Journal of Business Ethics (2009) 88:579–594
DOI 10.1007/s10551-009-0312-9
© Springer 2010

CSR and the Corporate Cyborg: Ethical Corporate Information Security Practices

Andrea M. Matwyshyn

ABSTRACT. Relying heavily on Thomas Dunfee's work, this article conducts an in-depth analysis of the relationship between law and business ethics in the context of corporate information security. It debunks the two dominant arguments against corporate investment in information security and explains why socially responsible corporate conduct necessitates strong information security practices. This article argues that companies have ethical obligations to improve information security arising out of a duty to avoid knowingly causing harm to others and, potentially, a duty to exercise unique capabilities for the greater social good and to buttress stable functioning of social institutions.

KEY WORDS: corporate governance, corporate social responsibility, information security, identity theft, non-disclosure

Andrea M. Matwyshyn is an Assistant Professor of Legal Studies and Business Ethics at the Wharton School at the University of Pennsylvania. Her research focuses on the intersection of business, technology, and information security regulation. Before joining the University of Pennsylvania as a faculty, she taught at University of Florida, where she also ran an interdisciplinary research center on information security, law and business, and at Northwestern University School of Law. She has been a research affiliate of the University of Cambridge Center for Industry and Governance and a visiting research scholar at the University of Edinburgh School of Law and Singapore Management University School of Law. She is regularly cited in the popular press as an expert in the field of corporate information security and internet contract law. Her most recent work includes editing a the book is now out book on corporate information security best practices and law called ''Harboring Data: Information Security, Law and the Corporation'' (Stanford Press, Sept. 2009). A portion of her articles can be found at http://ssrn.com/author=627948.

Introduction

Information is ''the new corporate currency,''[1] and its management is the new corporate challenge. However, many companies are struggling with this new challenge: corporate information leakage is rampant. As corporate assets have progressively shifted toward intangibles over tangibles,[2] the value of these assets has become increasingly contingent on the security of the systems housing corporate information. Strong corporate information security has, therefore, become an integral part of good management – a necessity for retaining and building the value of key corporate assets. Yet, in practice it appears to be deficient among many companies.

Although law is still nascent in the area of corporate information security regulation, strong ethical arguments exist for aggressive improvements in corporate data control practices, even in advance of regulation. Throughout his work, Thomas Dunfee explicitly rejected the idea that law and business ethics necessarily converge and called for more in-depth analysis of the relationship between law and business ethics in context of particular issues and corporate social responsibility.[3] Relying heavily on Dunfee's work, this article seeks to conduct in-depth analysis of the relationship between law and business ethics in the context of corporate information security. It debunks the two dominant arguments against corporate investment in information security and explains why socially responsible corporate conduct necessitates strong information security practices. This article argues that companies have ethical obligations to improve information security arising out of a duty to avoid knowingly causing harm to others and, potentially, a duty to exercise unique capabilities for the greater social good and to buttress stable functioning of social institutions.

Today's corporate cyborg, the information economy and information security

As the types of assets that dominate many companies have moved away from tangibles toward intangibles,[4] corporate structure has also evolved. Internal corporate information flows are increasingly mechanized through computerization; externally, however, corporations work to maintain a human face to build brand and customer loyalty. On the one hand, companies are struggling with growing into heavily technology-driven structures of information management,[5] but on the other, they still view the external projection of human characteristics of foremost business importance. In other words, today's corporation has changed itself into a type of ''cyborg'' – a creature that is half machine and half human.

Information management and computer systems are driving dramatic change inside companies. Since Time Magazine named ''The Computer'' as its person of the year in 1983,[6] corporations' reliance on information systems has increased significantly, as have the capabilities of those systems. This integration of information technology into corporate operations during the last two decades has changed the ways that companies handle information – both sensitive internal information and personally identifiable consumer information. Companies have increasingly centralized sensitive corporate information[7]: trade secret information,[8] financial information,[9] business partner and customer information is centralized in companies' internal computer systems. Further, as internet purchases became a regular part of consumer economic behaviors in the late 1990s, a new economic environment emerged. The defining characteristic of this new commercial environment has been widespread corporate collection, aggregation, and leveraging of personally identifiable consumer data with the assistance of information systems.[10] More than ever before, corporate entities see commercial opportunities in the wealth of readily available personally identifiable consumer data; companies place a premium on consumer information databases and have changed the way consumer data is valued in corporate acquisitions.[11] Many companies today data hoard for marketing and other purposes. They collect as much information as possible about their customers in the name of targeting products more effectively and generating secondary streams of revenue through licensing their databases of consumer information.[12]

