Security and Privacy in Outsourcing with Customer-Specified Risk Tolerance

Raymond A. Patterson, Erik Rolland, and Lisa Yeo [*]

Raymond A. Patterson, Ph.D.
Accounting & MIS
School of Business
The University of Alberta
4-30E Business Building
Edmonton, AB, Canada, T6G-2R6
Phone: (780) 492-5826
Fax: (780) 492-3325
ray.patterson@ualberta.ca

Erik Rolland, Ph.D.
Department of Accounting and Information Systems
The A. Gary Anderson Graduate School of Management
University of California
Riverside, CA 92521
Phone: (805) 280-5050
erik.rolland@ucr.edu

Lisa Yeo, MBA
Accounting & MIS
School of Business
The University of Alberta
Edmonton, AB, Canada, T6G-2R6

[*] Authors are listed in alphabetical order.

Abstract

Outsourcing coupled with technology that enables data to reside anywhere has opened up new challenges to the protection of personal privacy. Privacy laws differ internationally as does the value different cultures place on personal privacy. Such differences have implications for government as well as businesses. The corporation must be aware of the security efforts of all its partners and consumers must be aware of the security of all service providers in the extended value chain, not just the business they are interacting with directly. In this paper we propose a method for controlling risks associated with spreading personal information across an extended value chain. In addition, this method accommodates customer-specified levels of risk tolerance. For businesses, the goal is to minimize the cost of securing data spread across vendors and international boundaries.

Keywords: Privacy, Security, Outsourcing, Mixed Integer Linear Programming

1. Introduction

We live in a world that is extremely interconnected. Outsourcing has become a standard of business, allowing organizations to specialize (focus on their own core competencies) and take advantage of cost savings. Technology in particular has enabled data to live anywhere – we can transmit huge databases in seconds to data centres overseas. As a result, a consumer's data may reside not just with the primary company they've chosen to do business with; it may reside with companies and in locations which explicitly jeopardize the security and the privacy of the data.

Why do we even care about protection of privacy? Personal privacy is considered a basic legal right in most political systems (Bessette and Haufler, 2001), consumers demand a level of privacy, and there may even be a need to protect corporate trade secrets. Consumers in particular are worried about the loss of their personal information leading to financial or identity theft. For organizations, information security is a problem that is linked to both the customers' and suppliers' trust, and severely impacts the financial well-being of the organization.

International Privacy Concerns

When data crosses international boundaries, it comes under different laws. The USA PATRIOT Act of 2001, for example, has the ability to gain access to corporate databases regardless of the corporation's country of origin. Access under PATRIOT, however, may contravene privacy laws in that company's country of origin. How, then, can a company make decisions on protection of personal data and even where to store their data?

Conflicting laws impede the free flow of information which is a necessary component of the new information-based economy (Bessette and Haufler, 2001). Bessette and Haufler (2001) state that, while it seems obvious that countries with the greatest stake in the free flow of information would cooperate to find a common legal framework, this has so far not been the

case. Indeed, the United States and European Union have been working on this for over a decade with no clear resolution, although the US only began negotiating in earnest once the European Union threatened to cut off all transfers of personal information due to perceived weaknesses in protection of privacy laws in the United States (Bessette and Haufler, 2001).

Safe Harbor was introduced in 2000 as a way for US companies to voluntarily agree to meet stringent privacy requirements, allowing them to continue to process personal information from EU companies. The EU accepted that companies complying with Safe Harbor would meet the 'adequacy' standard for privacy protection defined in the European Commission's Directive on Data Protection from 1998 (US Department of Commerce, 2006).

In the absence of coordinated international privacy standards or regulations, multinational organizations have been forced to create information systems that will support the diverse requirements in order to ensure compliance in each country (Rudraswamy and Vance, 2001). This approach is inefficient; it increases the cost to each individual organization and reduces the efficient operation of the business (Rudraswamy and Vance, 2001).

Protection of Personal Information

People are willing to share their personal information when they see the benefit in doing so (Yu & Cysneiros, 2003) and believe that the entity they are sharing with will protect that information (Meinert, Peterson, Crossland, and Criswell, 2005). As long as the risk of loss of privacy from a particular vendor remains below a certain threshold, the consumer will share. This risk threshold will depend on the type of information that is collected; sharing of publicly accessible information such as a telephone number will have a lower threshold than something like a social security or social insurance number (Meinert et al., 2005).

Concerns about protection of privacy originally arose from worries about how governments would use information collected about their citizens – fears of "Big Brother" (Bessette and Haufler, 2001). Now, however, corporations are collecting increasing amounts of data about their customers and this information can be "collected, organized and even matched" with other information sources to build a more complete picture of the individual (Bessette and Haufler, 2001). While this allows for more tailored offerings to the customer, it also means the individual loses control of their information (Bessette and Haufler, 2001).

Culture may play a role in sensitivity to privacy protection (Rudraswamy and Vance, 2001). For example, Smith and Kallman (1996) found that Canadians have higher privacy concerns than Americans for "collection," "secondary use," and "unauthorized access to information" (Rudraswamy and Vance, 2001). Cultural values have been seen to play a role in political systems and legislation (Milberg et al., 1995), thus cultural sensitivity to privacy will play a role in the development of privacy regulations. As a result, it will likely be a long time before global standards for protection of privacy will be developed. Given conflicting international regulations, customer expectations, and business requirements, is it possible to quantify the need for privacy protection measures?

In this paper we investigate the security and privacy risk associated with firm outsourcing decisions. While outsourcing, in general, involves a whole series of risks, this paper proposes a model for specifically controlling security and privacy risks.

2. Literature Review

Varying international laws

The problem of transborder data flows has been recognized for decades. The Organisation for Economic Co-operation and Development (OECD)'s Guidelines on the Protection of Privacy and Transborder Flows of Personal Data dates back to 1980 (OECD, 1980). Milberg et al. (1995) examine the role that cultural values play in approaches to privacy protection, an idea further explored by Bellman et al. (2004) through surveys of Internet users from 38 countries. Bellman et al. (2004) found that different national regulations reflect the different cultural values; for businesses, this suggested a need for 'localized privacy policies' (Bellman et al., 2004). Examples of such country-specific policies in the US include the Sarbanes-Oxley act (SOX), the Gramm-Leach-Bliley act (GLBA), and the Health Insurance Portability and Accountability Act (HIPAA). These laws reflect local US cultural values with respect to privacy and security on issues related to financial reporting, the financial industry, and healthcare respectively. Most states/countries have security and privacy laws and regulations which reflect their local cultural values.

