their caution with their customers' funds and financial information. A regulatory action can become a public relations disaster, leading to loss of customer and investor confidence. In discussions with security professionals from around the country, cost estimates of

reported breaches run from $1 to 2 million for each security breach reported in the news media [Westby and Worstell 2007].

Individuals may have a great deal of exposure and attendant risk with offshoring. Much of it also exists domestically, but offshoring presents new or exacerbated forms. We have lots to lose: privacy, property, and exposure to other forms of malicious activity or crime (e.g., being added to more phishing lists, damaged reputation, even possible physical harm). As businesses are increasingly being made responsible for the breach of individuals' data, these R&E are as much a concern of outsourcing procurers as they are of the individual consumer.

So far, loss of IT jobs to offshoring has gotten most of the attention [e.g., ACM JMTF 2006]. The complexities of the issues, and difficulties in obtaining strongly convincing data one way or another, resulted for the most part in those with actual control over the jobs, namely companies, more or less continuing to operate in their own interests. Within the U.S. in the last two years alone, there was a hemorrhaging of exposure of the personal data of tens of millions of Americans. Privacy Rights Clearing House maintains a running list since February 15, 2005 [PRCH 2006]. They report almost 90 million records compromised, with 40 occurrences in June 2006 alone. Data losses pile up from negligence, crime, and accidents. Very serious and high profile events, e.g., ChoicePoint or the Veterans Administration [Vijayan 2006a; Gross and Vijayan 2006], make big news splashes, although it is not clear if much help for the victims or much in the way of additional protection or prevention has come of all of the increased visibility. Is this something new? Is it unique to the United States? We suspect that part of why we are seeing reports of so many breaches in the U.S. is because quite a few states passed laws requiring them to be reported [Vijayan 2006b].

There is no way that this can be unique to the United States, as evidenced by a series of reports regarding identity theft in India [Bakshi 2005; Brown 2006; Harvey 2005: and McKenzie 2007]. Another example is the circa 2003 case of a Pakistani employee who threatened to post U.S. patients' medical data on the Web if claimed back pay was not forthcoming [Weinstein 2004]. No doubt total losses and loss potential are less abroad simply because far fewer organizations hold far less sensitive data on people in America. But risks may be greater for the amount of data held that, at this point, can only be described qualitatively. Foreign providing companies and their governments have few incentives or capabilities to detect and report breaches. Differences in legal protections of data and privacy are such that most developing countries have weaker laws in this regard than the United States and perhaps even less for victims who are not their own citizens. In some ways, this is a pitiful statement since protections in the U.S. are rather weak, particularly as compared with the European Union, which does far less offshoring of their citizens' sensitive data and is even concerned about offshoring such data to the U.S. The law enforcement histories of most if not all providing countries for vigorously and successfully pursuing such cases, or white-collar crime more generally, leaves much to be desired. Their histories with regard to protecting intellectual property rights and software as well as other forms of IP piracy, are not encouraging. One would expect that the risks are increased just by spreading the data across multiple jurisdictions, with the greatest risk in the weakest legal environments. And what is to stop a providing firm from passing data on to another providing firm in yet another jurisdiction, perhaps via its own offshoring subcontract and without the original procuring company's knowledge? Given the possibilities through the use of global IT, identity theft may be more safely exploited by criminals in less developed countries than in the home countries of the victims.

As stated previously, all of these risks to individuals can become a significant financial and reputation risk to businesses who are the custodians of the personal data of individuals.

V. PRUDENCE AND MITIGATION

What can be done to mitigate such risks? So far, economic and market incentives do not seem to afford much protection while legal and regulatory pressures are having an impact on improved security practices. Still improved protection does not seem to be keeping up with the increasing

numbers of violations and prospective victims. Smart criminals may not even victimize the latter until some time long after the data is acquired, making it more difficult to attribute injury to a specific data breach. “Thieves are stealing far more identities than they need,” Bruce Schneier, cryptologist and CTO of BT Counterpane says, “Criminals are not stealing identity information in ones and twos; they're stealing identity information in blocks of hundreds of thousands and even millions. If a criminal ring wants a dozen identities for some fraud scam, and they steal a database with 500,000 identities, then—as a percentage—almost none of those identities will ever be the victims of fraud” [Schneier, 2005]. However, if most of us want to gamble on percentages, we would prefer that the outcome is a jackpot rather than becoming a fraud victim. And if we are increasing the number of threat actors by exporting data around the world, we are increasing our chances for loss. So the point is to develop risk mitigation strategies.