Meanwhile, corporations have simultaneously gone to great lengths to externally humanize themselves to generate consumer trust and brand loyalty. They engage in philanthropy[13] and advertise in ways that are intended to create emotional connection between the brand and the customer.[14] Recently, these advertising outreach efforts have extended to social networking websites such as Facebook. In 2008, approximately $1.6 billion was spent on US online social network advertisements.[15] Business enterprises have pages, ''friends,'' fans, and send and receive messages. If content creation can be used to judge impact, these personification efforts appear to be working – hundreds of user-generated ''fan'' pages to companies, products and corporate officers and corporate characters have been created.[16]

This duality in corporate identity – internal mechanization in context of external humanization – has given rise to new ethical and legal concerns. Companies increasingly rely on computer systems; yet, they do not necessarily understand their dangers and the new types of business risks these systems introduce. Consequently, rather than projecting the ''trustworthy'' human face they seek to project, companies frequently unintentionally generate an untrustworthy one. Shortfalls in corporate information security and data-handling practices illustrate this tension and its unintended negative consequences. As the negative publicity following information security breaches at companies such as the TJX Companies[17] and Heartland[18] demonstrates, mismanagement of information systems can dramatically undercut the efforts of a company to build a trusted human face with the outside world. Yet, empirical data demonstrates that companies are not anticipating and managing information risk. For example, in 2008, in an annual information security survey by Pricewaterhouse Coopers of over 7,000 respondents who comprised CEOs, CFOs, CIOs, CSOs, vice presidents and directors of IT and information security from 119 countries, at least three of ten respondents could not answer basic questions about the information security practices of

their organizations. 35% did not know the number of security incidents in the last year; 44% did not know what types of security incidents presented the greatest threats to the company's most sensitive information, assets, and operations; 42% could not identify the source of security incidents; 67% said their organization does not audit or monitor compliance with the corporate information security policy – whether the attack was most likely to have originated from employees (either current or former), customers, partners or suppliers, hackers, or others.[19] Rampant data breaches of millions of records in 2008 further speak for themselves, demonstrating widespread inadequacies in corporate information handling.[20] Each of those breached records is attached to a company or a consumer potentially harmed by the disclosure.

As information control issues present novel challenges for most enterprises, debates have arisen inside entities regarding duties of information care owed to the corporation, its shareholders and the consumers and partners whose data is housed in the company's databases. On the one hand, data security champions argue that maintaining best practices in information security within the enterprise is "the right thing to do" both for the company and society as a whole. On the other hand, data security skeptics argue that short term expenditures on such "nonessential" items should be curtailed. The sections that follow seek to provide the articulation for the data security champion's argument – that strong corporate information security is indeed "the right thing to do." Section "Why weak information security is socially irresponsible conduct" challenges the two main arguments of the information security skeptics that they are already acting responsibly without investing in information security – first, that simply complying with current information security law constitutes acting responsibly and, second, that the obligations imposed by corporate law and their duties to their shareholders restrict the ability to make large investments in information security internally. Section "Why strong information security is socially responsible corporate conduct" next argues that a socially responsible corporation is one which considers not only the impact of its real-space practices, but also the social impact of its information practices on its stakeholders.[21]

Why weak information security is socially irresponsible corporate conduct

Proponents of stronger information security face internal corporate tensions with regard to setting of corporate priorities and investment levels.[22] The primary objections raised by information security skeptics to curtail spending on information security improvements fall along two lines – first, that doing the "right thing" simply means complying with law, and second, that seeking to maximize shareholder returns negates the ability to spend on such "non-essential" items as information security.[23]

> "We are complying with legal requirements on information security practices and data breaches; by definition, that means we are doing enough."

