

Chapter 6: Offshoring: Risks And Exposures

6.1. Introduction

In June 2005, the news media reported that some 40,000,000 credit card accounts at CardSystems of Phoenix, AZ, had been compromised by an infiltration. "The intruder gained access to names, account numbers, and verification codes critical for committing fraud. A MasterCard spokeswoman said the company was aware of information being removed from the CardSystems database on about 68,000 MasterCard accounts, putting those cardholders at a higher level of risk." Pacel and Sidel (2005). (Also see Computer Security Institute (2005) for a more detailed analysis.)

By mid-year 2005, there was a wave of security breaches and lapses that calls into question the security of electronic financial and commercial transactions. Australian and British press reports identified a black market in India for personal information gleaned from financial offshore processing centers. Consumer complaints led to the arrest of employees at a center processing Citicorp data in Pune, India. Officials at the UK National Infrastructure Security Co-ordination Centre revealed that "hackers, often linked to the Far East, were attacking vital UK government and corporate computer networks, seeking commercially and economically valuable information. The revelations show that computer viruses released via the Internet increasingly are being used to garner confidential information, ranging from personal banking details of consumers to industrial espionage." US investigators concurred, noting that US institutions have suffered similar attacks for "at least a few years . . . mostly from computers in China." (Europe WorldWatch 2005).

Some people suggest that these are simply cases reflecting the true risks of the digital age with the implication that outsourcing and offshoring are minor additions to the mix. This chapter argues, instead, that offshoring exacerbates existing risk and introduces new types of risk by opening more opportunities for incursion, accident, or exposure; and it may greatly complicate jurisdictional issues. This concern does not lead to a wholesale condemnation and rejection of offshoring but rather to the recognition of the inadequate attention so far paid to these risks. We hope that the issues raised here will lead to greater awareness and thus to more prudently cautious, thoughtful, and effective practices in preventing and dealing with these risks.

Offshoring decisions are largely business decisions and are often little influenced by consideration of long-term risks, political consequences, or social impact. Many corporations would argue, not unreasonably, that they do consider some long-term risks such as to reputations, and they should and do consider risks that directly affect their business operations, but that it is not their job to consider the social impact or possible political or larger national security consequences of their offshoring decisions. But somebody, most obviously government, needs to consider these impacts and consequences.

So it follows that the risks examined in this chapter come in three categories. There are risks for companies that engage in offshoring. There are risks to individuals who are innocent and often helpless victims of the kinds of security compromises just described. Much of this is in the form of privacy violations or identity theft. Finally, there are risks to the defense and economic security of nations.

Given the subject matter and the rapidly growing number of security and privacy violations experienced in cyberspace, this chapter is by its nature inclined to sound alarms and encourage caution. Risks in cyberspace often have to be presented as possible or plausible scenarios, independent of the extent to which they have occurred so far. It is generally impossible to find accurate and comprehensive statistics on attacks and their results, although it is clear that there is a lot going on, and many experts agree that the problem is growing. Given the paucity of evidence, risks are discussed here in terms of the relatively few examples that become public. Those who do not want to deal with these risks for whatever reasons typically argue that the risks should not be taken seriously until there is compelling evidence that the risk is real. The variety and extent of malicious activity in cyberspace has often been underestimated in the past. Unfortunately, many of the forecasted risks have come true. Spamming and phishing, for example, now make up a majority of the traffic on the Internet. One dangerous risk, the use of the cyber infrastructure to launch devastating attacks against national and international physical infrastructure, such as transportation or electric power systems, has not yet been realized. But this does not mean that vigilance is not needed.

Few of the risks to be considered here are unique to offshoring. But, depending on various factors such as the laws in the countries involved, the risks may be significantly amplified by aspects unique to the international nature of the attacks. For example, they may take the form of exposing potential victims to a larger population of possible criminals who are not likely to be held very accountable for the harm done to citizens of another country, or that parts of the lengthened and expanded channels of the operation are under little or no effective control by either the procuring or providing company or their parent countries.

Most of the information used in this chapter comes from US sources. Many experts believe that the risk of cyber attacks is significantly under-detected and under-reported in the United States. These problems of detecting and reporting appear to be far worse in the rest of the world. The reasons for this are not hard to understand and probably reflect that their citizens are not often victims of cyber-crimes, that it is difficult to find and train (and pay) capable people to collect such information and carry out investigations, and that almost any other form of crime probably has higher priority for the limited law enforcement resources available in many populous, poor countries. We were also limited by an inability to obtain and deal with locally published, non-English source material. Thus much of our coverage is about attacks on companies and individuals in the United States. There is some justification for this coverage. In particular, the United States offshores more work than any other country. But it should be clear that individuals and firms around the world, not only in the United States, are vulnerable to cyber attacks, and attackers can just as readily be located in the United States as in some other country. Similarly, all governments that use information technology in their critical infrastructures must face the possibility that this technology can place their national systems and national security at risk.

6.2. Vulnerabilities: Data and Network Security and Beyond

A basic principle of security is that, the longer the supply chain and lines of communication, the more opportunity there is to attack them. The adage that a chain is only as strong as its weakest link often applies as the complexity of securing computer networks is increased by routing through multiple providers. The inherent complexities in international data communications are further compounded by jurisdictional issues regarding regulation and legal responsibility.

Commercial or organizational alliances in the modern world rely on integrating the computer systems of their allies or partners to some degree. Manufacturing companies integrate suppliers into their supply chain systems. The transportation, warehousing, and

sales systems of the distributor are linked with those of the manufacturer. These linkages may open up additional vulnerabilities in both systems. Martin Libicki, in a forthcoming book, identifies these as *systems intimacy* issues. He states, "Close relationships in cyberspace, as in real life, can make either partner more vulnerable. A relationship, solely by virtue of the value it brings to its partners, may be attacked by the competitors of both. Third parties can exploit weaknesses in one to get at the other(s)." (Libicki 2006).

Outsourcing in general involves an even greater degree of intimacy because entire business processes may be entrusted to the partner, and this often entails a greater degree of system integration. Software development outsourcing is perhaps the most intimate relationship of all because it constitutes a continuing impact and often access to the procurer's system long after the initial work is complete. Offshoring is an extension of this intimacy across and through multiple national and international data networks under the jurisdiction of multiple parties who may or may not be hostile to the commercial and national interests of both the providing and procuring parties.

Offshoring risks can be categorized into systems intimacy risks and outsourcing risks. They include the following types of vulnerabilities.

Systems Intimacy Risk

- *Data communications vulnerabilities.* Communication channels include multiple service providers of various nationalities. The channels are well beyond the control of either the procuring company or the provider. Usually they are private leased lines, which means that a certain capacity is dedicated to the buyer, but there is no guarantee that the line is indeed private in the sense that others are not listening. These channels are often not encrypted, or encryption is entrusted to the control of the communications service provider. If encryption is provided, it may not include end-to-end transaction encryption, thus leaving data exposed at certain points along the communication path.
- *Loss of control over network perimeters.* A link with an Offshore Development Center (ODC) opens a broadband communications channel directly into the procuring company that could then become dependent on the ODC for user authentication. In one situation, security at an ODC was so notoriously lax that its internal web servers were listed on hacker websites as useful hosts from which to mount denial-of-service attacks. Users at that ODC were also vulnerable to attackers hijacking their sessions to penetrate the ODC's client network (Ramer 2004).
- *Increased network complexity.* Network configuration management in an expanding and ever-changing environment challenges most IT security capabilities. Understanding the flow of critical transactions becomes almost impossible when an ODC is thrown into the mix. If the development center produces software for multiple procuring companies and does not effectively isolate the networks dedicated to each procurer, configuration management approaches the impossible. Validating the security of trusted partners in a multi-client, multi-vendor, mixed environment is a similarly difficult task.
- *Clashing security strategies.* The procuring company and the ODC may take varying approaches regarding known vulnerabilities, intrusion detection, perimeter defense, or other security issues. These discrepancies could create vulnerabilities for both the procuring company and the offshore provider. For example, the procuring company could rely on very strict access control limiting users to only those files that they need. Let us assume that the providing company relies on very strict two-factor authentication but, once the resource proves he (or she) is an authorized user, he is allowed relatively free range

within the system. This situation could present a threat to the provider. A disgruntled employee of the procuring company could access the provider's system and plant malicious code. Or the malcontent employee, such as someone about to lose his job to offshoring, could use the provider's system to launch an attack on the procurer and thus create problems for the relationship that he blames for the loss of his job.

- *Gaps in personnel security.* High turnover in rapidly growing IT industries, such as is occurring in India and the Philippines, leads to administrative stress. Even in India, perhaps one of the better prepared of the offshoring destination countries when it comes to security, many companies still have weak personnel policies (NASSCOM-Evalueserve 2004). There is often a lack of personnel security infrastructure such as searchable credit records or criminal databases (Bhat 2002).
- *Drastically diminished ability to know about and respond to security breaches.* Without strict and enforceable contract provisions, an offshore provider has little incentive to notify its clients that they have had a security breach. Even if it does, the jurisdictional and organizational issues make effective incident response extremely difficult.

Outsourcing Risks

- *Loss of control over security of software development.* When a company has its software produced in an ODC, it defines the performance requirements but relinquishes day-to-day control over software development to the overseas vendor. Clients spend hundreds of thousands of dollars testing software applications to ensure that they meet requirements. Rarely, however, do security departments inspect the code for trojans (malicious software disguised as legitimate software), viruses, or other forms of malicious code that perform threatening or illicit activities. Virus scanners identify and sanitize widely known viruses, but they will not find code specifically designed to sabotage or provide particular information. Viruses are increasingly targeted at obtaining commercially valuable information, ranging from consumer banking details to industrial espionage (Symantec 2005). The risk of embedded malware is enhanced by offshoring due to factors that may include less personal loyalty from offshore contractors than from employees or onsite contractors, increased vulnerability of the supply line, and increased potential for intervention by hostile covert groups such as government intelligence or organized crime. Even when inspections are possible, it may be difficult to find carefully crafted malware hidden in large volumes of code.
- *Loss of control of business processes.* By outsourcing to any location, a procuring company loses a certain amount of control of the business processes that are outsourced. There is a corresponding transfer of control over the information necessary to perform the process. This loss of control may be exacerbated by communications problems, cultural issues, and lines of communication that are more vulnerable when the work is offshored. Depending on the nature and sensitivity of the work involved (e.g., R&D or network management), this information may be of strategic interest to competing nations and their industries.

What seems particularly lacking within many procuring companies is an overall line of authority and responsibility for primary data records as they pass through one, two, or more offshore companies that perform operational tasks. Offshoring decisions are made based on data management strategies and costs, but responsibility for security is often not

considered. This kind of hands-off management responsibility cannot be presumed to work in the best interests of anyone concerned with risk attenuation.