RISK MITIGATION STRATEGIES FOR BUSINESS PARTNERS

Offshoring can be an effective business strategy, but there are potential risks and exposures that may affect business, individuals, and national capabilities and security. A serious and extensive risk assessment reflects basic and necessary prudence and should be part of any process to determine the value of offshoring arrangements. Given such an assessment, and the initiation of an offshoring agreement, effective mitigation strategies should include [Goodman et al. 2006]:

- *Security due diligence.* The key factor is a thorough security assessment including reviews of both technical and process controls. Evidence of a SAS 70[4] or a security certification, while good information, cannot be a replacement for a close look at how the procuring company assets could be compromised. The review must examine mechanisms for protecting both customer data and intellectual property, as legal liability for this rests with the procurer.
- *Business and national security due diligence.* Does the provider have the technical and security skills needed? Does it conduct effective background checks? Is it financially stable? What relationships does it have with other companies and governments? Is the information they are processing or might have access to through shared networks have national security implications? This is not only a concern for the defense industry or military but is important for all companies who are a part of critical infrastructure.
- *Active risk management*. This includes the development, implementation, and maintenance of an ongoing security program between the procurer and provider. The program should include appropriate forms of monitoring, regular reporting of security metrics, incident response and reporting, business continuity, disaster recovery management. It should include regular security audits performed by security professionals who are independent of the provider. Such an active risk management program for offshoring should have a policy and guidelines that include the following:
    - Providers must 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, and a breach should be grounds for redress and possible termination. However, contracts must be structured to encourage appropriate incident response in order to avoid cover-ups.

[4] SAS 70 or Statement on Auditing Standards No. 70: Service Organizations defines the standards used by an auditor to examine the internal controls for a service provider. SAS 70 reports examine the controls put in place by the management of an organization. A SAS 70 can also report on the effectiveness of such controls. However, the reports must be read carefully to verify that controls the procuring company cares about are in place.

- Providers must be certified for adherence to prescribed standards such as ISO 27001 (previously BS 7799) or the Financial Institutions Shared Assessment Program (http://www.bitsinfo.org/FISAP/index.php). However, certification must be an entry requirement and not a free pass. An audit or certification is always a snapshot of a point in time, and a provider's security state can change quickly.
- Procuring organizations must conduct regular security assessments that closely examine the storage, processing, and transmission of their sensitive data. These assessments must follow the path of data and transactions and examine specific controls and not rely on general controls.
- Providers must be prohibited from indirect third-party outsourcing arrangements without explicit approval from the procurer.
- Databases must be encrypted at rest and records encrypted in transit. 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.

Along similar lines, we might also point to the recommendations on privacy by the U.S. Public Policy Committee of the Association for Computing Machinery [USACM 2006]. By implementing strict privacy controls in their global sourcing processes, companies can protect themselves and their stakeholders.

VI. CONCLUSION

While offshoring is a very political issue we again remind the reader that the purpose of this paper is *not* to reject what is often a very effective play in the strategic game of business. However, it is essential that anyone using this play carefully examine the risks involved and to address them. We encourage IT practitioners to examine the extensive sources of information on this subject.[5] To conclude, we offer you the subtitle of this paper as three words of advice, *prudence before playing*.

LIST OF ACRONYMS

ACM	Association for Computing Machinery
ACM JMTF	ACM Job Migration Task Force
ASD (NII)	Assistant Secretary of Defense (Networks and Information Integration)
BS	British Standard
CTO	Chief Technology Officer

[5] A volume on a broad range of subject matter concerned with managing risks at the enterprise level, written primarily by MIS academics, will be published in early 2008 [Baskerville et al. 2008]. Among the chapters is one that surveys the rapidly growing set of international organizations concerned with cyber security. [Nain et al. 2008] Of particular note is a series of four (possibly to become five in 2009) volumes dealing explicitly with the international dimensions of cyber crime, cyber security more generally, privacy, and enterprise security management [Westby et al. 2003; 2004a; 2004b; 2005]. These books were produced by expert groups of engineers, lawyers, and business people under the direction of Jody R. Westby. The fifth volume, one that will be explicitly devoted to managing the risks of outsourcing, is currently in preparation [Westby 2009].

FRCP	Federal Rules of Criminal Procedure
FTC	Federal Trade Commission
IP	Intellectual Property
ISO	International Standards Organization
IT	Information Technology
NSA	National Security Agency
ODC	Offshore Development Center
PCI	Payment Card Industry
PRCH	Privacy Rights Clearing House
R&E	Risks and Exposures
SAS 70	Statement on Auditing Standards No. 70: Service Organizations
WWW	World Wide Web

REFERENCES

EDITOR'S NOTE: The following reference list contains the address of World Wide Web pages. Readers, who have the ability to access the Web directly from their computer or are reading the paper on the Web, can gain direct access to these references. Readers are warned, however, that:

1. These links existed as of the date of acceptance but are not guaranteed to be working thereafter.

2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.