Perhaps, the first objection raised by internal corporate information security skeptics involves the law. They assert that acting responsibly for a business entity in the area of information security simply means complying with the law; they assert the law defines for them what constitutes good business practices.[24] This objection fundamentally misunderstands the relationship between responsible corporate conduct and legal regulation. Throughout his work, Thomas Dunfee explicitly called for more in-depth analysis of the relationship between law and business ethics in context of particular issues, and he rejected the idea that law and business ethics necessarily converge.[25] Pointing to examples such as the unjust law, he cautioned against relying on law as the only source for articulating responsible corporate conduct.[26] This caution is well-heeded in the context of information security regulation. Although both U.S. and international regulators are beginning to take action in the realm of information security regulation, legally speaking, the field of information security regulation is in its infancy. It is barely a decade old in the United States, doctrinally inconsistent, and in a state of flux.[27] It is only since 1996 that questions of data security and privacy have begun to gain momentum as issues of heightened legal and national importance within the United States, partially as a result of international influences.[28] Despite the E.U.'s more aggressive[29] stance toward data protection, the United States did not have any

consumer information security legislation[30] in effect until April 2000.[31]

To date, the information security legal regime adopted in the United States to address issues of corporate data vulnerability is an imperfect patchwork of state and federal laws, widely critiqued in legal scholarship.[32] On the federal level, health data, financial data, and children's data are statutorily regulated, through the Health Insurance Portability and Accountability Act,[33] the Gramm-Leach-Bliley Act,[34] and the Children's Online Privacy Protection Act,[35] respectively. However, not all business entities are currently proactively regulated by information security statutes, and much of information crime involves data not necessarily deemed particularly ''sensitive'' by federal statutes at present. Many entities that aggregate large amounts of information do not fall into any of the legal categories of statutorily restricted data. The biggest economic losses arise not out of illegal leveraging of the statutorily protected categories of data; rather, the biggest losses arise out of stolen personally identifiable information frequently not protected by federal law, such as social security numbers and credit card information. On the state level, state data breach notification laws have been passed in most states during the last 3 years. Currently, approximately 44 states, the Washington DC, and Puerto Rico have data security breach notification statutes on their books.[36] Generally speaking, these notification statutes compel entities who have suffered ''data breaches''[37] to provide written notice to the consumers whose data has been impacted. However, significant variation exists across data breach notification statutes and their presence has empirically failed to mitigate the rate of data breaches.[38] Meanwhile, data breaches are escalating not only in frequency but also in severity.[39] Therefore, it is fair to assert that law is not adequately addressing information security problems in corporations at the present time. Socially responsible corporate conduct beyond that mandated by information security law is warranted by the nature of the information security problems the corporate sector faces.

Further, companies may assume their legal compliance in error, thinking only information security-specific regulation generates legal duties of data care for the company. Although it is true that information security legal doctrine is underdeveloped at the present time, other bodies of law pertain as well, especially to the corporation's officers and directors. In fact, poor information management among U.S. corporations[40] quickly approaches a level of neglect that may violate fiduciary duties.[41] Owing to the implications of weak information security for the integrity of corporate financial reporting processes in particular, it can be argued that the levels of information security mismanagement among U.S. companies today approach the levels that trigger a breach of fiduciary duty under the *Caremark/Stone* standard under Delaware law. *In re Caremark Int'l Inc. Deriv. Litigation*[42] held that corporate directors' ''liability to the corporation for a loss may be said to arise from an unconsidered failure of the board to act in circumstances in which due attention would, arguably, have prevented the loss,'' if they were guilty of ''such an utter failure to attempt to assure a reasonable information and reporting system exists'' as would establish a lack of good faith.[43] The Delaware Supreme Court endorsed and elaborated this standard in *Stone v. Ritter*,[44] and recently, a Delaware bankruptcy court has also extended the Caremark duty to corporate officers.[45] Thus, in Delaware directors and officers may be liable for their mere omissions if (1) the directors fail to implement a reporting and information system knowing that they should have done so, or (2) having implemented such a system, they consciously failed to monitor or oversee its operations.[46] The extent of neglect by directors and officers overseeing corporate information security practices is approaching this point of liability articulated in *Caremark/Stone*. Further, Sarbanes–Oxley Act Section 404 requires that officers provide certification of the integrity of information contained in financials.[47] Accurate certification of the integrity of information cannot occur in a culture where information security is lax: where access to alter corporate information is easy to obtain, no guarantees of integrity are actually possible.