While there is support for the OECD guidelines, privacy laws are certainly being developed with focus on national priorities (Bellman et al., 2004; Jones and Meller, 2001; Baumer, Earp, and Poindexter, 2004). Bessette and Haufler (2001) note that it has been easier to come to agreement on international issues surrounding encryption of data than protection of privacy; in part due to differences in the relationship between business and government in different countries.

In the absence of coordinated international privacy protection standards or regulations, multinational organizations have been forced to create information systems that support the diverse requirements (Rudraswamy and Vance, 2001; Milberg et al., 1995). This is inefficient, being expensive to develop and maintain, and cumbersome to operate.

OECD Guidelines

In 1980, the OECD member countries adopted guidelines on the protection of privacy and transborder data flows of personal data (OECD, 1980). In recognition of the increasing flow of data across international borders enabled by advances in technology, the countries recognized a need to coordinate protection requirements and practices. The guidelines have eight principles:

1. 'Collection Limitation – limits on the personal information obtained, the information should be obtained lawfully and with consent of the individual
2. Data Quality – data should be relevant to the purpose collected, accurate, complete and up to date.
3. Purpose Specific – purpose of data collection should be specified at time of collection and use should be limited to those purposes.
4. Use Limitation – data should not be used for anything but the specified purpose unless the subject explicitly agrees or by authority of law.
5. Security Safeguards – data should be protected against loss, unauthorized access, destruction, modification or disclosure.
6. Openness – there should be openness about developments, practices, and policies with respect to personal data.
7. Individual Participation – the individual has the right to inspect the data held on them.
8. Accountability – the data controller must have measures in place to be able to meet the principles stated.' (OECD, 1980)

The goal of these guidelines is not to impose unreasonable restrictions on data collectors; rather it is to balance the protection of privacy of the individual with the need for data to flow freely across borders.

Despite agreement on the principles of privacy protection, countries differ in their approaches to ensuring this protection. The European Union quickly created the Directive on Data Protection in 1998 to enshrine protection, although individual members of the EU have modified the model in creating their own national privacy laws (Neil, 2005). Conformance with the EU directive is compulsory for all EU members. The United States, on the other hand, preferred self-regulation for protection of privacy, allowing each industry to set its own principles and practices (Bessette and Haufler, 2001; Aldhouse, 1999).

The USA PATRIOT Act of 2001 runs contrary to United States' preference for market-driven privacy practices. PATRIOT was passed in the wake of the September 11, 2001 terrorist attacks in the US and allows lawful access to personal data by federal law enforcement agencies without the knowledge of the individual. This has raised some red flags for not only American citizens but also anyone who may have data housed with a company subject to PATRIOT. The Assistant Privacy Commissioner of Canada (Office of the Privacy Commissioner of Canada, 2005) sums up the changes that PATRIOT has brought:

> *"What has changed with the passage of* USA PATRIOT Act *is that certain U.S. intelligence and police surveillance and information collection tools have been expanded, and procedural hurdles for U.S. law enforcement agencies have been minimized. Under section 215 of the* USA PATRIOT Act, *the Federal Bureau of Investigation (FBI) can access records held in the United States by applying for an order of the Foreign Intelligence Surveillance Act Court. A company subject to a section 215 order cannot reveal that the FBI has sought or obtained information from it."*

The British Columbia experience

In the spring of 2004 the British Columbia (BC) government was looking at outsourcing administration of the public health program. The BC Government and Service Employees Union launched a lawsuit to block this action; one of the lawsuit's allegations was that outsourcing to an US company would violate BC's privacy laws by making records subject to USA PATRIOT act seizure provisions (Loukidelis, 2004). Loukidelis, the BC privacy commissioner, released a report in October 2004 that stated it was likely that information housed with a US based company would be subject to PATRIOT and that such an exposure would violate BC's privacy legislation. The commissioner recommended that BC and the Canadian government enact legislation blocking the application of PATRIOT to companies housed in BC and Canada, respectively (Loukidelis, 2004).

The BC government did not wait for the privacy commissioner's report before creating legislation (Cate, 2005); Bill 73 requires that personal information held by a public body must be held and accessed in Canada only (section 30.1) (Murray, 2004) and requires a service provider to notify the Minister if a foreign demand for access to personal information is received (Cate, 2005; Murray, 2004).

CIBC Visa cardholder agreement

In 2004, CIBC sent a new Visa cardholder agreement to cardholders stating that cardholder information shared with third-party service providers located in the US, would be subject to USA PATRIOT regulations. Cardholders filed complaints with the Canadian Privacy commissioner leading to an investigation under the Personal Information Protection and Electronic Documents Act (PIPEDA):

> "In short, an organization with a presence in Canada that outsources the processing of personal information to a U.S. firm cannot prevent its

> customers' personal information from being lawfully accessed by U.S. authorities" (Office of the Privacy Commissioner of Canada, 2005).

Further, it was noted that CIBC was not notifying customers that their information *would* be accessed, simply that there was the *risk* that it could be "lawfully accessed by U.S. authorities because of where it is processed" (Office of the Privacy Commissioner of Canada, 2005). Thus, information sent for processing to another jurisdiction is subject to local laws, which may be in conflict with the consumers' preferences. As a result, Canadian consumers found that their privacy preferences cannot be enforced when their information leaves the country.

Blocking laws

In March 2006, the Alberta government introduced Bill 20: Freedom of Information and Protection of Privacy Amendment Act which includes language intended to block the application of USA PATRIOT to data that resides in Alberta without going through an Alberta court (Jablonski, 2006). British Columbia's Bill 73 amended the existing Freedom of Information and Protection of Privacy Act (FOIPPA) to block public bodies from storing or providing access to personal information outside of Canada (Murray, 2004).