The magnitude of risk is summarized in a Symantec Corporation Internet Security Threat Report analysis covering the period from July to December 2004. This analysis is based on the top 50 malware samples from output of 20,000 sensors monitoring 180 corporations worldwide (Symantec 2004). One alarming finding was that there was a rise in threats designed to compromise confidential information. Malicious code, including the proliferation of trojans and bots (short for robot, a program that automatically searches the Internet for data), created to expose confidential information or compromise systems, represented 54% of the samples. Remotely controlled trojans and bots constituted 33% of the top 50 malware attacks, one of the most serious threats from and to offshoring. 1,403 new vulnerabilities (more than 54 new vulnerabilities per week) were detected. Of these, 97% were considered moderately or highly severe, meaning that successful exploitation of the vulnerability could result in a partial or complete compromise of the targeted system. Malware, allowing attackers to circumvent traditional perimeter security measures (e.g., firewalls), accounted for 48% of all vulnerabilities.

Offshoring is usually done to minimize expense, but assessments should compare total expense for both a given level of performance and a given level of risk or protection. To date, the comparisons have often been at the performance level without due consideration to the risk factor.

6.3. Corporate Risks and Information Security

Corporate Outsourcing Risks

Commercial risk from offshoring is multifaceted; in today's knowledge economy, information security risk should be a critical issue. There are also operational business issues including productivity, efficiency, and quality. Business managers everywhere struggle with costs, delivery times, and product quality. Geographic and cultural spread can adversely affect delivery times and product quality even as costs seem to be reduced. Communication paths become longer and more convoluted; communication is more apt to suffer distortion and error from language and cultural difference. Supply chain networks become more diverse, less centralized, and hence less controlled. Protection from manufacturing sabotage and theft becomes more difficult because of the size and extent of the system. Intellectual property protection becomes more porous as infrastructure expands on an international scale. Legal barriers and costs increase as companies cross international boundaries, due to conflicting regulations, procedures, and practices. Safety issues loom large, exacerbated by decentralized operational logistics.

COMMUNICATION

All business depends on reliable, consistent, and clear communication. Manufacturing processes rely on explicit process steps that companies strive to iterate and perfect. Marketing relies on clear and concise descriptions, as well as emotional appeal. A sales department relies on brand, trust, and perceived value. Contracts between procurer and provider rely on all of these, along with some additional complexities. Disputes inevitably arise, and trust is taxed; quality and deliveries will occasionally be compromised; and legal language will be at best a palliative for a situation suddenly gone awry and not easily remedied.

The effectiveness of each of these communication attributes may be strained by physical and legal distance and by cultural difference. Brand names in one country or language may have an altogether different meaning, even pejorative, in another. Trust in a brand can be damaged by local events that can have much wider ramifications. *Copy exactly* is a terrific

concept for manufacturing, but if the instructions are in one language, and the operating crew is literate in another, it may be hard to accomplish.

Sometimes the results can be catastrophic. The Union Carbide process control plant disaster in Bhopal, India was caused by a faulty check valve that likely could have been found by a maintenance team if they had been properly coached, but it killed twice as many people as the September 11 terrorist attacks in the United States and wounded 100 times as many. Many other semiconductor, chemical, pharmaceutical manufacturing, and agricultural processing plants present such risk (Wikipedia). The damage to corporate reputations can quickly outweigh cost advantages.

Companies with daily global interaction, for example, Boeing and Airbus, have a related issue. Whenever a new safety finding occurs, it is imperative to reach the ground support crews at every airport where its planes fly – which is to say, almost everywhere in the world – as soon as possible (Flug-review). Moreover, it must be done with clear, precise, understandable diagrams and instructions. It should not be surprising to learn that Boeing and DuPont each publish more distinct pages of engineering text annually than any other organization on the globe. Only the electrical engineering professional society (IEEE) rivals them. Most companies do not have communication problems of this magnitude, but they lack sophistication in their communication structures. Email, so often relied upon in today's business world, is a notoriously poor mechanism for establishing and maintaining precision. Video and voice conferencing systems lack archival capability, focusing almost completely on the meeting as opposed to the result. Consequently, Deloitte and Touche's recent report on negative experience with offshoring lists *complex governance/management attention* as the leading dissatisfaction issue; this is a clear result of inadequate communication mechanisms (Deloitte and Touche 2005).

Many people have observed that as a company grows linearly in size, its communication paths grow geometrically. From Fred Brooks' observations (1995) about the optimal size of a software development team to Tom Malone's comments (2004) about corporate communication, it has been long established that expanded staff size and extended geography may adversely affect communications, and therefore the effectiveness of human transactions. Communication difficulties are not just due to offshoring; an MIT study found that once people sit in separate buildings (even on the same site), their communication paths seriously erode. This rule also applies to people sitting on separate floors in a skyscraper. What is different in offshoring is that the people on the other end have much less historic cultural alignment and, if they are working for a provider company, perhaps much less allegiance to the procuring company's overall mission and goals as well. Small wonder that the previously mentioned Deloitte report (2005) cites *limited transparency* and *loss of knowledge* among the top five issues.

MANUFACTURING SABOTAGE AND THEFT

Manufacturing sabotage and theft are not large issues for offshoring situations since their costs are absorbed by the provider. They may affect deliveries, and they will certainly affect ultimate costs, but upfront they are not particularly significant issues. On the other hand, for offshore facilities that are part of a multinational company, sabotage and theft have proven on occasion to be very significant. In order to understand manufacturing or services sabotage, the context must be considered. The question needs to be considered whether this is a problem in general that is merely exacerbated by the corporation's size and breadth, or whether the problem traces specifically to something inherent in the offshoring model. For example, there are instances on record where foreign nationals working on H1-B visas in the United States have stolen intellectual property just as there are instances of American or European workers doing the same thing. Whether there is a higher risk of intellectual property theft if one hires foreign nationals is an open question.

INTELLECTUAL PROPERTY (IP) PROTECTION

IP issues occur at several levels. Many nations do not respect other nations' patents or copyrights; most require that individual patents be filed in their country. The costs of this country-by-country protection are high; the protection afforded is variable. The most notorious countries from a software standpoint seem to be in East Asia and Eastern Europe (Alexandrov 2005).

Loss of knowledge is cited as the fifth most significant issue in the Deloitte report; *vendor employee turnover/training* also is a high concern. These topics are broader than IP protection since they include lore, trade secrets, and company processes. IP protection is a risk with all outsourcing; the broader topics are more apt to become issues with offshoring (Deloitte and Touche 2005). The entertainment industry and the software industry, both groups whose major products are contained in codified, digitized sets of bits easily accessed, purloined, and redistributed on the Internet, are plagued internationally by illegal copying, sometimes referred to as software piracy.

The US Digital Millennium Copyright Act (DMCA) of 1998 is a good example of an attempt to legislate intellectual property protection in a way that was at odds with emerging technical capabilities. Such legal attempts to thwart the pressure of new methods are referenced by many hackers as justification for their actions (Electronic Entertainment Policy Initiative 2005; Gantz and Rochester 2005). Sometimes companies strike interesting partnerships with individual countries, and sometimes countries single out companies for sanctions. Microsoft, as the largest software vendor in the world, often has faced such dichotomies, for example, fighting with the European Union to control source code, while, at the same time, providing source code to the Chinese government and acceding to Chinese rules about use by Chinese citizens and organizations in order to gain entry into the Chinese market (Associated Press 2005).

LEGAL BARRIERS AND COSTS OF OFFSHORING

In order to offshore work, companies face a long list of issues about international trade including trade barriers, tariffs, taxes, import and export restrictions, currency hedges, and transfer of partially completed assemblies versus full products, etc. The hidden costs associated with all of these covenants and requirements can be high. The Deloitte report (2005) focuses on this issue and singles out two topics in the top ten, namely, *cost savings questioned* is sixth on the list and *hidden costs* is eighth.

Legal contracts consume a lot of time for the offshoring company. Terms and conditions, notably recourse available in the event of differences, are often reported as major difficulties requiring time-consuming, energy-sapping activities. Among the issues of consequence is jurisdiction in the event that things go to litigation. Usually, the offshored vendor's country will have jurisdiction with the expected risk issues that follow as a consequence for the purchaser and disputing party (Deloitte and Touche 2005). Some of these business and legal issues associated with offshoring are discussed in Chapters 1 & 4.

OTHER COMMERCIAL RISKS

Executive and worker exposure – personal safety – has escalated as an issue, particularly for locales of turmoil. Hostages are taken and sometimes killed. Specific activities are targeted for disruption: oil production in Iraq, WTO meetings in Seattle or Beijing, software companies in Belfast, and Israeli technology companies are but a few of the targets. When a *Wall Street Journal* publisher can be targeted for execution in Moscow, who can consider himself safe? Such risks are not unknown in the United States; Charles Geschke, CEO of Adobe, and William Hewlett's son were taken hostage in the 1970's in the Bay area. But a foreign setting, especially in tumultuous areas or in areas where law enforcement capabilities are weak, seems to raise the *non-control* element much higher. A particularly noteworthy case for the IT industry was the German Red Army plans in 1986 to target the

chief technology officers of the top 16 multi-national high-tech companies. Only one died before the plan was thwarted by international vigilance (absoluteastronomy.com).

Corporate Information Security Risks

Outsourcing software development or other IT-related business processes often leads to large cost savings or quality improvements especially when the work is done in low-wage countries such as India. At the same time, there are greatly increased risks including financial, performance, reputation, intellectual property, and legal and regulatory exposures. For each of these categories, it is necessary to carefully assess the risk, quantify the potential losses, and develop cost-effective risk mitigation strategies, without which there is no effective risk mitigation. Unfortunately, few outsourcing projects include such assessments.

The financial industry has invested heavily in risk assessment and mitigation. Banks have spent billions of dollars on computer security to guard against fraud and theft. International trade risks in commodities are well known, and many risk mitigation methods are in place from payment mechanisms to insurance (a form of risk transference). Information security risks are regularly downplayed, apparently for three reasons: (1) the failures that have occurred are not public knowledge, (2) the exposures have been of relatively low cost to the companies themselves, and (3) breaches are less tangible than, for instance, ships sinking at sea, physical bank robberies, or highway accidents. Some Indian IT outsourcing service providers have been more publicly concerned about information security than the Western companies procuring their services. Numerous leaders of the Indian IT industry have related that they are concerned about security, but, as business managers, they probably will not invest more in security than is required by their clients (NASSCOM; Ramer 2002-2003).

Procuring companies have been conspicuously quiet about security. This apparently curious fact can perhaps be explained by realizing that, when people perceive a security threat, they act to avoid it or protect themselves against it, but if they do not perceive the threat, they do not worry about it. Procuring companies also downplay information security to avoid the threat of negative public opinion and potential regulation. Both of these responses, while rational in some ways, do not often proceed from a concrete analysis of the actual risks involved in the projects. In contrast, leading Indian provider companies have identified client security concerns as an obstacle to growth and, through the Indian software trade association, NASSCOM, have initiated campaigns to enhance security awareness and change perceptions.