Information security presents a sphere of corporate decision making in line with concerns articulated in Dunfee's work: the law is currently inadequate to limit harms to third parties from corporate information security conduct, yet the harms are undeniable. As such, the ethical duty not to harm creates the stronger articulation of acceptable corporate information security conduct than does the current legal standard. According to

Thomas Dunfee, a high degree of trust is placed in the hands of directors of corporations. For Dunfee, directors of companies are some of the most important fiduciaries in society. Failure by directors to fulfill their role properly can lead to disastrous consequences for many stakeholder groups. Consequently, a duty not to harm others applies to their decision making and the corporate conduct they authorize. Dunfee argued that based on this moral duty of doing no harm to others, the potential negative consequences of directors' actions or inaction suggest that reference to the law alone for standards is simply not sufficient. A higher set of ethical concerns should prevail in corporate decisions.[48]

Thus, legal compliance by itself does not indicate responsible corporate information security conduct. In light of the current state of corporate information security regulation, corporate information security conduct may be legally compliant, yet result in significant harm to both the corporation itself, its shareholders, partners and other stakeholders; these harms are explained in the next section. Further, companies may misunderstand the current state of the law and presume compliance in error.

> "Our need to maximize returns for our shareholders prohibits investments in information security for the good of other stakeholders."

Perhaps the strongest argument of corporate information security skeptics is rooted in cost. They assert that because investments in information security are allegedly nonessential, spending on strong information security conflicts with the duty of the company to maximize returns for shareholders. The return on investment in security is not necessarily visible in the short term, and therefore, this type of an investment allegedly squanders corporate assets that could be better utilized to generate strong short-run returns for shareholders. However, this erroneous belief arises from a lack of understanding of the long-term negative consequences to corporate assets when information security is inadequate. In 2007, the average cost of a data breach rose to $6.3 million from $4.8 million in 2006.[49] Information security improvements are unlikely to reach this level of expense. But, from the standpoint of responsible corporate conduct, acting responsibly toward shareholders, first and foremost, involves not causing harm to shareholders. Causing harm to corporate assets when prevention was reasonable and possible harms the value of shareholders' investments. In other words, the proper calculus with respect to shareholders in this context is whether the company is likely to cause easily avoidable harm to its shareholders by choosing to ignore information security risks. The answer is almost always a resounding yes.

Security breaches diminish the value of corporate assets and usurp resources; the value of each corporate record compromised is currently estimated by some researchers to be $202.[50] Certain corporate assets, such as databases of customer information and preferences, are valuable only because of their confidentiality.[51] One data breach could greatly diminish the value of such an intangible asset.[52] For example, the damage that a corporate insider can generate in one episode of information theft has been, in at least one instance, approximated to be between $50 million to $100 million.[53] Similarly, corporate proprietary information protected solely by trade secret law could lose all value in an information crime incident because the information's status as a trade secret is entirely contingent upon its confidentiality.[54] Corporate integrity is further affected by a parallel diminution in brand value and corporate goodwill. A company considered to be vulnerable generally suffers a decrease in the value of its investments in brand identity building because it breaches its explicit and implicit promises of data care. A brand can become tainted in the minds of business partners and consumers if it is associated with lax information security.[55] Finally, if a security incident results in a consumer data privacy violation, availability of capital is further diminished because of the subsequent need to cover fines, court costs, attorneys' fees, settlement costs, the bureaucratic costs of setting up compliance mechanisms with consent decrees, settlement agreements, and court decisions.[56] Further, external attackers are highly motivated: information thievery is highly lucrative.[57] By some estimates, the information crime economy is now equally or more lucrative than the drug economy for its participants.[58] As corporate databases of personally identifiable information become larger, they become progressively more attractive targets for information criminals for purposes of

identity theft and extortion. Organized crime syndicates have begun launching extortion rackets against businesses, threatening them with attacks from zombie drones, armies of security compromised corporate and user machines.[59] Depending on the size of the army of zombie drones, such an attack could cripple a business and disrupt operations for an extended period of time. Alternatively, the target of an attack using compromised corporate machines could be a government agency, turning compromised machines into instruments of cyber warfare. Meanwhile, the consumers attached to the data residing in the machines or databases under attach may suffer irreparable harm.