There are some problems with this piecemeal approach. Alberta and British Columbia have taken provincial, unilateral actions to address a multinational issue that "requires a serious, multinational response" (Cate, 2005). The BC Privacy Commissioner recognized the need for a cooperative approach. His recommendation 16 called for a "comprehensive, transnational protection standards and for multilateral agreements respecting … information sharing for government purposes" (Loukidelis, 2004), although only for Canada, the United States, and Mexico.

A unilateral approach has also placed an undue burden on corporations trying to do business across borders. Multinational companies now require detailed contracts to satisfy the

requirements of Canadian laws such as BC's FOIPPA – even to the point of needing to restrict access to personal information by US employees of a service provider (Cate, 2005). Such restrictions negatively impact the efficient operations of an outsourcing agreement, for example.

The Assistant Privacy Commissioner of Canada noted in her findings on the CIBC case that not only are there US laws pre-dating PATRIOT that allow lawful access to personal information in the US, there are also Canadian laws with the same provisions (Office of the Privacy Commissioner of Canada, 2005). Indeed, Canada and the US have been cooperating for years to be able to share information and have traditionally "negotiated when efforts to obtain that information conflicted with the values of either nation" (Cate, 2005).

Cost to consumers

Personal information can be used to commit financial crimes such as credit fraud, be used inappropriately by government agencies, or even to commit identity theft. While identity theft is not the sole consequence of loss of personal information, it is one that can be measured.

According to a Javelin report, identity theft affected 8.9 million Americans in 2006 (Johannes, 2006). In the cases where the method of obtaining personal information could be identified, 35% were through methods under the control of businesses (that is, not under the control of the consumer) (Johannes, 2006). The data was stolen from a company that manages financial data in 6% of the cases, as a result of misuse of data from a transaction 7% of cases, taken by a corrupt employee in 15% of cases with the remaining 7% obtained in some other way (Johannes, 2006). In contrast, 30% of the cases reported that data was obtained when the individual's wallet was lost or stolen (Johannes, 2006). Are consumers over-estimating the risk of sharing their data with businesses?

The average time to resolve an identity theft was 40 hours in 2006. However, two thirds of victims have lingering problems after resolution such as incorrect credit reports, banking problems, and harassment from creditors (Johannes, 2006).

Protection of Privacy as Good Business

Data security is often considered a cost of doing business; however, there may be real benefits to protecting customer information. A study conducted by Privacy & American Business and Deloitte & Touche LLP (2005) found that 64% of consumers chose not to buy online if they were uncertain how their personal information would be used. A survey by the Ponemon Institute has found that 70% of respondents consider "two breaches in the same company would be sufficient grounds…to take their business elsewhere" (Ponemon, 2006). It is evident, then, that even a single breach can have an impact on the reputation of an organization (Ponemon, 2006).

In the end, consumers are concerned about the protection of their personal information. Privacy is considered a basic human right by many and the need to protect personal information collected by businesses or government agencies will have an impact for the foreseeable future. Further complicating the need to protect privacy are the differences among cultural sensitivities with respect to personal privacy.

Outsourcing, Risk, and Security

The risk categories associated with outsourcing are numerous, and includes issues related to contracts, scope, costs, expertise, decision processes, technical returns, and privacy and security (Tafti, 2005). Tafti details risk factors associated with each of these categories. Our primary concern is with privacy and security. According to Tafti (2005), three primary risk factors for privacy and security are: corporate policy, audit and control, and host government

laws and regulations. He concludes that "Without a thorough assessment of various risks involved in offshore outsourcing of IT activities, however, any benefits may be offset by significant losses due to various risk factors and missed opportunities."

Sutton (2006) discusses the risks associated with extended firm value-chains, and the integration of internal information systems with inter-organizational systems, in which the privacy and security challenges are very similar to those of outsourcing. Sutton (2006) concludes that 'IT governance practices and enterprise risk management strategies have not kept pace with rapid changes in organizations, technology, business models, including linked supply chains, leaving many enterprises vulnerable to unidentified risks inherited from business partners.'

Klosek (2005) outlines several risk management strategies to mitigate privacy risks associated with offshore outsourcing in light of US laws and regulation. In this paper, she urges US firms to assure that contractors, outsourcers, and service providers comply with emerging standards in both the US and the host countries. The proposed strategies include internal privacy and data audits, due diligence into the service providers experience with privacy and security, understanding local laws in all jurisdictions involved, especially regulations on data subject consents for transferring data,

In this paper we focus on the part of security and privacy that are related to the disclosure and/or loss of data, and the risks discussed in this paper are risks directly related to data loss and disclosure. In an interconnected and outsourced world, an individual's personal information may reside with third-party businesses anywhere within the extended supply chain. Data could be compromised at a number of locations – through the original consumer-business relationship or through one of the business' service providers. Data can also be compromised in-transit to an

off-site storage facility. In February 2005, UPS lost Bank of America backup tapes containing personal information such as Social Security numbers of 1.2 million federal employees (Collett, 2005). This incident was followed quickly by similar backup tape losses in May, June, and July (Collett, 2005).

A consumer's personal information is compromised if any involved vendor is compromised. Is there a way to quantify this risk? The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) have developed a set of trust services (www.webtrust.org). These proposed trust services are professional assurance and advisory services to address the risks and opportunities of information technology. They have developed a set of criteria and principles that govern risk issues related to inter and intra organizational privacy and security (WebTrust and SysTrust, respectively). SysTrust aims at measuring the operational reliability of the firm's information systems. WebTrust aims at assuring security, online privacy, availability, and confidentiality needs in electronic commerce transactions. In total, these principles address security, availability, processing integrity, privacy, and confidentiality. These are examples of forms of assessment of risks related to privacy and security in outsourcing.

3. Model Formulation

As shown in Figure 1, a consumer's personal information interacts with more than just the place of business with which the consumer shares their information. In this example, the consumer chooses to share the information with the business without realizing how that information may be disseminated with that business' service providers. For the business in Figure 1, there is most likely some level of risk of data loss/privacy breach that they are willing

to accept. This level may relate to the point at which their reputation begins to suffer, which is related to a threshold of risk that the consumer, or class of consumers, is willing to accept, or to an accepted privacy/security standard. Once this threshold value is reached, the reputation of the business suffers and consumers will choose to do business elsewhere. In an outsourcing setting, the goal, then, for the business, is to find the most cost effective way to ensure they remain below the consumer's risk threshold.