THREATS

Risks turn into incidents through two basic kinds of action, accidents and intentional acts. Many are direct, for instance, a computer system fails on-site, a disgruntled employee sabotages the equipment, a well-intentioned employee makes an error, or an external hacker perpetrates an effective denial-of-service attack. There can also be collateral damage where an external incident or accident causes incursion. While accidents can lead to significant damage, this discussion concerns threat actors. These incidents are arguably the most dangerous of anticipatable incidents because they are carefully targeted. Controls against threat actors also help guard against accidents as well. Accidents caused by human error or acts of nature are an essential part of disaster recovery and business continuity planning that are not in our scope.

We briefly discuss six such threats: rogue employees, hackers, organized crime syndicates, industrial espionage, unfriendly nations, and terrorists.

- *Rogue employees.* Citibank customer complaints of fraud led to the arrests in April 2005 of former employees of a call center in Pune, India. They were charged with defrauding Citibank account holders of \$300,000. In this case, four

rogue employees accessed account numbers and PIN numbers to transfer money out of the accounts (Computerworld 2005). Rogue programmers have installed back doors into code, trojan programs that send out sensitive information, and logic bombs that sabotage operations.

- *Hackers.* The term refers to a special breed of programmer characterized as a person who is simply intellectually curious without evil or financial motivations; increasingly it has morphed to include individuals who may have dark intentions, varying from a self-described desire to thwart e-commerce, in general (e.g., viral attacks), to targeting specific companies for specific vendetta reasons (Electronic Entertainment Policy Initiative 2005).
- *Organized criminal syndicates.* Criminal syndicates around the world regularly engage in identity theft for financial gain. Bruce Schneier, CTO of the security firm Counterpane, has said that there is regular trade in credit card numbers and the only reason that most of us have not experienced fraud is that the thieves have not yet had a chance to use our account number (Schneier 2005). In May 2005, a criminal syndicate in New Delhi sold access information to 1,000 British bank accounts. The information was collected from a network of employees at a call center that the British banks had outsourced to. (The Hindu 2005).
- *Industrial espionage.* Competitive intelligence and industrial espionage are supposedly separated by an ethical wall and a legal structure. But in countries where information theft is not illegal, the dividing line evaporates. Offshoring increases the possibilities and profitability of these activities, while decreasing the cost.
- *Unfriendly nation states.* More than 30 states have been identified as developing cyber warfare capabilities. A number of these techniques have been extensively studied for impact. Offshoring to states that have lasting conflicts of interest with the home state of the procurer, whether in legal jurisdictions or other disputed matters, heightens risk elements (Billo and Chang 2004).
- *Terrorists dedicated to attacking national interests.* Numerous organizations are dedicated to cyber attacks on Indian IT sites. Groups of Pakistan-based cyber-hackers have routinely defaced websites and claimed to have penetrated the perimeters of Indian IT companies. *E-jihad* sites have launched extensive denial-of-service attacks on US, Israeli, and Indian targets (Institute for Security Studies 2003). Indian outsourcing sites came under attack by jihadi groups in Bangalore in June 2005 and in Mumbai in 2003.

Corporate Strategic Risks of Outsourcing

Outsourcing key business functions can create a strategic risk that is often disregarded in the day-to-day drive to cut costs and meet deadlines. In the modern hyper-competitive culture of international business, alliances are critical because markets do not allow time for companies to respond to competitive challenges by developing their own capabilities. Instead, a new product or competitive advantage is more easily challenged by entering into an alliance with an existing company that already has that product or capability. However, as Martin Libicki, a security researcher at the RAND Corporation, points out:

“Third parties may want to attack a relationship simply because it is the heart of an opposing alliance. Sundering relationships can render opposing alliances less effective.

The logic of sundering mirrors the logic of binding. The ability to form coalitions ... is of growing value in competitive arenas. Coalitions, these days, float on the exchange of information; notably the privileged exchange of

sensitive information (much as personal relationships are ratified and maintained through the exchange of favors) such as inventory data (e.g. Proctor & Gamble's evolving relationship with Wal-mart) or design information (e.g. for new cars). The greater the importance of proprietary and personal information flowing among enterprises, the more important is the ability to protect such information to its cohesion. Thus the more important good security is to the choice of partners." (Libicki 2006, 9, 3)

There is another set of potential problems associated with outsourcing and that is exacerbated by offshoring. These problems relate to the fact that virtually all procurer-provider relations in the domain of interest to us involve connecting or sharing the information systems of the procurer and the provider. This happens to greater or lesser degrees with greater or lesser vulnerabilities, depending on how it is done.

Various security vulnerabilities can result from this relationship. For example, the procurer allows extraordinary and unsecured access to the provider, the procurer may even have the provider at least partially provide security to the procurer's system, or the procurer could become more dependent on the provider. One can imagine how the two systems can be fairly secure in different ways and how connecting them could create a joined system that is less secure than either one. The connection could expose the procurer to security problems from the provider or expose both to security problems from third parties. Both procurer and provider companies must conduct risk assessments to make sure that the explicit ways the systems get connected do not open such vulnerabilities

6.4. Risks to the Individual: Privacy and Identity Theft

A contentious and challenging aspect of offshoring is its risk impact on individuals. Individuals are pawns in many respects in this global restructuring of business, but they stand to bear the brunt of many issues as risks occur: loss of privacy, loss of jobs, loss of property, and loss of security are and will continue to be experienced at the individual level. Some facets affect employees, while other exposures impact customers. Many effects will be borne by the general population within the home country of the procuring companies; some effects will impact the citizens of many countries. Regrettably, for the most part, individuals will have little to say or do to protect themselves.

Section 6.2 dealt with data security. Without data incursion, there is seldom an issue so protection against the risk of data intrusion is the first order of business. Businesses, governments, and military groups understand a wide range of issues pertinent to data security, and they can make decisions and put policies and procedures in place to mitigate risks. Individuals, though, have little impact on data security procedures or policies.

It is therefore fundamental to describe the risks and exposures of offshoring from the point of view of the individual and to suggest some possible mitigation strategies for them. First, note that so much offshoring has already occurred that the risks are in place and must be dealt with. This topic is politically charged. Many people, particularly in the United States and Europe, have an increasing feeling that *THEY* are putting *OUR* jobs, financial records, health records, and privacy at risk. Some people believe that national security is being compromised as well. Such views, to the extent that they become salient, can have significant political impact (Knox 2005).

What are Privacy Rights?

An offshoring issue of great consequence is the differing cultural and legal definitions of privacy around the world. Personal data of tens of millions of individuals are widely available. Individuals who would make illicit use of this data may have vastly different

geopolitical, cultural, and legal environments than those whose private data is being used. The goal may be criminal as perceived by the victim and his home country, but not necessarily illegal or punishable from the point of view of the extant government, court, or culture in which the perpetrator lives. Historically, citizens have looked to their own government and its legal system for the protections to which they believe they are entitled.

Consider the issues raised if data about AIDS patients is purloined by an extortion group in a web-based cell in the provider country, followed by a set of threats to expose the diagnoses to employers, insurers, and neighbors. Privacy has certainly been invaded, financial impact could be severe, and the social cost to the individual is incalculable. Where could victims of this kind of action turn? The fact is that provider countries often have a very different set of laws regarding citizen rights than do the procurers. Those laws are interpreted or enforced with respect to theft of data on local grounds rather than with reciprocal rules. Thus, some nations' laws invite certain behaviors that other countries would consider illegal.

Privacy in Some Leading Procuring and Providing Countries

A core function of any nation is to secure its borders, including those less tangible and porous boundaries of the information space. Not all nations seek to protect the privacy of their citizenry. In the United States, when privacy conflicts with free speech, the right of the speaker rather than the subject dominates. In Europe, privacy is protected assiduously by most nations, but even there, free speech is also encouraged in ways that abet privacy assaults on occasion. Other countries, such as Israel, have strong laws governing privacy around medical and other sensitive personal areas, but their governments also have histories of dealing strictly with perceived threats to the public welfare in ways that may trample individual privacy rights on occasion. China, which for years has been a concern of human rights groups, presumes that the Four Cardinal Principles govern the nation: Leadership of the Chinese Communist Party, Marxism-Leninism-Maoism Thought, People's Democratic Dictatorship, and Remaining on the Socialist Road. These principles are not supportive of individual privacy rights.

European companies in the main adhere to strong data privacy protection, ensured by zealous data auditing and control. Swiss banking data privacy is legendary, but privacy of individual data – especially health and financial data – also has a long history of protection across the continent. By contrast, India, China, and the United States have been much more open with personal data; selling consumer lists to advertisers is a good example of a common practice in the United States that could be considered infringement upon an individual's privacy. Because of relatively unique European history, many European countries have been loath to send data to countries where the data is not strongly protected. India has proposed information privacy policies for offshoring company data that square with European data privacy policies, and these policies could provide a potential competitive advantage over the United States for offshoring work originating in the European Union (Peterson 2002).

There is no single directional arrow in terms of privacy and offshoring. In some cases, data are offshored to areas where there is stronger protection, and, in some cases, offshoring creates privacy risk distinct from security and operational risks. In order to examine the general issue of privacy more closely, this section will consider several major locations of offshoring and then discuss a set of possible responses.

The European Union

Europe and Canada have the most comprehensive data protection systems of any countries. Countries that send data to Europe can expect protection equivalent to that of the sending nation because the European Union (EU) harmonized and coordinated twenty-five national regulatory systems under the Data Protection Directive in 1995. Each nation

develops its own implementing legislation that complies with the Directive. The Directive was issued both to establish minimum standards on the fundamental right of privacy and to ensure the free flow of personal information between states.

The European Data Protection Directive restricts the data that may be compiled, and it controls data once compiled. There are data that may not be compiled if privacy violations would create human rights violations: sexual orientation, religion, and racial identification. These requirements come from the basis of privacy as a human right, that is, privacy as a right of autonomy. The substantive principles underlying the directive are that data must be purpose-specific in collection and processing, relevant to the reason for processing, accurate, and deleted when the stated purpose has ended. There must be unambiguous consent by the data subject for data collection.

Substantive consent requires notification by the data controller of the identity of the controller and the intended uses of the data. Other information that must be provided before data collection occurs includes the consequences of not providing data, rights of access and correction, and any exceptions for research. The rights of access and correction ensure data integrity by ensuring that subjects can correct, erase, or block inaccurate data.