3. The authors of the Web pages, not CAIS, are responsible for the accuracy of their content.

4. The authors of this article, not CAIS, is responsible for the accuracy of the URL and version information.

ACM Job Migration Task Force (ACM JMTF). (2006). *Globalization and Offshoring of Software*, Association for Computing Machinery, 2006, 286 pages, http://www.acm.org/globalizationreport .

Baskerville, R., S. Goodman, and D. Straub (eds.) (2008). *Information Security Policies, Processes and Practices*, M. E. Sharpe, New York, to appear spring 2008.

Bakshi, M. (2005). "A Shattered Image," *The Hindu Business Line*, http://www.thehindubusinessline.com/ew/2005/04/18/stories/2005041800180300.htm (April 18, 2005).

Beaumont, R., et al. (2005). *Protecting the United States Telecommunications Infrastructure: The Way Forward,* Final Report, USTI Security Study for the Assistant Secretary of Defense (NII)

and the NSA, Applied Physics Laboratory, Johns Hopkins University, Laurel, MD, Spring 2005, approx. 300 pages.

Brown, B. (2006). "FBI Special Agent Recounts Outsourcing Horror Story," *NetworkWorld.com*, http://www.networkworld.com/news2006/051606-fbi-outsourcing-horror.html (May 16, 2006).

Deloitte Consulting LLP. (2005). *Calling a Change in the Outsourcing Market*, April 2005.

Friedman, T. (2005). *The World Is Flat*, New York: Farrar, Strauss, Giroux.

Harvey, O. (2005). "*Your Life for Sale*," *The Sun*, London, May 28, 2005.

Hoffman, T. (2006). "'Prenuptials' for Offshoring: IT Customers Who Overlook Rights and Remedies In Outsourcing Deals May Live to Regret It," *Computerworld*, January 23, 2006, 34.

Federal Trade Commission (FTC). (2006). http://www.ftc.gov/opa/2006/01/choicepoint.shtm .

Goodman, S. et al. (2006). "Chapter 6. Offshoring: Risks and Exposures," in ACM Job Migration Task Force, *Globalization and Offshoring of Software*.

Greenemeier, L. (2007). "TJX Stored Customer Data, Violated Visa Payment Rules," *Information Week*, January, 29, 2007.

Gross, G. and J. Vijayan. (2006). "Huge Data Breach Puts VA's IT Policies under a Microscope," *Computerworld*, May 29, 2006, 1, 44.

Keizer, G. (2007). "ID Theft Forecast: Gloomy Today, Worse Tomorrow," *Computerworld*, March 7, 2007.

McKenzie, S. (2007). "*AFP: India Key to ID Theft War,"* http://www.zdnet.com.au/news/security/soa/AFP-India-key-to-ID-theft-wars/0,130061744,339273923,00.htm?r=1 .

Nain, D., N. Donaghy, and S. Goodman. (2008). "The International Landscape of Cyber Security," Chapter 9 in [Baskerville et al. 2008].

Privacy Rights Clearing House (PRCH). (2006). "Chronological List of Data Breaches," http://www.privacyrights.org/ar/ChronDataBreaches.htm .

Ramer, R. (2003). Personal communications from client interviews at an ODC in Mumbai, May 2003.

Schneier, B. (2005). "Most Stolen Identities Never Used," December 12, 2005 http://www.schneier.com/blog/archives/2005/12/most_stolen_ide.html .

USACM. (2006). Policy Recommendations on Privacy, June 2006 http://www.acm.org/usacm/Issues/Privacy.

Vijayan, J. (2006a). "FTC Makes a Point with ChoicePoint Penalties: Hits Firm with Largest Civil Fine Ever In Data Breach Case," *Computerworld*, January 30, 2006, 1, 54.

Vijayan, J. (2006b). "Debate Continues on Breach Notification," *Computerworld*, March 6, 2006, 8.

Weinstein, L. (2004). "Outsourced and Out of Control," *Communications of the ACM*, Vol. 47, No. 2, February 2004, 120.

Westby, J. (ed.). (2003). *International Guide to Combating Cybercrime*, Privacy and Computer Crime Committee, Section of Science and Technology Law, American Bar Association, ABA

Publishing, Chicago IL, February 2003. http://abastore.abanet.org/abastore/index.cfm?section=main&fm=Product.AddToCart&pid=5450030 .

Westby, J. (ed.). (2004a). *International Guide to Cyber Security,* Privacy and Computer Crime Committee, Section of Science and Technology Law, American Bar Association, ABA Publishing, Chicago IL, July 2004. http://abastore.abanet.org/abastore/index.cfm?section=main&fm=Product.AddToCart&pid=5450036 .

[Westby, J. (ed.). (2004b). *International Guide to Privacy*, Privacy and Computer Crime Committee, Section of Science and Technology Law, American Bar Association, ABA Publishing, Chicago IL, 2004. http://abastore.abanet.org/abastore/index.cfm?section=main&fm=Product.AddToCart&pid=5450037 .