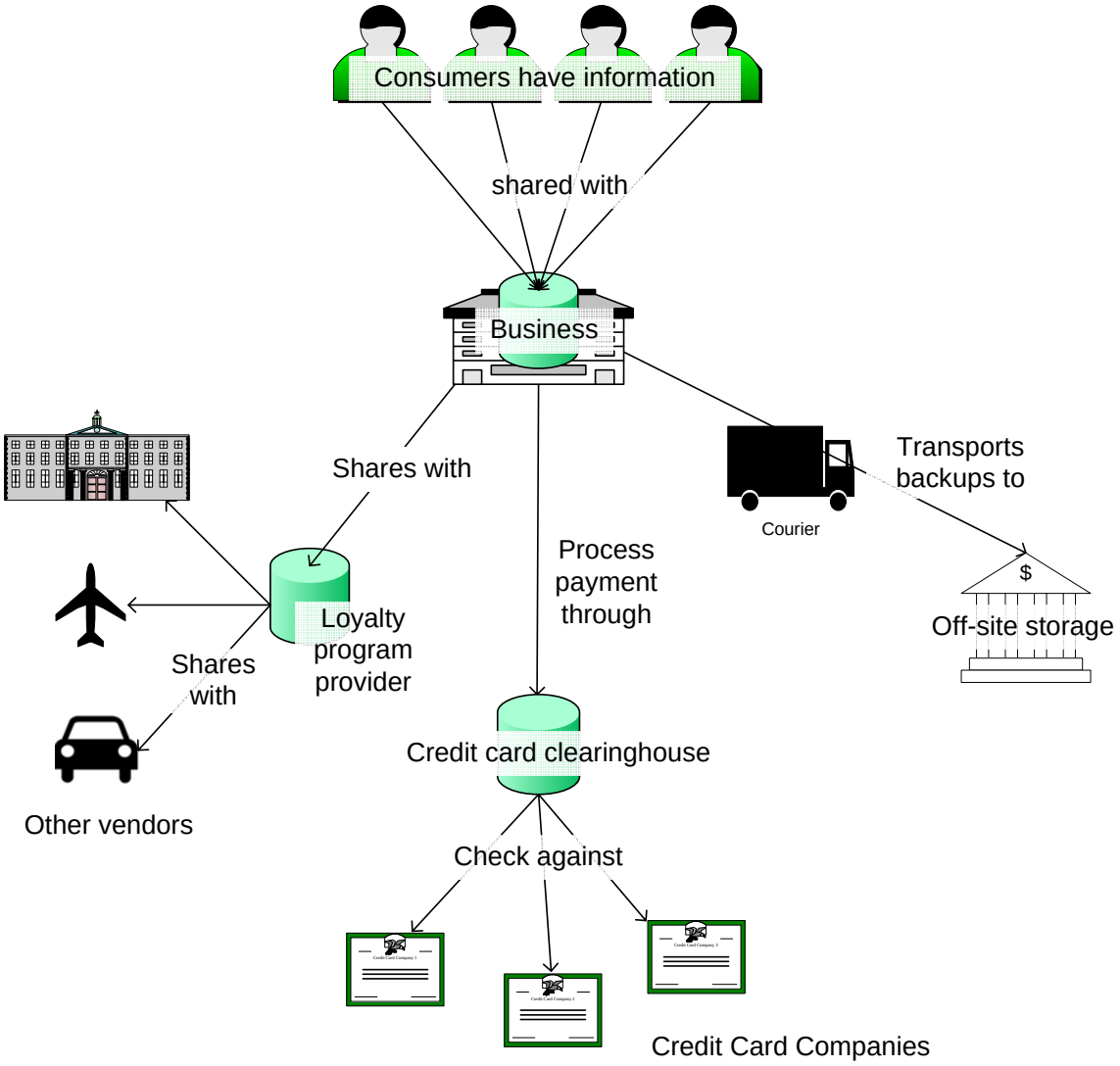

Figure 1 –Consumer Personal Information Sharing

In this section we model the type of information outsourcing situation found in Figure 1. Before we begin with a discussion of the model, we must first define the sets, parameters, and decision variables. Note that the parameters, F_{ih}, C_{ihjk}, T_j, and r must be gathered from business experience.

Set definitions:

H = {h | h is a particular level of security available}

I = {i | i is a risk point associated with a particular vendor}

J = {j | j is a customer class of people whose personal data is at risk}

K = {k | k is a component of the overall information portfolio which is at risk of disclosure}

Parameters:

F_{ih} = Fixed cost of outsourcing to vendor i at security level h

C_{ihjk} = Variable cost of using vendor i at security level h for customer class j's component k

T_j = Threshold of risk for person j

M = Some very large number

r_{ihjk} = risk related to the compromise of component k for person j from the vendor i at security level h due to exposure

Decision Variables:

$$X_{ihjk} = \begin{cases} 1 \text{ if exposure of component k of person j from vendor i at security level h} \\ 0 \text{ else} \end{cases}$$

$$Y_{ih} = \begin{cases} 1 \text{ if vendor i is utilized at security level h} \\ 0 \text{ else} \end{cases}$$

R_{jk} = the maximum risk related to the potential compromise of component *k* for person *j* among all vendors that hold this data

Model Overview:

There is a cost associated with securing personal data regardless of the laws involved. The goal is to minimize the organization's cost of outsourcing while holding security and privacy risks to acceptable levels. There is an initial fixed cost associated with protecting the information, as well as a variable cost associated with each transaction. The fixed costs includes costs associated with certified audit assessments, due diligence, and contracting.

Each consumer or group of consumers will have a threshold of tolerable risk, T_j. As long as the risk of compromising personal data remains below this threshold, the consumer will continue to do business with the firm. The goal can now be described as protecting personal data at the most cost effective level while keeping the maximum risk for each consumer (or group of consumers) below their risk tolerance level, T_j. Academic literature proposes two approaches to assessing risk perception: psychometric methods (Slovik, Fischhoff, and Lichtenstein, 1980; Slovik, 1987; Slovik, 1992) and cultural paradigms (Douglas and Wildawsky, 1982). While risk assessment is a complex matter, the tolerance level could be established by exposing consumers to standard operational security metrics, such as those described by Robinson (2004). These metrics include factors such as intrusion success, unauthorized access attempts, unauthorized information disclosures, and others (Robinsons, 2004). T_j is a simplified measure of the overall tolerance for the various security metrics.