After the directive was developed in 1995 and implemented by 1998 in most member states, a concern about the lack of data protection in the United States became urgent. Data flow could not simply continue unconstrained to the United States since, from the perspective of the European Union, the United States is an unregulated data haven. The European Union strongly encouraged the United States to harmonize its own privacy regulation with the directive; however, the request was rejected by both the US executive branch and the Congress.

In the 2000 Agreement on Safe Harbor Principles, the European Union and the United States developed a process to prevent an interruption of the data flow from Europe to the United States. The Safe Harbor Act requires American companies to develop privacy policies that align with the Data Protection Directive, inform European customers of their privacy rights under this policy, create easy-to-use complaint mechanisms, register with independent dispute-resolution mechanisms to resolve complaints, and notify customers of any change in policy. However, few companies have signed up for Safe Harbor. At the first anniversary of the Safe Harbor, only 54 companies had registered and complied with the Safe Harbor guidelines (Peterson 2002).

In 2001, the Data Commission approved standard contractual clauses for Data Transfers to Non-EU countries to deal with those nations where neither implementing legislation nor Safe Harbor agreements exist. The Safe Harbor gives EU citizens protection and compliant American companies a relative advantage in obtaining offshoring contracts from EU states. Despite the apparent value in terms of low cost, strategic advantage, and protection from liability, few American firms have taken advantage of the Safe Harbor. Thus, at this point European companies have only a few low-risk choices for offshoring to American firms. Most American and Indian firms to which EU companies offshore must make custom data protection agreements.

The United States

From the perspective of the European Union, the United States is an unregulated data haven. In the United States, personally identifiable data can be accessed by those who assert a legitimate business need even in business sectors where privacy protection exists, for example, finance, health care, and telecommunications. Sectoral legislation includes the Driver's Privacy Protection Act, the Video Protection Act, Electronic Communications Privacy Act, and elements of the Health Insurance Portability and Accountability Act (HIPAA, 1996) (Swire and Steinfeld). Similarly, the Gramm-Leach-Bliley Act (1999) was designed to increase individual financial privacy (Janger and Schwartz 2002).

However, the US approach has proven inadequate. Authorities such as Bruce Schneier have criticized the accuracy and integrity of personal data aggregated by commercial brokers (Schneier 2005b). A recent and widely scrutinized example makes the limits of the US approach clear. ChoicePoint, a commercial data broker, was created as a separately owned subsidiary of Equifax, Inc., and a copy of all Equifax data was transferred to the new company (Solove and Hofnagel 2005). As a subsidiary, ChoicePoint was not required to comply with the privacy regulations governing US financial and credit institutions. Consequently, the regulations that prohibit Equifax from selling its data do not apply to ChoicePoint. Indeed, there have been several news reports in recent years alleging ChoicePoint's disregard for accuracy in its data, and it is this exposure of personally identifiable (and often inaccurate) data that places individuals at risk for identity theft.

ChoicePoint acted explicitly to purchase the Mexican voter rolls which are protected under federal Mexican law (Peralte and Ferris 2003). The three Mexican nationals who sold the data to ChoicePoint were prosecuted, but ChoicePoint itself was not subject to Mexican federal law and it still markets the data internationally. ChoicePoint was also subject to scrutiny in 2000 when the listing of Florida felons provided to purge the data rolls was found to have systematic factual biases against African Americans (Pierra 2001). The basic elements of data protection – notification, consent, auditing, and accuracy – are all absent in ChoicePoint processes (Solove and Hoofnagel 2005). The ability to commit a felony in one nation (Mexico) and then use the results of the felonious data collection, illustrates the limits of the reach of national laws in a networked global economy. The inability to identify a basic classification (living in Florida, convicted of a felony) reflects the risk of lack of data integrity when there are no data protection requirements. In mid-2005, the company announced major changes in its policy and approach. How wide-ranging the results will be remains to be seen (Wall Street Journal 2005).

In the United States the approach to privacy has been specific to particular sectors of the economy. When abuses of data in a business sector are identified, they are addressed by legislation directed to that sector. In protecting data, the conflict between autonomy and seclusion is often implemented as a distinction between prohibited data (no one can ask for the data); opt-in (you must be asked for the data); and opt-out (you must pursue the opportunity not to be included). For example, the Gramm-Leach-Bliley Act allows customers to opt-out of data marketing.

AUTONOMY

Privacy as autonomy underlies many of the sectoral laws that have been implemented in the United States. Privacy in the choice of health care for women, US postal mail, and personal memberships are all grounded in the right to autonomy. The essential observation of privacy as autonomy is that people under surveillance are not free. Actions taken with knowledge of direct data surveillance will be more constrained than actions taken anonymously. While this is sometimes taken to mean that anonymity is not accountability, the freedom of citizens to interact with government and the anonymity necessary for whistle-blowers illustrate the false dichotomy.

Without anonymity for those with little power, those with power have lessened accountability. Anonymity in a democracy is a critical factor in accountability. Perhaps the classic example is the secret ballot for the voting process. This was a hard-won position in the late nineteenth century that today is seen as an inalienable right. The right of autonomy was first defined in the United States legal system by Justices Earl Warren and Louis Brandeis, who also coined the famous phrase *right to be let alone* that underlies privacy as seclusion.

SECLUSION

While the right to be let alone, the right of seclusion, seems at first irrelevant to the issue of offshoring, the changing mores of the web and some of its abuses have brought this segment into sharper focus. The most prevalent violation of seclusion privacy is spam, which frequently originates offshore. In the United States, the CAN Spam Act was seen by many in the anti-spam community as legalizing spam, and by some in the ISP community as providing a uniform legal mechanism for prosecution of spammers. While CAN Spam created a national law, it overrode many stronger state anti-spam laws (Ford 2005). In typical American fashion, specific legislation was enacted to deal with direct abuses, for example, the *Do Not Call* list and the opt-out provision in Gramm-Leach-Bliley.

PROPERTY

The United States is a nation with strong respect for individual property rights, although these rights are constantly being tested. The right to property extends to personal data as property. Excluding specific sector protections, data in the United States are currently regarded as property. Subject rights over data are lost when data are disclosed because property is an alienable right. That is, once sold, there is no longer a personal interest in property any more than one retains a legal right over a house after it has been sold. The property interest in data then becomes entirely the interest of the data owner which is how a data broker is empowered to operate. Thus, the data broker has no direct customer relationship with the subject of the data, and consequently the broker owes the data subject no duty of care. Similar lack of care governs most data considered to be in the public domain. American law even allows for public sector data to be priced and delivered through aggregators and data brokers.

DATA PROTECTION

Data protection legislation has much in common with other privacy legislation: *notice*, *consent*, *integrity*, and *exercise of rights* are all germane. This commonality is based on the Fair Information Practice Principles (Privacy Protection Study Commission 1977). Notice requires that no compilation be secret. Consent requires that data be used only with the consent of the subject. There is continuing contention between passive consent (i.e., opt-out) and requirements for active consent (i.e., opt-in). Integrity requires that data are correct. The most common citizen interaction with integrity is with credit records. Credit reporting organization must provide citizens with credit reports and the right to redress if data are incorrect. Before the 1970 Fair Credit Reporting Act, credit data were often based on gossip (e.g., investigative credit reports) and other spurious sources. Errors in credit reports could not be corrected by the individuals who were the targets of the reports. Similar errors are found today in reports on individuals prepared by data brokers (Schneier 2005b). *Redress*, *access*, and *enforcement* are the mechanisms by which data subjects are ensured integrity. Access requires that individuals are able to view data about themselves. Redress requires that there are mechanisms to correct data.

India

India's property model is analogous to that of the United States, allowing authorized use of personal data. Since the 2000 Information Technology Act, strong prohibitions have been in place regarding data theft (Government of India 2000). India is a bastion for freedom of speech and autonomous action. There is no comprehensive government-filtering regime for Internet content. Internet kiosks flourish with resounding condemnations of government policies, and different social groups engage in battles of words without governmental oversight or intrusion. Anonymous posting is allowed. For an Indian youth, the cultural environment is fully conducive to viewing the web as a simple extension of the local mores. Hence, dissent and spamming about one's beliefs targeting another country not only go unsanctioned, but may be endorsed or supported culturally.

On the other hand, India has a significant regulatory structure in medicine, telecommunications, elections, and other industries deemed critical by the government. For example, election equipment is designed not to show public totals, and votes are held to be private. Each of these regulatory or surveillance regimes concerns itself with an individual's privacy. For example, when the Telecom Regulatory Authority received a proposal by the major carriers in India for publication of a cellular phone directory, the outcry could have been lifted from any Western paper. Health care studies examine the physical privacy provided for patients in terms of examinations and discussion of diagnosis under the medical regulatory authority. Thus while there is not specific privacy regulation in distinct sectors in India, the regulatory bodies in medicine, telecommunications, and elections address privacy rights as part of their regulatory function. As a result of India's involvement in long-term struggles against terrorism in Kashmir and elsewhere, wire-tapping and searching public discussion areas for activity in regard to terrorism are not uncommon.

Data are primarily alienable property in India as in the United States. Data are private property so governmental seizure would have to be strongly justified and public in nature. There is no Safe Harbor agreement between India and the European Union. The current intellectual property regime, and lack of corresponding enforcement, suggests that an enforcement regime on data as property might not be effective.

China

China has a communist government and an institutionalized ruling political party, thus the very concept of personal privacy is contrary to the underlying philosophical organization. China is organized on the Four Cardinal Principles, listed earlier in this chapter, none of which have implications that extend protection to individual privacy. Criticism or violation of the Four Cardinal Principles is prohibited. The overall data philosophy is concerned with state control of Internet use rather than citizen privacy. For example, Internet-based discourse in China has a series of disapproved words and a prohibition of criticism of current leaders and the Four Cardinal Principles. Anonymous electronic speech is officially prohibited in China. Speech on the Internet in China is controlled through technical means (filtering of postings, prohibition of websites, and detection of encryption) and political means (punishment of those who receive or transmit unacceptable words, ideas, concepts, or content). Microsoft has recently acceded to the Chinese government on this point with respect to blog management.

In some cultures, privacy includes the right to seclusion or freedom from excessive intrusion. For example, the right to seclusion in Britain includes the right of citizens to ask to be excluded from junk mail where, as in the United States, this only extends to spam and marketing phone calls. However, there is no right to seclusion in the People's Republic of China. Spam is an approved and active business in China. Asia as a region has had such significant problems with spam that many IT operations blacklist all Chinese incoming mail. For example, both China and Korea have been one-click selections for blocking on Spamcop for years. China is active in hosting websites for spammers and supporting the market for lists for unsolicited bulk email. For example, the Hong Kong-based Fxstyle.net offers, in English, 238 million email addresses for spamming for any business. The information includes more than 10 million AOL, Hotmail, Yahoo, EarthLink, and MSN addresses as well as 1 million personal profiles complete with name, address, email, birthday and country, presumably harvested from the profiles of those advertisers. The target of the web page, the bulk of the email addresses, and the cost of removing that email create costs that are borne by individuals outside of China, yet the laws of their home country pertaining to spam do not apply. Recent research shows that free email accounts receive an order of magnitude more spam than legitimate email from China (Hulten, Goodman, Rounthwaite 2004).