Therefore, responsible corporate conduct requires more than simply comporting conduct with the lowest possible floor set by law. As discussed, a company's ignoring information security concerns can hold dire consequences – irreparable damage to corporate assets. As the next section explains, failure to consider the information security consequences of corporate decisions violates the ethical duty to avoid causing harm to corporate stakeholders.

Why strong information security is socially responsible corporate conduct

Increasingly, scholars and managers alike recognize the existence of core standards of business ethics applying to all commercial activities.[60] They encompass factors such as acting honestly and in good faith. They warn against conflicts of interest, require the exercise of due care, and emphasize fairness and just results. In *The Marketplace of Morality*, Thomas Dunfee argued that morality is expressed within markets and may result in pressures on organizations to respond. He delineated three categories of morality firms encounter – Benign, Disputed, and Problematic. Benign morality refers to moral desires which are unarguably consistent with most ethical principles and with which most people agree. Disputed morality involves beliefs that cannot be validated by a general consensus of ethical analysis, involving moral desires that reflect one side of a hotly contested social issue. Problematic morality refers to expression of morality inconsistent with well-established, widely recognized moral principles. Dunfee argued that if the morality expressed creates an obligation on the firm, then the firm should comply and take steps to bring organizational practices and standards into compliance with the identified morality. Particularly if the morality is Benign and demands action of the firm, the firm should act.[61]

Applying this lens to the issues surrounding corporate information leakage and vulnerability, it becomes clear that corporate neglect in maintaining best practices in information security constitutes conduct that runs afoul of perhaps the most basic of Benign moral concerns – the duty to avoid harming others. Further, Dunfee argued that in the rare instances where a particular firm possesses a key capability, a duty may exist to exercise these unique capabilities for the greater social good. The current state of widespread information security inadequacies is beginning to threaten the continued stability of some of our social institutions.

Strong information security protects against harming stakeholders impacted by corporate self-harm

As described in previous sections, certain types of information security mistakes are recurring inside companies, resulting in harms to shareholders and consumers as a consequence of harm to corporate assets. The five most common information security errors visible today in corporate information security risk management include the following: a lack of information security planning overall,[62] nonresponsiveness to external reports of breaches,[63] inadequate partner vetting and voluntarily granting criminals access to information,[64] theft by rogue employees,[65] and a failure to update existing security.[66] Thomas Dunfee's work offers two useful approaches to mitigating harm to shareholders due to corporate information security self-harm: (1) setting a tone of information care by the corporation's leaders and (2) crafting a strong code of information security conduct.

Setting a tone of information care by the corporation's leaders

Companies whose officers and directors value information security create a top-down culture of data care. As Dunfee argued, the ethical behavior of

a corporation's leaders tends to have an impact on the ethical behavior of other corporate agents.[67] The officers and directors act as "ethical role models" for others inside the company.[68] The organizational literature demonstrates the importance of senior executives[69] and board members in influencing the ethical behavior of lower level employees. Therefore, simply through the officers and directors of a company articulating through words and actions that information security and ethical data handling practices are a corporate priority, a trickle-down shift in information security attitudes should occur.

According to annual longitudinal research by Pricewaterhouse Coopers, many company leaders lack a well-rounded view of their information security compliance activities: "business and IT executives may not have a full picture of compliance lapses. Fewer than half of all the respondents say their organization audits and monitors user compliance with security policies (43%)"[70] and "only 44% conduct compliance testing."[71] Part of the challenge these corporations face exists in building security into a legacy environment unfamiliar with information security principles. Omissions in technology management can harm as much as commissions, and viral unintended problems harm not only the company but also its partners, customers, and the public at large. Room for improvement exists in building top-down corporate cultures of strong information security.