Depending on the transaction, the firm will collect different components, *k*, of information from the consumer, *j*. It will then share some components, *k*, with some vendors, *i*, in its extended value chain. Each vendor, *i*, has some level, *h*, of security that it provides to the

components. The security level is a managerial assessment of the vendors compliance with security and privacy standards. This could be as simple as a scale of low, medium, and high compliance.

There is a fixed cost, F_{ih}, for securing vendor *i* at security level *h*. If vendor *i* is used to process a component *k* for a customer *j*, then there is also a variable cost, C_{ihjk}, associated with this use for the security level *h*.

Given that vendor *i* must process a component, *k*, for customer *j*, there is some risk, r_{ihjk}, related to the compromise of component *k* for person *j* from the vendor *i* at security level *h* due to manipulation exposure. Again, this risk level could be established using standard operational security metrics, such as those proposed by Robinson (2004). Again, these metrics could include factors such as intrusion success, unauthorized access attempts, unauthorized information disclosures, and others (Robinsons, 2004). R_{jk} is used to represent the maximum risk related to the potential compromise of component *k* for person *j* among all vendors that hold this data. The maximum risk, R_{jk}, is not cumulative. Rather, it is the maximum risk of exposure from any vendor.

X_{ihjk} represents the manipulation exposure of component *k* of person *j* from vendor *i* at security level *h* and is likewise 0 if unused or 1 if the component *k* of person *j* is able to be manipulated by vendor *i* at security level *h*. Not all vendors, *i*, must be used at a security level, *h*. Thus we use Y_{ih} which will equal 1 if vendor *i* is used at security level *h* and 0 otherwise.

Optimization Model:

$$Min \sum_{i} \sum_{h} F_{ih} Y_{ih} + \sum_{i} \sum_{h} \sum_{j} \sum_{k} C_{ihjk} X_{ihjk} \qquad (1)$$

Equation (1) is the objective function which minimizes the total fixed cost of using particular vendors at their particular level of selected security, as well as the variable cost of performing particular tasks *k* for particular customers *j*.

$$\sum_{k} R_{jk} \le T_j \qquad \forall j \qquad (2)$$

The cumulative maximum risk associated with all of the components of risk for each person *j* must remain at or below an acceptable threshold T.

$$\sum_{j} \sum_{k} X_{ihjk} \le M * Y_{ih} \qquad \forall i,h \qquad (3)$$

If vendor *i* is used at security level *h* with the variable X_{ihjk}, then the variable Y_{ih} signifies the use of that vendor *j* at security level *h*.

$$R_{jk} \ge \sum_{i} \sum_{h} r_{ihjk} X_{ihjk} \qquad \forall j,k \qquad (4)$$

This constraint calculates the maximum risk that each customer *j*'s component *k* is exposed to among all vendors *i* at all security levels *h* for which person *j*'s component *k* is exposed. R_{jk} will equal to the maximum risk among all of the vendors *i* at any security level *h* which handle the data for person *j*'s component *k*.

$$\sum_{h} Y_{ih} \le 1 \qquad \forall i \qquad (5)$$

For each vendor *i*, allow only 1 security level *h* to be selected.

$$\sum_{i} \sum_{h} X_{ihjk} \ge 1 \qquad \forall j,k \qquad (6)$$

Every person *j*'s risk component *k* must be handled by at least 1 vendor *i* at security level *h*.

The parameters, F_{ih}, C_{ihjk}, T_j, r and v must be gathered from business experience.

4. Computational Experiments

In order to test the model proposed in section 3, we generated a series of test problems. For our experiments, we use 3 security levels (*h*) and 3 components (*k*) of the overall information portfolio which are at risk of disclosure for each customer. We assume that increasing *h* is equivalent to increasing security, meaning increasing fixed cost, increasing variable cost, and decreasing risk.

Fixed Cost:

The fixed cost F_{ih} of securing vendor *i* at security level *h* was set as follows:

$F_{i1} = 200+(ran*100)$, where *ran* is a random number in [0..1].

$F_{i2} = F_{i1}*(1+ran)$, where *ran* is a random number in [0..1].

$F_{i3} = F_{i2}*(1+ran)$, where *ran* is a random number in [0..1].

Variable Cost:

The variable cost C_{ihjk} of using vendor *i* at security level *h* for customer class *j*'s component *k* was set as follows:

$C_{i1} = ran*100$, where *ran* is a random number in [0..1].

$C_{i2} = C_{i1}*(1+ran)$, where *ran* is a random number in [0..1].

$C_{i3} = C_{i2}*(1+ran)$, where *ran* is a random number in [0..1].

Risk:

The risk r_{ihjk} related to the compromise of component *k* for person *j* from the vendor *i* at security level *h* was set as follows. For each *i*, *j*, *k* combination:

$r_{i1jk} = 0.1 + (0.7*ran)$, where *ran* is a random number in [0..1].

$r_{i2jk} = r_{i1jk} * (1 - ran)$, where *ran* is a random number in [0..1].

$r_{i3jk} = r_{i2jk} * (1 - ran)$, where *ran* is a random number in [0..1].

For each customer (*j*) and work component (*k*), the risk (*r*) associated with each vendor (*i*) is randomly distributed over the range [0.1,0.8] for the lowest (cheapest) security level. The risk for each security level (*h*) decreases as a random percentage of the cheaper (previous) security level as security is increased from level *1* to level *3*.

The customer's threshold for risk (T_j) is measured on a [0,1] scale, where zero (0) is complete intolerance of risk, and 1 is a tolerance for any amount of risk. As T_j approaches one, the optimal solution disregards risk and only minimizes cost. Thus, in this uncapacitated version of our problem, the solution is expected to drive to the provider or providers that generate the absolute cheapest solution when T_j=1 for all customers.