Identity Theft and Credit Card Fraud

Many people are concerned about the ease with which their identity or their credit cards can be stolen. Identity theft can lead to property loss (commonly thought to be only bank account theft, but it can involve property deed transfers or transfer of income allocations) and damaged credit worthiness, and it often involves a long hassle with a multitude of faceless and possibly irresponsible organizations in order to clear a besmirched credit record. It can even lead to a person being labeled a fugitive felon and cause their lose voting rights to be lost when a stolen identity is used in committing a crime.

In the United States where identity theft appears particularly acute, a major factor is that companies are able to sell Social Security numbers tied to names of individuals, complete with addresses, birth dates, and other pertinent information that enables not just invasion of privacy, but also the alteration and use of the data for criminal intent.

Identity theft and credit card fraud are huge problems globally. Given the wave of incidents within the United States in 2005, as described at the beginning of this chapter, it may not be saying much to suggest that consumer data are at any greater risk of exposure in an outsourcing provider country such as India rather than in a procuring country. But it could be more likely that the events will be brought to light and some how constructively dealt with in the country where most of the victims are citizens. However, privacy is a key issue in the debate over offshoring. *Business Week Asia* ran a story on this in August 2004:

"186 bills that aim to limit offshore outsourcing are pending in the U.S. Congress and 40 state legislatures. Dozens of those involve restrictions on transmission of data. For example, the SAFE ID Act, sponsored by Senator Hillary Clinton (D-N.Y.), and a similar House bill by Representative Edward J. Markey (D-Mass.), would require businesses to notify U.S. consumers before sending personal information overseas -- and would bar companies from denying service or charging a higher price if customers balk. Although no such bills have been enacted so far, "next year I think all of this legislation will be back and spike up again as a huge issue, especially if the U.S. recovery stalls", says R. Bruce Josten, US Chamber of Commerce, who helped industry fight the legislation." (Engardio 2004)

The particularity of identity theft in the United States is compounded by the fact that the criminal liability and recourse when an American is defrauded is far from clear domestically and is further complicated by offshoring. Theoretically, the US company that farmed out the work is legally responsible. Indian call centers usually sign their contracts in the United States. Thus, both offshoring procurer and provider can be sued in domestic courts by their corporate customers. However, liability for international security and privacy data breaches is unsettled in case law. Americans must often begin with local police to make a claim of fraud. Many local police departments lack the personnel to address individual fraud cases and are ill suited to address complex international technical jurisdictional issues. A problem with privacy risk in the United States is the likelihood that the large organizations that are most able to mitigate risk instead transfer the costs to individuals who are left without jurisdictional recourse especially when the data is offshored.

A number of cases have surfaced, including the situation at MphasiS, one of India's largest call center providers, where Citibank accounts were penetrated and the events were only found by account holders who called the bank to complain. Nonetheless, an Indian official with MphasiS said later that week:

"While we are unhappy with the incident itself, we are at the same time quite pleased that detection systems worked. While such incidents unfortunately do happen everywhere, timely and exemplary enforcement ensures that no-one needs fear that culprits or potential culprits can get away and the reputation and credibility of the entire system is actually preserved and enhanced." (McCue 2005)

One long-term American consultant to India, when asked to comment on how well the enforcement provisions really work, was quite candid:

"There is no way that the company itself will be prosecuted. MphasiS is one of the top ten providers and their President is the current president of NASSCOM. The individual perpetrators will be prosecuted under a Government of India act but as is typical with Indian justice, it may be years before it comes to trial. For example, there was a bribery scandal in the 1980's involving Bofors, the Swedish defense supplier, and before the case came to trial in the late 1990's several of the accused had died of old age. NASSCOM advocates strong security to its members but it doesn't really have any enforcement power. The only enforcement provisions that would really be effective . . . would be pushed from the demand side. In my work over there, I heard again and again, that providers will conform to whatever security measures the customers require, with an implied 'but unless they require them we will do the minimum we deem necessary'. Therefore, if US companies aren't acting to protect their clients then the government has to step in and protect the privacy of its citizens." (Ramer 2005)

Not surprisingly, most companies in offshoring businesses assert that these were isolated instances. Other observers are not so sanguine. The day after the MphasiS story broke, TBR News had a follow-up story about 310,000 accounts that were illegally accessed via Lexus/Nexus, coupled with the 145,000 that had been fraudulently exposed at ChoicePoint. These predated the 40,000,000 ostensibly accessed records reported two months later at CardSystems. While offshoring did not figure in all of the reported breaches, the net effect has been unsettling for the data handling industry (Timmons 2005; Rigby and Kolker 2005).

Following the April 2005 incident at MphasiS, many in the Indian IT industry called for serious reforms and security improvements, including calls for a law on data protection as well as more stringent laws on enforcement of contracts (Thiagarajan 2005). However, two months after the MphasiS fraud case, a new scandal broke out. A reporter from *The Sun* of London was able to purchase the account information of 1,000 British bank customers for a price of \$5,000. The reporter was told the information came from a network of Delhi call center workers. The contact person boasted that he could provide information on 2,000 accounts a month (Harvey 2005).

Dealing with the Risks and Exposures for Individuals

India's national leadership is seeking data protection legislation to directly compete with US firms for work involving data that are currently offshored from Europe to the United States. Such a change in the competitive landscape would increase the challenges of globalization for the United States in terms of long-term learning, productivity, and employment. The United States has a structural decision to make with respect to international competitive strategy, that is, whether (1) to compete as a high-quality service provider with security and privacy used as competitive advantages, or (2) to compete in the global market as a data haven.

As more and more countries get into the offshoring game, the price pressures on providers of offshored services only increases. According to banking industry sources, effectively securing a transaction can add 15 to 18 percent to the cost (O'Bryan 2003). The real costs of offshoring should include legal, security, auditing, and contingency planning costs, all of which increase when offshoring. A critical but often overlooked issue is that many offshore providers do not perform realistic annual disaster recovery testing. Instead they test with a limited number of client companies at a time. With increased price pressures, the temptation to skimp on security measures strengthens. Thus the need for common and verifiable security standards gets stronger as well.

Outsourced IT-enabled services, whether the service is software development or loan processing or even a call center, involves interaction between the procurer's network which probably is more controlled, known, and trusted, and another network which the client has much less control over, less knowledge of, and can trust less. Networked security will be greatly enhanced if verifiable security standards for offshoring are put in place.

Politicians in a number of US states, as well as in Congress, have begun inquiry into some of these risks and exposures. Of the thirty-six states in 2004 that sponsored legislation that would limit offshoring, only two enacted bills that year. But in 2005, sixteen states had bills introduced in the opening sessions, a clear indication that concern has not abated (Cooney 2005). Given the recent spate of high-profile cases and high number of affected people, much more legislative involvement can be anticipated. This is worth putting into some longer-term perspective. Just as other technologies advanced and enriched the early risk-takers and owners, there were frequently undesired consequences. Pollution from power plants is but one of dozens of examples one could cite. When the undesired consequences rise to impact a sufficient number of citizen's rights (clean air, water, noise), governments generally rise to the occasion to pass laws to protect the citizens. Looking back, the lag time is generally substantial and great harm may occur before citizens acting through their combined power of government set out to seek remedies.

We are now a decade or so into the use of widespread computer networking in which individuals can be brought into harm's way with little to no financial risk to those who actively or negligently inflict harm on others. Just as with sprinklers and fire codes, speed limits and air bags, clean air regulations and smoke stack scrubbers, both legal and technical means can play a role in the information sphere to protect the rights and assets of individuals.

The problem of vetting offshore providers in today's world is complicated. Procuring companies are primarily focused on obtaining the financial benefits of offshoring; most appear to be naive about the risks, or they do not have the time or resources to care. This may account for why this kind of topic so seldom arises in discussions of offshoring. Government vetting in today's world (e.g., by greatly extending the scope and authority of the activities of the interagency Committee on Foreign Investment in the United States) would likely be a nightmare. The best defense is a set of policies that protect against giving providers strong forms of access/control which, in addition to raising the security/privacy concerns, can also make the procurer dependent on, and perhaps hostage to, the provider if it is done foolishly. (Contrary to popular opinion, export controls were remarkably effective for most of their existence for several complex and reinforcing reasons. Industry has often argued against them on the basis that they stifled technological progress, that technology flows were impossible to retard, etc., but those concerns really didn't come into play until the late 1980s.) What can be done in individual jurisdictions is to prevent the transfer of risks to individuals who are the least able to mitigate or recover. Entities that choose a risk should be the ones who pay or profit from the risk premium and any downside. The problem of weak or more seriously compromised provider organizations is considered further in Section 6.5.

It would be highly desirable if economic incentives and competition would be sufficient for companies, both the procurers and providers, to effectively protect the privacy of their customers. So far, as is the case with regard to other forms of cyber security problems, this has not proven to be the case, and it does not seem to be improving as rapidly as the increasing numbers of violations and victims. More generally, the following measures might be considered by lawmakers or regulators and could also be included in offshoring contracts for dealing with situations where there are risks of privacy and identity theft.

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 clear requirements for reporting incidents. Breach should be grounds for termination and financial redress
- Providers should be certified in some way, perhaps through adherence to prescribed standards. The risk is that such standards only provide cover for malfeasance and not true protection. A difficult question is: Who would certify the providers and effectively stand behind the certifications? It would clearly have to include government parties in the provider's home country.
- Offshore providers should agree to no indirect third-party outsourcing without explicit approval from the procurer. This should be contractual, with high sanctions, for example, grounds for termination.

For provider countries:

- Provider countries should enact data privacy laws that apply to foreign citizens whose sensitive data is offshored to their country, or agree to recognize the laws of the procuring countries as applying to foreign citizens and make them enforceable in the providing country. Violation of national privacy laws, in addition to breaches of contract, should be covered.
- These laws should be backed by either demonstrated capacity to enforce (e.g., by a good record of enforcement) or by secured assets in order to ensure penalty
- Providing countries should be certified as Safe Harbors as is done by the European Union, but in the more general context of the procuring country and the foreign citizens who are vulnerable to the compromise of their sensitive data.

For procurer companies:

- There should be reporting requirements and stiff fines for failing to protect sensitive information – just like failing health inspections, speeding, or polluting. While a procurer may be theoretically subject to privacy regulations, experience shows that practice is woefully lacking (Ramer 2005b).