Westby, J. (ed.). (2005). *Roadmap to an Enterprise Security Program*, Privacy and Computer Crime Committee, Section of Science and Technology Law, American Bar Association, ABA Publishing, Chicago IL, January 2005 http://abastore.abanet.org/abastore/index.cfm?section=main&fm=Product.AddToCart&pid=5450039 .

Westby, J. and K. Worstell. (2007). "*Litigation AND Records Management,"* Forum presentation at BSI Americas Inc., ISO 27001 Virtual Conference;, notes from post-presentation discussions, April 16, 2007. http://www.bsiamericas.com/InformationSecurity/VirtualConference/index.xalter

Westby, J. (ed.). (2009). *Outsourcing Risk Management,* Privacy and Computer Crime Committee, Section of Science and Technology Law, American Bar Association, ABA Publishing, Chicago IL, to appear 2009.

APPENDIX I

LAWS AND REGULATIONS

Key laws and regulations include the following:

International Laws and Regulations:

1. **EU Data Protection Directive:** European Union Directive 2006/24/EC of March 15, 2006, on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, *available at* http://eurocrim.jura.uni-tuebingen.de/cms/en/doc/745.pdf.

2. **European Union – Security Provisions in Country Implementations of Data Protection Directive** See http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm

3. **The Canadian Personal Information Protection and Electronic Documents Act** http://www.privcom.gc.ca/legislation/02_06_01_e.asp

4. **The Japanese Personal Information Protection Law** http://www.ictparliament.org/CDTunisi/ict_compendium/paesi/giappone/GIA11.pdf

5. **National Omnibus Laws** – For a list of data privacy laws around the world please see http://www.privacyexchange.org/legal/nat/omni/nol.html

Key US Federal Regulations include:

1. **GLB Act**: Gramm-Leach-Bliley Act, Public L. 106-102, Sections 501 and 505(b),

2. 15 U.S.C. Sections 6801, 6805.

3. **Homeland Security Act of 2002**: 44 U.S.C. Section 3532(b) (1).

4. **HIPAA**: Health Insurance Portability and Accountability Act, 42 U.S.C. 1320d-2

5. And 1320d-4.

6. **Sarbanes-Oxley Act**: Pub. L. 107-204, Sections 302 and 404, 15 U.S.C. Sections 7241 and 7262.

7. **Federal Rules of Evidence 901(a):** *see* American Express v. Vinhnee, 2005 Bank. LEXIS 2602 (9th Cir. Bk. App. Panel, 2005).

8. **FDA Regulations:** 21 C.F.R. Part 11.

9. **FFIEC Guidance:** Authentication in an Internet Banking Environment, October 12, 2005, available at http://www.ffiec.gov/pdf/authentication_guidance.pdf. See also "Frequently Asked Questions on FFIEC Guidance on Authentication in an Internet Banking Environment," August 8, 2006 at p. 5, available at http://www.ncua.gov/letters/2006/CU/06-CU-13_encl.pdf

10. **GLB Security Regulations**: Interagency Guidelines Establishing Standards for Safeguarding Consumer Information (to implement §§ 501 and 505(b) of the Gramm-Leach-Bliley Act), 12 C.F.R. Part 30, Appendix B (OCC), 12 C.F.R. Part 208, Appendix D (Federal Reserve System), 12 C.F.R. Part 364, Appendix B (FDIC), and 12 C.F.R. Part 568 (Office of Thrift Supervision).

11. **GLB Security Regulations (FTC)**: FTC Safeguards Rule (to implement §§ 501 and 505(b) of the Gramm-Leach-Bliley Act), 16 C.F.R. Part 314 (FTC).

12. **HIPAA Security Regulations**: Final HIPAA Security Regulations, 45 C.F.R. Part 164.

ABOUT THE AUTHORS

Seymour E. Goodman is professor of International Affairs and Computing, jointly with the Sam Nunn School of International Affairs and the College of Computing at Georgia Tech. He co-chaired the policy group of the ASD (NII)/NSA study [Beaumont et al. 2005], and co-chaired the Risks and Exposures Subcommittee of the ACM JMTF study [ACM JMTF 2006]. He also serves as International Perspectives contributing editor of the *Communications of the ACM*.

Rob Ramer is a senior consultant in Risk Management for Aeritae Consulting Group in St. Paul, Minneapolis. He has more than 25 years of IT experience and works with clients in financial services, retail and healthcare to assess and manage information security risks. Prior to joining Aeritae, Mr. Ramer built an international consulting company that provided risk management for companies engaged in global sourcing. He served on the R&E subcommittee of the ACM JMTF study. Mr. Ramer can be contacted at rramer@aeritae.com.

Communications of the Association for Information Systems

ISSN: 1529-3181