When the customer becomes less tolerant of risk (T_j is decreased), then the lowest cost solution will become too risky and other solutions must be explored. Eventually, T_j is decreased to the point which there are no feasible solutions. Also, as T_j decreases for all customers, the problem is more difficult to solve. The particular solution will depend on the specific cost and risk structure of the problem, so it is impossible to make categorical statements regarding the characteristics of the solution.

Higher fixed costs drive the solutions toward single-vendor solution (see Table 1). In Table 1, variable costs are zero and the risk threshold T_j is held uniform for all customers *j*. T_j is varied from 1 down to 0.005. We use 30 vendors (*i*) and 20 customers (*j*) in Table 1. If the fixed costs are high enough relative to variable costs, then we would only expect to see multi-vendor solutions when no single vendor can satisfy the risk threshold for all customers. As fixed costs (*F*) increase sufficiently, relative to variable costs (*V*), there is a drive towards a single

source solution. Then as the customers' risk tolerance threshold (*T*) decreases sufficiently, the solution moves toward more outsourcers to accommodate the increasingly stringent risk thresholds (see Table 1).

Threshold *T*	Solution Value	Execution Time in Seconds	Number of Vendors Used
1.000	253	36.783	1
0.900	350	55.169	1
0.800	350	51.024	1
0.700	350	49.391	1
0.600	350	17.114	1
0.500	424	29.162	1
0.400	599	59.666	2
0.300	641	43.302	2
0.200	895	62.420	3
0.100	1397	59.616	4
0.050	2041	19.749	5
0.025	4235	3.315	9
0.005	infeasible		
1.000	299	59.085	1
0.900	299	37.283	1
0.800	299	37.796	1
0.700	299	31.085	1
0.600	499	120.984	2
0.500	549	143.377	2
0.400	622	106.543	2
0.300	638	170.425	2
0.200	846	84.482	2
0.100	1312	147.802	4
0.050	2277	82.239	6
0.025	4557	5.198	11
0.005	infeasible		
1.000	301	48.149	1
0.900	316	40.838	1
0.800	316	38.766	1
0.700	316	16.864	1
0.600	361	34.990	1
0.500	405	67.788	1
0.400	575	66.836	2
0.300	677	66.105	2
0.200	968	107.464	3
0.100	1589	223.421	5
0.050	2254	26.879	6
0.025	4315	8.953	10
0.005	infeasible		

Table 1: Fixed Cost Only

Conversely, as fixed costs (*F*) decreases sufficiently, relative to variable costs (*V*), there is a move to the maximum number of outsourcers at all threshold levels (*T*) (See Table 2). In Table 2, fixed costs are zero and the risk threshold T_j is again held uniform for all customers *j*,

as T_j is varied from 1 down to 0.005. We use 30 vendors (*i*) and 20 customers (*j*) in Table 2. In order to minimize variable costs, the outsourcer that minimizes cost for each customer and account type will be utilized, and typically result in a very large number of utilized outsourcers over all threshold levels.

Threshold *T*	Solution Value	Execution Time in Seconds	Number of Vendors Used
1.000	173	3.315	30
0.900	175	1.933	30
0.800	186	2.634	30
0.700	193	1.862	30
0.600	203	1.322	30
0.500	221	1.382	30
0.400	249	1.402	30
0.300	275	1.172	30
0.200	378	1.031	30
0.100	665	0.701	30
0.050	1232	0.430	30
0.025	2433	0.421	30
0.005	infeasible		
1.000	183	1.382	30
0.900	193	2.684	30
0.800	202	2.453	30
0.700	207	2.414	30
0.600	222	1.843	30
0.500	236	1.592	30
0.400	256	1.522	30
0.300	313	1.963	30
0.200	450	1.032	30
0.100	711	0.781	30
0.050	1088	0.370	30
0.025	2147	0.461	30
0.005	infeasible		
1.000	155	1.022	30
0.900	161	1.512	30
0.800	170	1.792	30
0.700	176	1.171	30
0.600	190	1.702	30
0.500	210	1.382	30
0.400	249	1.553	30
0.300	293	0.912	30
0.200	433	1.032	30
0.100	782	0.721	30
0.050	1350	0.381	30
0.025	2091	0.340	30
0.005	infeasible		

Table 2: Variable Cost Only

The risk (*r*) emanates from the vendors, and similarly the cumulative risk (*R*) results from *r* and implicitly from the vendors. The risk tolerance threshold (*T*) for risk emanates from customers.

In Table 3, both fixed and variable costs are used with 20 vendors (*i*) and 10 customers (*j*). The set of three experiments shown in Table 3 allows the risk tolerance threshold T_j to vary by customer. In experiment one, the customer risk tolerance threshold for each customer (T_j) is a random number in [0..0.2]. In experiment two, the customer risk tolerance is a random number in [0..0.5], and in experiment three, the range is [0..1]. When fixed and variable costs are both present and relatively significant enough to impact the solution, we find that over a wide variety of risk thresholds, the pattern of the number of vendors used remains fairly unchanged.

Threshold (T) = random * 0.2

Solution Value	Execution Time in Seconds	Number of Vendors Used
4108	3.114	6
3378	1.402	5
5007	1.071	4
3054	2.604	4
3292	1.863	4
3841	2.614	4
4220	1.863	5
4043	2.784	6
4771	2.394	6
3886	2.203	4

Threshold (T) = random * 0.5

Solution Value	Execution Time in Seconds	Number of Vendors Used
2097	20.369	3
2776	16.303	4
2318	8.062	4
3229	6.960	4
3194	4.176	5
2281	5.128	3
2386	11.096	3
2903	4.626	4
2345	5.217	3
2705	23.714	5

Threshold (T) = random * 1.0

Solution Value	Execution Time in Seconds	Number of Vendors Used
4035	3.024	4
2771	2.343	4
2272	4.336	3
3025	1.352	4
3547	1.723	6
2295	9.283	4
2112	22.572	3
2434	3.075	4
2208	12.668	3
1791	47.168	3

Table 3: Both Fixed and Variable Cost

4.1 Discussion

Why is this problem different from the typical vendor selection problem? We have added risk, and risk impacts the solution significantly. The experimental results indicate that the number of vendors utilized in an outsourcing situation not only depends on the customer's risk tolerance threshold, but also on the cost structure. If fixed costs are dominant, the solution will

go to a single-source solution. As customer risk tolerance decreases in this situation, the number of vendors utilized will increase. If variable costs are dominant, the solution will drive toward the maximum allowable number of vendors as the cheapest solution is sought. This occurs over all levels of customer risk tolerance. When both fixed and variable costs impact the solution, then an intermediate number of vendors will typically result.