For procurer countries:

- They should consider legislation or other strong forms of regulation requiring any of the measures listed here.
- Certain kinds of information about a nation's citizens or businesses may be considered to be particularly sensitive and vulnerable. Consideration should be given to reviewing such categories and banning certain data from being hosted outside of the originating country.

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 or 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 access.

- Databases should be encrypted to help protect data at rest and in transit and prevent unauthorized data mining for purposes not intended by the procuring organization or contrary to relevant laws.
- Systems should be instrumented to facilitate incident discovery, reporting, and forensics.

6.5 Risks for National Capabilities and National Sovereignty

One important aspect of offshoring risks that is often ignored or treated perfunctorily is the impact on national capabilities. Sovereignty is basic to a national government's reason for existence, and effective sovereignty must include national defense, national economy, and national well-being. While individuals and even companies may bear the immediate and visible brunt of IT globalization, including loss of jobs, compromise of data, and loss of intellectual capital, the overall social impact must be evaluated for a full contextual understanding of the impact of offshoring. In this regard, the IT issues that are addressed in this entire report have considerable consequence to the national interests for many countries. Thus this section examines the threats to a nation's sovereignty that are exacerbated or introduced by IT outsourcing.

Effective sovereignty must include a national economy that is able to provide for its citizen's well being and is not subject to arbitrary manipulation by external forces. As economies have moved from bricks and mortar, and rail and road infrastructures, to an information technology-controlled infrastructure, offshoring of IT raises two key risks, namely, the vulnerability of infrastructure or defense systems to remote electronic attack, and the loss of the ability to fix or replace economic infrastructure

Modern economic infrastructure is dependent on an increasingly global IT network and vulnerable to remote attack through inter-networked systems. Operators in Mumbai or Manila help customers with credit card transactions. Programmers in Bangalore or the Ukraine maintain computer operations for European airlines. Railroads, power companies, and defense contractors regularly use global outsourcing to cut costs and deliver services to their clients. Unauthorized hacker access to these systems could, with malicious intent, cause blackouts, air or rail accidents, or communication system shutdowns. Financial fraud or sabotage of financial system through cyber attacks could be more devastating than physical attacks.

Modern defense systems are arguably even more dependent on information technology than infrastructure systems. From fighter aircraft to command-and-control systems to robot-bomb detonators, software is an essential ingredient. Defense systems developed without proper controls significantly increase the risk of weapons systems failure or sabotage. It is in this context that cyber warfare presents a serious threat.

Earlier sections of this chapter identified the mechanisms by which offshoring increases the risks of IT systems development and maintenance. It expands the range of process vulnerabilities and widens the field of potential threats, thus offshoring significantly increases the risk of a successful infrastructure attack or the compromising of weapons systems. In such situations, offshoring can undercut the national capability to repair and replace these critical components of a nation's defense.

Information Technology is critical because it is intimately bound up with technological innovation. The ability to take an engineering advance and create a functioning software system is a critical part of the process of technical innovation. Therefore the future economic welfare of a nation can be put at risk if it is unable to reproduce technological innovation at a sufficient rate to remain competitive with other players. Concern over

investment in innovation in developed nations, particularly the United States, is discussed in Chapter 8. The impact of offshoring on infrastructure, defense systems, and national capabilities to remain competitive will be discussed in the rest of this section.

Rising Threats to Infrastructure and Military System

Commercial Off-The-Shelf (COTS) product purchasing strategies have been adopted by the United States and other countries in building their IT-based military systems. These countries have also shared national and international commercial Internet infrastructures to facilitate network-centric warfare (NCW) systems. On the positive side, this methodology reduces costs and delivers a wide range of equipment quickly, thus increasing flexibility and functionality. However, COTS purchases can lower reliability and limit opportunities to verify that the software performs its stated purposes. It is more difficult for the buyer to gain insight into source and application code documentation for COTS products especially if the providing companies are offshore (Gansler and Binnenndijk 2004). Many COTS components, and sometimes entire systems, are developed and maintained by providing companies who may themselves procure development and services from other nations who could have privacy, intellectual property rights, security, diplomatic, and defense policies at odds with the original procuring country. Thus, a COTS strategy increases the possibility that a hostile nation or non-government hostile agents (terrorist/criminal) could compromise the system or services. Regardless of the trust level between the countries and/or corporations, a single person working on military or critical infrastructure software could cause havoc by installing programs that compromise combat zones, military and civil command and control systems, and system access.

Offshoring significantly increases the risks to military systems because many network components are produced and or shipped through countries that may be hostile to the national interests of the procuring military organizations. Eugene Spafford, Chair of the U.S. Public Policy Committee of the Association for Computing Machinery (USACM), testified as follows in October 2005 before the House Armed Services Committee.

“Our military and government rely on COTS products and contractors to equip and staff our IT infrastructure. Consider that some of those products that are employed in highly sensitive applications are being crafted, tested, packaged and supported by individuals who would never be allowed into the locations where those applications are used because of national origin, criminal history, and/or personal behavior. Furthermore, some of the hardware and software components in use in critical applications are designed and produced in countries that may be adversaries in future military or political conflict. These factors enable “life cycle” attacks where key systems can be compromised during early manufacture, shipping, and maintenance as well as end operation. We do not have the tools or resources to thoroughly check these items to ensure that they do not have “hidden features” or flaws that may be used against us. We need special attention and methods to produce these supervisory systems and critical applications.” (Spafford 2005)

In Section 6.2, we discussed a recent Symantec threat assessment that shows rising vulnerabilities and malware designed to compromise confidential information. Tying that to the widespread use of COTS in most countries’ military systems, the national security risk becomes clear. The effects of possible critical IT infrastructure breaches include, but are not limited to, the following.

- From a national security perspective, large-scale attacks that manipulate the availability and integrity of military command and control systems can cause malfunction, or in the worst case, loss of life, due to weapon trajectory changes and battlefield misinformation.

- Disruption of IT-based systems and services can potentially increase a loss of situational awareness of an attack, decreasing identification time and time to respond. Not only could these attacks be catastrophic, recovery could be more difficult if the deployed products were developed offshore and the capability to manufacture and develop the hardware and software to replace non-trustworthy or damaged systems is no longer available within the procuring country.
- A significant example of a loss of national capability through global sourcing, though not IT related, is the 2004 closing by UK health authorities of the sole US supplier of a flu vaccine plant. This caused an immediate reaction in the United States especially for citizens at risk. Agreements were obviously not in place between the two countries to supply early warning of the vaccine contamination (Stannard 2004). This experience is especially alarming in the context of growing concern over the predicted bird flu pandemic. The lack of capability to manufacture enough vaccine could lead to major political conflict between procuring and providing countries and, in the worst case, massive fatalities could occur as the virus spread, unabated by an antidote. This example illustrates how technical capabilities can severely impact the ability of a nation-state to provide for its populace.
- Covert access to vital command-and-control systems could undermine military strategies and battlefield success by either exposing or taking advantage of military tactics or distorting data.
- Unauthorized access to confidential records could leave military and civilian personnel open to blackmail and other forms of compromise affecting national security. Compromises causing intermittent failures or loss of integrity of data can also affect loss of life on the battlefield. If failures were deliberately caused, for instance, from built-in malware vulnerabilities such as trojans and bots, an attack such as a buffer overflow or a web-based attack could allow the undetected bypass of security mechanisms such as firewalls or virus scans.
- Allowing access to remotely controlled bots for later attacks could undermine the military and public/private infrastructure of these shared networks as well as those in countries to which they connect.

A broad potential risk, one that could be considerably exacerbated by offshoring, is that the providing organization (or at the least, significant parts of its ownership or management) could be compromised and used by organized crime or foreign governments to the detriment of organizations and citizens in the procuring country. This could serve as a means for bringing about the negative consequences discussed previously. There are many instances of businesses becoming beholden to organized crime interests or fronts for government agencies in nations around the world. Globalization provides substantial new opportunities and reach in this regard.

For such a scenario in an offshoring context, it is easy to imagine the providing organization gaining control over data assets and management (e.g., databases, network operations) that would give it a powerful platform to engage in such activities as unauthorized data mining, intelligence operations, malware planting, attack planning, and money laundering. Given its position as a provider, this might continue for a long period of time, enabling it to do a great deal of damage in a relatively protected way.

In some countries, including Russia, parts of Eastern Europe, and China, among others, where there has been a lack of a well-established rule of law that effectively protects individuals or private enterprises, it may be difficult or impossible for provider organizations

to resist overtures by organized crime or government security agencies. Potential providers have very little means (physical or legal) to defend themselves against such overtures.

Critical Infrastructure – Operation and Investment

From a social perspective, attacks such as those described previously can also cause malfunction and destruction of critical civilian infrastructure, for instance, transportation, power, and financial systems, not to mention loss of civilian life, chaos, and loss of public confidence in the national infrastructure and government. From an operational and investment standpoint, it would be difficult to replace the aging backbone of domestic and foreign-built equipment in the procuring countries' infrastructure and also problematic to train maintenance personnel to install, connect, and operate it. Thus, the impacts on nuclear energy, electric, or water purification facilities could be detrimental not only to health but also to the economy.

The UK Financial Services Authority (FSA) issued a report in May 2005 warning that offshoring could damage consumer protection efforts and lead to increased financial crime (Watson 2005). The report highlighted the greater difficulties of implementing strict controls in offshoring. At the same time, the FSA stressed that risks could be addressed with appropriate risk management strategies. The FSA noted that two key risks were business continuity and high staff turnover.

The high turnover noted in the Financial Services Authority report is a security threat because of the gap in personnel security noted in Section 6.2. Staff turnover has been a problem in the rapidly expanding IT sectors of countries such as India because skilled staff members are in high demand (NASSCOM-Evalueserve 2004). The high demand coupled with the absence of searchable credit or criminal databases greatly increases the likelihood of hiring higher risk employees.

Modern technology-based economies are highly dependent on an extensive array of IT-controlled infrastructure. IT-dependent systems include water and electric power, emergency communications, transportation, oil and gas production and delivery, and health care. These systems are vulnerable to hacking, sabotage, and natural disaster. Hurricane Katrina and the New Orleans flood illustrates how quickly a situation can degenerate when infrastructures fail. Supervisory Control and Data Acquisition Network (SCADA) Systems control critical infrastructure facilities such as nuclear power plants, and these SCADA systems are vulnerable to attack. Systems are not only vulnerable to attacks through their non-Internet-based control systems, but through other, outdated control systems as well. "They're designed to be managed remotely and the remote management is not authenticated, meaning you don't know who's managing it," according to Alan Paller, the research director for the SANS Institute." (Simmons 2005).

Offshoring introduces additional failure points into a system, and it also makes these systems vulnerable to concerted attack in the event of hostilities.

Access and manipulation of financial and telecommunication systems could cause long-term national and global economic damage which, if severe or frequent enough, could cause loss of public confidence in infrastructures and the governments' ability to protect the population. More immediately, the economic costs of interrupted finance would likely paralyze many modern societies. Examples are as simple as a local airline computer failure that led to five hours of queuing to board one international flight (British Air Flight 286, San Francisco to London, March 5, 2005) in order to achieve correlation of baggage with passengers. The September 11 terrorist attacks came within an estimated one mile of destroying the redundant backup for the Eastern Seaboard Point of Presence, the hub concentrator for both voice and web-based traffic for 100 million people, and nearly 65% of America's financial transaction backbone. On the other hand, the Internet protocol proved its survivability under the duress of these events. Although NYSERNet's research network

ran through Ground Zero with transport provided by Verizon, on lines that were severed when Building 7 of the World Trade Center collapsed, the network never wavered. Moreover, the technology's flexibility helped restore commodity service on Long Island and in Westchester County by remapping onto the NYSENet network (Lance 2002).

The September 11 terrorist attack was a warning flag to the US financial infrastructure. The damage, as incredible as it was, could have been much worse. US regulatory agencies took steps to increase scrutiny of offshoring of the financial services electronic commerce systems. The US financial system has become a worldwide network, and along with the Security and Exchange Commission, the US Federal Financial Institutions Examiners Council (FFIEC) began requiring audits of offshore providers. FFIEC issued regulations designed to increase the scrutiny of offshore service providers.

National Economic Health, Security, and Outsourcing

For most nations, creating and maintaining a robust economy with adequate jobs is a key to a sound and stable government. Governments are supported because citizens believe their leaders' policies best serve their national defense, economic, and social interests. When confidence in government with regard to these factors falters significantly, instability is usually not far behind. A country's national security and social policies are influenced by its technological development, natural resource availability and utilization, strength of defense, soundness of financial and operational infrastructure such as transportation and energy systems, trade policies, citizens' ability to create and innovate, and cultural and historic heritage. However, this discussion will focus primarily on issues that may be affected by offshoring.

Offshoring exacerbates some old issues and raises new ones. The rapidly changing technology transfer associated with offshoring has already begun to change country objectives, policies, and cultures for both procuring and providing countries. In recent historical experience, the procuring nation has rarely feared the loss of economic and intellectual advantage to the providing country, yet, as manufacturing industries have shifted jobs away from North America and Europe, that is precisely the concern for those concerned about offshoring.

A key concern for the United States and other developed countries is whether their technological investment and innovation will decline so steeply as to put them into economic decline. The question therefore is how the developed countries that have been technology leaders can preserve their technological capabilities for innovation to maintain successful economies even if they are no longer broadly preeminent over their rivals. There are numerous studies, reports, and commentaries making these points (see, for example, National Summit on Competitiveness 2005; Harsha 2005; National Academies 2005; Lewis 2005).

One example is the testimony given by Nicholas Donofrio, Executive VP for Innovation and Technology at IBM, before the House Science Committee. Donofrio called for a national innovation ecosystem that he said must be fostered by a coherent national policy. In his testimony, he quoted from the December 2004 Report of the National Innovation Initiative and it is worthwhile to review it in some detail. "The push and pull of supply and demand do not occur in a vacuum. They are strongly influenced by public policy and the overall infrastructure for innovation offered by our society. Public policies related to education and training, research funding, regulation, fiscal and monetary tools, intellectual property and market access demonstrably affect our ability to generate innovation inputs and respond to innovation demands. The same can be said of infrastructure – be it transportation, energy, health care, information technology networks or communications. Taken together, the policy and infrastructure environments create a national platform that can accelerate – or impede – the pace and quality of innovation." (Donofrio 2005)

At What Point Does Declining IT Capability Impact National Security?

The United States, which has offshored significant amounts of manufacturing capability over the past half century, is increasingly offshoring its IT capability. Does this really matter? Consumer electronics went offshore without much ill effect on either the national economy or the national security in the 1980s. So did memory chips for computers, and after that, the PC's themselves, plus their displays. Some economists argue that, in fact, this offshoring led to large productivity gains for the United States (Mann 2003, 2004, 2004b).

Many argue that software is different; it does not act as a commodity since the development cycle never ceases. There is often an innovative edge tied to market differentiation that moves well beyond the current frontier of commodity service. This is the uniquely special characteristic of software compared to any other building material. If a country loses control of that frontier, does it risk losing control of its future in both national security systems and in many critical sectors such as financial services, health care, utilities, and industrial controls? Since the critical capability of market differentiation and the agility of systems depend on software capability, the answer is neither easy nor encouraging for US planners.

The future economic welfare of the United States (or other developed countries) could be at risk if offshoring, combined with the absence of appropriate policies, damage the nation's ability to produce technological innovation. It is competitive products and higher productivity that lead most directly to national wealth, but many observers believe that technical innovation is the underpinning for competitive products and higher productivity in the knowledge economy. The concern is that the decline in investment in American research and development and education spending could accelerate to the point where it jeopardizes future reproduction of intellectual capital. This topic is discussed in detail in Chapter 8.

Several popular books explore this issue of national risks from offshoring, one by journalist Thomas Friedman, another by a former trade official in President Reagan's administration, Clyde Prestowitz. These books present visions of the future, though with less than academic rigor. In *The World is Flat*, Friedman explores the results of a highly interconnected globalized world, driven hard by offshoring of IT and its effects on the United States (Friedman 2005). The result, in Friedman's view, is an inexorable and extremely rapid shift of many presumed US advantages, most especially white-collar jobs, to other countries. He predicts a shock wave impact on American politics, business success, and unemployment rates that will likely result in clarion calls for revised educational approaches and tariff legislation as well as much acrimony. But he stops short of saying either that it is a momentum that can be stopped, or for that matter, needs to be

In *Three Billion New Capitalists: The Great Shift of Wealth and Power to the East*, Prestowitz argues that the United States faces such serious fiscal and competitive challenges that it may be headed not only for a declining standard of living but for a 1930's-style depression. The subtitle for Prestowitz's book is telling in itself: *The End of Western Dominance and the Rise of Parity* (Prestowitz 2005). Prestowitz is gravely concerned because the United States is not prepared for the expected economic restructuring driven by globalization. He refers to the mismanagement of the US economy, manifest in low household savings, high budget shortfalls, and unsustainable trade deficits and foreign borrowing. A deeper problem for Prestowitz is the fact that the United States has no national strategy to protect its industry, skilled workers, and technological leadership. He argues that the United States's laissez faire economic ideology and confidence in its technological and productivity supremacy have prevented Washington from grasping the coming crisis and from developing a programmatic national response.

Dealing with Risks and Exposures in National Capability

The risks and exposures from IT offshoring are great and increasing. They include increasing cyber vulnerabilities, hostile cyber warfare policies, theft and abuse of personal and government sensitive and classified information in all countries, attacks on country infrastructure, and changes in business strategies and investment in research and development. Globalization is likely to continue and so are its international effects. These risks and exposures can never be completely mitigated, but strategies at both the national and international levels can be put in place to help manage them.

Problems cannot be solved until they are defined and accepted as valid by a sovereign entity and its citizens. Frank and open national dialogue regarding economics, trade, outsourcing, education, and research issues that does not focus on a corporate or protective agenda would allow citizens to engage in the dialogue and understand the issues.

One topic that the United States and other developed countries might address are plans to protect their nation's cyber-structure and IT competitiveness. The plan might include not only a strategy to address training and jobs but also strategies for legislation, international agreements, policing, tariffs, Internet policies, and a more equitable tax-structure for companies investing at home. It might address the need for more formal government/commercial agreements and funded research to address data protection and communications between stakeholders involved in homeland defense and critical infrastructure. It might also include a discussion of how to make a country more innovative, specifically in light of offshoring which is discussed in detail in Chapter 8.

The offshoring of homeland security technology development and management systems that send vital information such as biometrics, identification codes, tax and personal information overseas are of critical concern. Until better controls for this information are developed, it presents a high risk to all nations. Sensitive industries should have severe restrictions on offshoring. Offshoring of software and design projects in areas such as defense and the other critical infrastructure industries should be tightly controlled. Further research in methods to secure this data and the development of nation-to-nation and international treatment of both the data and how compromises will be handled is vital, including developing and implementing information security standards for international commerce.

Thomas Homer Dixon, the Director of the Trudeau Peace and Conflict Studies Center at the University of Toronto, has studied the relationship between violent conflicts and various kinds of environmental stress in poor countries. He found that environmental stress cannot, by itself, cause violence. It must combine with other factors, usually the failure of economic institutions and government. He concluded that a central feature of societies that adapt well is their ability to produce and deliver useful ideas or what he calls ingenuity to meet the demands placed on them by a worsening environment. Societies that adapt well are those able to deliver the right kind of ingenuity, at the right time and places, to prevent environmental problems from causing severe hardship and, ultimately, violence. If globalization is to be successful, recognition of the rights and equality of the global citizen has to be accepted and become the underpinning of policies and trade agreements. Dixon speculates on whether procuring countries and providing countries can learn from history and forgive past injustices and whether this might determine if global and worldwide innovation will continue.

6.6. Risk Mitigation and Risk Assessment

A basic approach to information security risk assessment is to analyze three key objectives: *confidentiality*, *integrity*, and *availability*. The risks to these objectives are greatly increased by offshoring because of inherent vulnerabilities in offshoring, global communications, and international business.

To illustrate, consider the example of ABG, a fictional software company that sells equipment for processing secure transactions. ABG's systems are only valuable to customers if (1) the internal security mechanisms are kept confidential from competitors and potential attackers; (2) the integrity of transactions are ensured (the data cannot be changed by an attacker); and (3) the process is available and efficient, that is, the process does not slow down or interfere with the client's primary business. Outsourcing the development of new features for the product increases the risks of a competitor or a potential attacker learning ABG's proprietary processes. It also increases the risk that the process will not be as reliable (or have as much integrity) due to the loss of control over the development process and a more complicated supply chain network. While any outsourcing increases these risks, developing the software in another country magnifies them significantly for a number of reasons. ABG no longer controls the network security or the process security of the development center. Offshore developers likely have less legal liability to ABG or its clients. The development and maintenance processes (discussion of proprietary designs, transfer of the software, patches, documentation) are conducted over international global networks with a greater potential for interception. A prime motivator for both provider and procurer becomes cost reduction, which tends to overshadow security or other quality concerns.

Risks exist at multiple levels – financial, performance, reputation, intellectual property, privacy, legal, and regulatory risks. Therefore, it is imperative to carefully assess the risks, quantify the potential losses, and develop cost-effective risk mitigation strategies. Systematic risk analysis and planning involves the following steps.

- Identify and estimate the value of the assets to be protected.
- Identify the potential threats (things that can go wrong) and threat perpetrators.
- Assess the vulnerabilities in the current systems protecting the assets.
- Develop a plan to protect the assets against the threats by remediation of vulnerabilities.