5. Conclusions

The protection of personal privacy is important to consumers. However, privacy is often at odds with security; too much privacy makes it difficult to identify threats to personal or national security. Laws try to balance the two needs, but the balance point is different for each country or culture.

Businesses are struggling to meet the demands of protecting the data they collect. Conflicting laws and cultural demands place an additional burden on companies trying to operating internationally and they need tools to minimize the burden of adhering to multiple laws. The ideal solution would be to create harmonized privacy laws internationally, but such a possibility is a long way off. For now, businesses are using detailed contracts and even multiple information systems to manage the conflicting demands.

Corporate Policy Implications

The model and Figure 1 indicate that security must be implemented across a firm's entire extended value chain. In an outsourcing environment, the firm needs to be aware of the security level of all partners. Individual firm security is only as good as the weakest link in the entire extended value chain of firms sharing data. Since data can be compromised at any point in the value chain, security must be managed across the entire extended network of service providers, be they auditors, couriers, product manufacturers, or government regulators. If your data is

compromised by one of your partners, your business may find itself liable, particularly in the perception of consumers. While it was UPS that lost the backup tapes in 2005 (Collett, 2005), it is Citigroup and Bank of America who suffer damage to their reputation. The lesson here is that firms must understand the controls in place at their vendors. A firm needs to know what happens to their customers' data once it leaves their immediate control. The model presented in this paper addresses this problem.

The model and computational testing clearly demonstrate to corporate information systems managers that it is important to consider the impact of customer-perceived risk and the customer's risk tolerance threshold on data sharing practices. Obviously cost structure has an impact on the number of outsourcing vendors with whom a corporation shares their customers' data. What is less widely recognized, and what is shown by the model and computational testing, is that risk can have a significant impact on the optimal quantity of outsourcing vendors with whom a firm should share sensitive data. In addition, the model and computational results clearly highlight the need to clearly track and monitor the security risks associated with the data security practices of all business partners in a firm's extended value chain.

It has been suggested that companies meet the demands of diverse privacy laws through contractual arrangements (Bessette & Haufler, 2001). This, however, is not an ideal approach as it can be difficult to enforce contractual rights across international boundaries as well (Bessette & Haufler, 2001). Just as a firm must be concerned about security along its extended value chain, consumers must be concerned with the security of all vendors in the chain, not just the firm they have direct contact with. Consumers expect the firm they deal with to protect their information and make their choices about risk on the totality of risk once they give their information to a firm, regardless of whether data processing is outsourced or not. However, this

approach may cause customers to over or under estimate the actual threat to their personal data. It has become important for consumers to look under the surface in order to fully understand their risk exposure.

Governmental Policy Implications

We conclude that regulating security in a single jurisdiction, such as Canada, will be largely ineffective since information outsourcing is global in nature and information is often subject to laws in other jurisdictions. USA PATRIOT has brought this issue into sharper focus over the last five years.

Taking unilateral action to block unwanted data access glosses over the multinational aspects of data flows. To regulate privacy and security in a single jurisdiction, significant value chain efficiencies may be forfeited. Imposing such inefficiencies on a firm's value chain by imposing arbitrary security and privacy thresholds for risk tolerance makes the firm less competitive globally.

Results from the model and computational testing support the idea that a firm's risk does, and, by extension their security policy, should extend beyond the firm's traditional boundaries to include the entire value chain that has been given access to sensitive customer data. Given the sensitivity to risk shown in the experimental results, it would be reasonable for national policy on data security to extend over the entire extended corporate data value chain. In other words, corporate responsibility regarding data security should not be shielded by the supposed Chinese Walls regarding data security of an extended value chain. This is especially true since in the case of data outsourcing the extended value chain may often lie in a foreign jurisdiction.

Coordination of security and privacy policy across closely tied trade jurisdictions, such as Canada and the U.S., helps to ensure that value chain inefficiencies are not artificially imposed

on the smaller trading partner. Canada has already adopted the EU's stance on protection of privacy even though, culturally, Canadians may fall closer to embracing the U.S. position on privacy (Bellman et al, 2004; Milberg et al, 1995). For now, the Canadian government recommends that companies include a privacy protection clause in contracts with third parties as the way to ensure the same level of privacy protection across multiple firms (Office of the Privacy Commissioner of Canada, 2004). Bessette and Haufler (2001) state that civil liberties groups prefer the contractual approach to increased regulation, but that a centralized mechanism to deal with disputes when the contractual obligations are not met is needed. However, if such a centralized mechanism were created, the contractual approach to protecting personal privacy would be more easily implemented than trying to have every nation agree on the same regulatory regime for protection of personal privacy.

A significant point to this paper is to demonstrate that security breaches have network effects; information from multiple sources, often publicly available, can now be combined to breach tolerable thresholds of privacy and security. For example, a quick search on a name will piece together information from a variety of sources. Thus, regardless of regulations or contracts, it may still be possible for an individual to lose control of their personal privacy.