Too often, providing companies simply hire guards and put expensive firewalls and access controls on their network, and then they declare to the procurers that there is no risk. The managers of the offshoring programs at procuring companies repeat this mantra. However, if the asset being protected is client privacy or corporate intellectual property, all it takes is a disgruntled or dishonest employee to copy the data and walk out of the well-protected offshore data center and sell the information to the highest bidder.

Recognition of higher risks for the procurer is not necessarily an argument against offshoring. Risks lead to innovation, and the free market is based on the principle of taking and overcoming higher risks to obtain higher rewards. The accepted response to a risk is avoidance, transference, or mitigation, responses all found within industry for managing the risk profiles of offshoring. The key is a conscious rational assessment and response to the risks in each situation.

Mitigation Strategies

Effective risk mitigation strategies need to be implemented once a risk assessment exists.

- *Security due diligence.* This should include certification to standards such as BS7799, CISP, or True Secure. (Note that SAS70 is not effective in info security space. Note also that Certification cannot be viewed as a license to ignore security risks.) Legal liability and responsibility for protecting both customer data and intellectual property lie with the procuring company management.
- *Business 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, governments, and organizations?
- *Active risk management.* This requires the development and implementation of an ongoing security plan between the outsourcing procuring company and the provider. The plan should include appropriate forms of monitoring, regular reporting of security metrics, incident response, and disaster recovery mechanisms.
- *Third-party risk assessments.* An independent third party should be responsible for regular security audits of the provider. This should be a professional security firm rather than an auditing firm. Past practice has used the CPA issued SAS70 audit as an acceptable security assessment and audit. However, SAS70 audits are usually produced by the audit firm employed by the provider. The scope of the audit is generally defined by the provider and typically includes a pre-audit that allows the provider to correct any embarrassing failures. Consequently, real risks are often overlooked. Therefore, it is essential that a procuring company ask for an independent security assessment.

6.7 Bibliography

Alexandrov, V.N. 2005. (Ex-Soviet CS Director, today Chief of High-Performance Computing Labs, University of Reading, England). Interview by Charles House July 7.

Associated Press. 2005. Microsoft Censors Chinese Blogs. (June). <http://www.wired.com/news/culture/0,1284,67842,00.html>.

Bhat, R. 2002. (Manager Efund BPO) Interviewed by Rob Ramer (Feb.).

Billo, C. and Chang, W. 2004. Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States. *Institute for Security Studies, Dartmouth College* (Nov.).

Brooks, F. 2005. *The Mythical Man-Month*. Addison-Wesley.

Computer Security Institute. 2005. It's All Fun 'Til Someone Loses an I.D.: This Summer's Big Breach Sheds Light Through Holes in Credit Card Security. *Computer Security Alert* (Sept.).

Computerworld. 2005. Indian Call Center Workers Charged with Citibank Fraud (April 7). <http://www.computerworld.com/printthis/2005/0,4814,100900,00.html>.

Cooney, M. 2005. States Target Offshoring – Again. *Computer World* (Network World) (Feb. 28).

Deloitte and Touche. 2005. Calling a Change in the Outsourcing Market. Internal Report, p. 24 (April).

Denning, Dorothy. <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>.

Donofrio, N. M. 2005. Testimony Before United States House of Representatives Committee on Science (July 21).

Electronic Entertainment Policy Initiative. 2005. The Camel Fully Enters the Tent (June 21). <http://www.eepi.org/archives/eepi-discuss/msg00109.html>.

Engardio, P., Puliyenthuruthel, J., and Kripalani, M. 2004. Outsourcing: Fortress India. *Business Week Online* (Aug. 16). http://www.businessweekasia.com/magazine/content/04_33/b3896073.htm

Europe WorldWatch. 2005. *Wall Street Journal* (June 20) A13.

Flug Review. <http://www.flug-revue.rotor.com/FRheft/FRH9802/FR9802h.htm> (Documents the Boeing / Lauda airline disaster).

Ford, R.A. 2005. Preemption of State Spam Laws by the Federal CAN-SPAM Act. *University of Chicago Law Review*, 72, 355.

Friedman, T. L. 2005. *The World is Flat*. Farrar, Strauss, Giroux.

Gansler, J. and Binnendijk, H. 2004. *Information Assurance: Trends in Vulnerability*. NDU Press, 3-5.

Gantz, J. and Rochester, J.B. 2005. *Pirates of the Digital Millennium*. Prentice Hall, Upper Saddle River, NJ.

Harvey, O. Your Life For Sale. *The Sun*, London, U.K. <http://www.thesun.co.uk/article/0,,2-2005280724,,00.html>.

The Hindu. 2005. U.K. Police Probing Call Centre Scam in India. (June 24). <http://www.hindu.com/2005/06/24/stories/2005062404241300.htm>

House, C. Private Communication with IEEE Vice President of Publications.

G Hulten, J Goodman, R Rounthwaite "Filtering spam e-mail on a global scale", Proceedings of the 13th international World Wide Web, May 2004, NYC, NY

Institute for Security Studies. 2003. Examining the Cyber Capabilities of Islamic Terrorist Groups. *Technical Analysis Group, Dartmouth College* (Nov.).

Janger, E.J. and Schwartz, P.M. 2002. The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules. *Minnesota Law Review* 86, 1219.

Government of India. 2000. The Information Technology Act.

Harsha, P. 2005. Lots of News Re: The Case for R&D and U.S. Competitiveness. *Computing Research Policy Blog* (Dec. 5). www.cra.org/govaffairs/blog/archives/000443.html.

Knox, N. 2005. French May Reject EU Constitution. *USA TODAY* (June 27).

Lance, T. 2002. A Vision for the Network: Educause. *NYSERNet* (Draft 12/16)

Lewis, J.A. 2005. Waiting for Sputnik. *Center for Strategic and International Studies* (Oct). www.csis.org/media/csis/pubs/051028_waiting_for_sputnik.pdf.

Libicki, M. 2005. From Intimacy, Vulnerability. *Conquest in Cyberspace*. (To appear).

Malone, T. 2004. *The Future of Work*. Harvard Business School Press.

Mann, C L. 2003. Globalization of IT Services and White Collar Jobs: The Next Wave of Productivity Growth. International Economics Policy Briefs PB03-11. *Institute for International Economics* (Dec.).

Mann, C.L. 2004. Global Sourcing and Factor Markets: The Information Technology Example. *ACM Job Migration Task Force Meeting* (Dec.). Washington, DC.

Mann, C.L. 2004b. What Global Sourcing Means for U.S. IT Workers and for the U.S. Economy. *Virtual Machines* 2, 5 (July/Aug.).

McCue, A. 2005. Indian Call Center Staff in \$350,000 Citibank Theft. *TBR News* (April 11). <http://www.tbrnews.org/Archives/a1528.htm>

NASSCOM. <http://www.nasscom.org/trustedsourcing.asp>.

NASSCOM – Evalueserve, “Information Security Environment”, Study, May 18, 2004. NASSCOM .

National Academy of Sciences, National Academy of Engineering, and Institute of Medicine. Committee on Prospering in the Global Economy of the 21st Century. 2005. *Rising Above the Gathering Storm*. National Academies Press, Washington, DC.

The National Summit on Competitiveness. 2005. (Dec.). Washington, DC. www.usinnovation.org.

O'Bryan, S. 2003. Lecture at Management Information Systems Research Council. *University of Minnesota*.

Pacelle, M. and Sidel, R. 2005. Security Is Breached at Card Processor. *Wall Street Journal* (June 20), A2.

Peralte, P.C. and Ferris, S. 2003. Mexico claims ChoicePoint Stepped Across the Line. *The Atlanta Journal-Constitution* (April 27).

Peterson, A. 2002. , EU Report Reveals Holes in US Safe Harbor Agreement. *Privacy Laws & Business* (Jan.).

Pierra, R.E. 2001. Botched Name Purge Denied Some the Right to Vote. *Washington Post* (May 31) A01.

Prestowitz, C. 2005. *Three Billion New Capitalists: The Great Shift of Wealth and Power to the East*. Basic Books.

The Privacy Protection Study Commission. 1977. *Personal Privacy in an Information Society*.

Ramer, R. 2002/2003. Interviews with Directors of Tata Consultancy Services, Mphasis, Tata Infotech, and Sonata Software (Feb. 2002, Jan. 2003, May 2003, Dec. 2003).

Ramer, R. 2004. (Based on interviews with security personnel at ODC site serving British and US clients.) *Communications with Risks and Exposure Sub-Committee* (April).

Ramer, R. 2005. TerraFirma Security Corporation. (Private Communication, April 25).

Ramer, R. 2005B. Correspondence with peer reviewers.

Rigby, B. and Kolker, T. 2005. LexusNexus Uncovers More Security Breaches. *Reuters*, Amsterdam (April 12). <http://www.tbrnews.org/Archives/a1528.htm>

Schneier, B. 2005. Testimony to Minnesota State Senate Commerce Committee (April 6).

Schneier, B. 2005B. Accuracy of Commercial Data Brokers. *Schneier on Security* 7 (June). http://www.schneier.com/blog/archives/2005/06/accuracy_of_com.html.

Simmons, G. Mission Critical Systems Still Vulnerable to Attack. http://www.foxnews.com/printer_friendly_story/0,3566,172787,00.html.

Solove, D. and Hoofnagel, C. 2005. A Model Regime of Privacy Protection. *GWU Law School*. Research paper #132 (March).

Spafford, E. 2005. Testimony before the House Armed Services Committee Hearing on Cyber Security, Information Assurance and Information Superiority (Oct. 27).

Stannard, M.B. 2004. U.S. ill-Prepared to Handle Bioterrorist Attack, Experts Warn Flu Vaccine Crisis Called Symptom Of Far Wider Problem. *San Francisco Chronicle* (Nov. 1).

Swire, P.S. and Steinfeld, L. Security and Privacy After September 11: The Health Care Example. *Minnesota Law Review*. (To appear).

Symantec Internet Security Threat Report. 2004. Threats for Jan- June 2004, 3.

Symantec Internet Security Threat Report. 2005. Threats for Jan- June 2005.

Thiagarajan, K. 2005. Wake-up Call in Order. *Hindu Businessline* (April 18). <http://www.thehindubusinessline.com/bline/ew/2005/04/18/stories/2005041800200300.html>.

Timmons, H. 2005. Security Breach at Lexus/Nexus Now Appears Larger. *New York Times* (April 12).

Watson, J. 2005. UK Report Highlights the Risks of Offshore Outsourcing. *VNUNet.com* (May 15). <http://www.crmbuyer.com/story/43085.html>.

Wikipedia. http://en.wikipedia.org/wiki/Bhopal_Disaster.

Wikipedia. http://en.wikipedia.org/wiki/Data_haven.