Bibliography

1. Aldhouse, F., "The Transfer of Personal Data to Third Countries Under EU Directive 95/46/ec." International Review of Law, Computers & Technology, Vol. 13, No. 1, 1999, p.75.
2. Baumer, D.L., J.B. Earp, and J. C. Poindexter. "Internet Privacy Law: A Comparision between the United States and the European Union." Computers & Security, Vol. 23, No. 5, 2004.
3. Bellman, S., E. Johnson, S. Kobrin, and G. Lohse, "International Differences in Information Privacy Concerns: A Global Survey of Consumers." Information Society, Vol. 20, No. 5, 2004.
4. Bessette, R., and V. Haufler. "Against all Odds: Why there is no International Information Regime." International Studies Perspectives, Vol. 2, No. 1, 2001, pp. 69-92.
5. Cate, F.H., Legal Restrictions on Transborder Data Flows to Prevent Government Access to Personal Data: Lessons from British Columbia. The Centre for Information Policy Leadership, 2005. Date accessed: July 15, 2006 (http://www.hunton.com/files/tbl_s47Details/FileUpload265/1260/Legal_Restrictions_Transborder_Data_Flows.pdf).
6. Collett, S., "Precious Cargo." CSO Magazine, August, 2005. Date accessed: April 24, 2006 (http://www.csoonline.com/read/080105/cargo.html).
7. Douglas, M., and A. Wildawsky, "Risk and Culture: An Essay on Selection of Technological and Environmental Dangers," University of California Press, 1982.
8. Jablonski, M.A., Bill 20: Freedom of Information and Protection of Privacy Amendment Act, 2006. Trans. Legislative Assembly of Alberta. Bill ed. Vol. 20. Alberta: Alberta, 2006. Legislative Assembly of Alberta. Date accessed: March 27, 2006 (http://www.assembly.ab.ca/net/index.aspx?p=bills_status&selectbill=020).
9. Johannes, R., Identity Fraud Survey Report. Ed. Mary T. Monahan. Consumer Version ed. Pleasanton, CA: Javelin Strategy and Research, 2006. Date accessed: March 27, 2006 (http://www.javelinstrategy.com/research).
10. Jones, J., and P. Meller, "U.S., E.U. Divided on Standards." InfoWorld, Vol. 23, No. 14, 2001.
11. Klosek, J., "Data Privacy and Security Are a Significant Part of the Outsourcing Equation", Intellectual Property and Technology Law Journal, Vol. 17, No. 6, 2005, pp. 15-18.
12. Loukidelis, D., "Privacy and the USA Patriot Act Implications for British Columbia Public Sector Outsourcing," British Columbia, Office of the Information and Privacy Commissioner. October 2004. Accessed on 9/14/06 at:

http://www.oipcbc.org/sector_public/usa_patriot_act/pdfs/report/privacy-final.pdf#search=%22bc%2Bprivacy%20report%22

13. Meinert, D., D. Peterson, M.D. Crossland, and J. Criswell, "Privacy Policy Statements and Consumer Willingness to Provide Personal Information." Journal of Electronic Commerce in Organizations, Vol. 4, No. 1, 2005.
14. Milberg, S.J., S.J. Burke, H.J. Smith, and E.A. Kallman, "Values, Personal Information Privacy, and Regulatory Approaches."Communications of the ACM, Vol. 38, No. 12, 1995, pp. 65-74.
15. Murray, J., Freedom of Information and Protection of Privacy Amendment Act. Trans. Legislative Assembly of British Columbia. Vol. Bill 73, 2004. Date accessed: April 24, 2006 (http://www.legis.gov.bc.ca/37th5th/1st_read/gov73-1.htm).
16. Neil, M., "Thinking Globally." ABA Journal, Vol. 91, 2005.
17. Office of the Privacy Commissioner of Canada. *PIPEDA* Case Summary #313: Bank's Notification to Customers Triggers *PATRIOT Act* Concerns. Vol. PIPEDA Case Summary #313. Ottawa, CA: Canada, 2005. Date accessed: July 15, 2006 (http://www.privcom.gc.ca/cf-dc/2005/313_20051019_e.asp).
18. Office of the Privacy Commissioner of Canada. Your Privacy Responsibilities., 2004. Date accessed: July 15, 2006 (http://www.privcom.gc.ca/information/guide_e.pdf).
19. OECD (Organisation for Economic Co-operation and Development). "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." Organisation for Economic Co-operation and Development. September 23, 1980. Date accessed: March 27, 2006 (http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html).
20. Ponemon, L., "The Value of Protecting Customer Privacy." CXO Media Inc., 2006. Date accessed: January 15, 2006 (http://www.cio.com/archive/011506/ti_numbers.html).
21. Privacy & American Business and Deloitte & Touche LLP, "New Survey Reports An Increase In ID Theft And Decrease In Consumer Confidence." Press Release, 2005. Accessed on 9/14/06 at:. http://www.pandab.org/deloitteidsurveypr.html
22. Robinson, C., "Collecting Effective Security Metrics", csoonline.com, April 9, 2004. Accessed on 9/14/06 at: http://www.csoonline.com/analyst/report2412.html
23. Rudraswamy, V., and D.A. Vance. "Transborder Data Flows: Adoption and Diffusion of Protective Legislation in the Global Electronic Commerce Environment." Logistics Information Management, Vol. 14, No. 1&2, 2001.
24. Slovik, P., B. Fischhoff, and S. Lichtenstein, "Facts and Fears: Understanding Perceived Risk" in R.C. Schwing and W.A. Albers, Jr. (Eds.), *Societal Risk Assessment: How Safe is Safe Enough*, pp. 181-214. New York-London: Plenum Press, 1980.
25. Slovik, P., "Perception of Risk", Science, Vol. 236, 1987, pp. 280-285.

26. Slovik, P., “Perception of Risk: Reflections on the psychometric paradigm”, in S. Krimsky and D. Golding (eds.) *Social theories of risk*, pp. 117-152, Westport: Praeger Publishers, 1992.
27. Smith, J.H. and E.A. Kallman, “Privacy attitudes and practices worldwide: an empirical study of the ISACA membership”, The Information Systems Audit and Control Foundation, Inc., Research Monograph Series, No. 8, 1996, pp. 40-41.
28. Sutton, S.G., Extended-enterprise systems’ impact on enterprise risk management”, Journal of Enterprise Information Management, Vol. 19, No. 1, 2006, pp. 97-114.
29. Tafti, M.H.A., “Risks factors associated with offshore IT outsourcing”, Industrial Management and Data Systems, Vol. 105, No. 5, 2005, pp. 549-560.
30. U.S. Department of Commerce, Export Portal, "Safe Harbor," 2006. Date accessed: July 15, 2006 (http://www.export.gov/safeHarbor/index.html.)
31. Yu, E., and L.M. Cysneiros. "Designing for Privacy in a Multi-Agent World." Trust, Reputation and Security: Theories and Practice. Ed. R. Falcone, et al. 1st ed.Springer-Verlag, 2003. Date accessed: July 15, 2006 (http://www.cs.toronto.edu/~cysneiro/articles/LNAI06-Privacy.pdf).