Crafting a strong code of information security conduct

Research demonstrates that the existence of corporate codes of conduct or corporate policy statements on ethical behavior has been found to be significantly related to ethical behavior.[72] In particular, codes which clearly stipulate standards for information security conduct and sanctions for data mishandling are likely to generate more ethical conduct on the part of employees with regard to data care, preventing corporate information self-harm. A corporate code of conduct should explicitly address information security and set forth a set of information security processes. Codes should designate key individuals responsible for security risk management and establish clear lines of communication for reporting internal and external security breaches. Self-assessment on a regular basis is also an important component of responsibility.[73] In particular, as Dunfee stressed in his work in other contexts,[74] directors need to create room for whistleblowing. In instances where corporations are not internally motivated to correct their information security mistakes, whistleblowers have and will continue to provide a useful source of information to protect society from otherwise unknown vulnerabilities.

Both legal and ethical factors warrant explicit inclusion of information security concerns in corporate codes of conduct. As discussed previously, Sarbanes–Oxley Act Section 404 requires officer certification of the integrity of financial statements. Meanwhile, Section 406(a) requires companies to adopt a code of ethics for senior financial officers, or to indicate the reasons why a code of conduct does not exist. These two sections working together seem to logically call for inclusion of information security in corporate codes of conduct. Further, should a violation of federal law be found, the existence of an information security code of conduct would mitigate sentencing. Under the U.S. Federal Sentencing Guidelines for Organizations, a company found to have an "effective compliance program" in place prior to a violation of federal law including, among other elements, a code of conduct or ethics, ethics training, an ethics officer, and a reporting system, may result in mitigated fines.[75] A corporate code of conduct that expressly addresses information security signals that weak information handling practices, such as unauthorized sharing and careless information storage, is negative. In this manner, a well-crafted code of conduct instructs employees that information security breaches are to be fastidiously avoided.

Strong information security avoids knowingly causing harm to all corporate stakeholders and the system as a whole

Recent scholarship on the concept of corporate citizenship[76] indicates that many scholars have come to treat business as embedded in, not apart from, society.[77] They assert the importance of broader social context and believe that responsibilities of business cannot be understood solely through the bilateral relations between the company and the parties with which it interacts.[78] Dunfee argued, for

example, that directors are obligated to ensure that their companies act as good citizens and that citizenship involves decision making that protects the community and does not involve unnecessary harm to it. He asserted that this core ethical value is emphasized by all of the various sources of ethical standards, as well as by legislation such as the Federal Sentencing Guidelines, the Caremark case, and the Sarbanes–Oxley Act.[79]

During 2008, estimates indicate that corporations were the biggest source of consumer information leakage, compromising over 35% of reported data breaches.[80] It is undisputable that lax corporate information security erodes commercial trust and imposes costs on third parties – business partners, shareholders, consumers, and the economic system as a whole. The reason for this transference arises from the nature of information risk: the impact of information risk is inherently transitive. This transitivity means that if a company shares sensitive corporate information with a careless business partner and that partner experiences a data leakage, the negative effects to the shared data are similar to those that would have occurred if the original company had been breached itself.[81] Similarly, if a company possesses a business partner's or a consumer's sensitive information and experiences a breach, the company imposes costs on the information subject to the same extent as if the information subject itself was breached. When a business partner's sensitive data is compromised, a breakdown of commercial trust occurs and both entities may suffer public relations consequences and information asset devaluation.

Data breaches impose costs on the economy and society as a whole. Information stolen from corporations about individual shareholders or consumers is sometimes used for purposes of identity theft. For example, individuals take it for granted that they may participate in the social institution of real property ownership provided that they maintain a good credit report. However, an identity theft victim frequently realizes the extent of his/her victimization only at the point of attempting to obtain a mortgage. At this juncture, a credit report is run and the victim learns that a fraudster has stolen the individual's identity and has already taken out a mortgage in the victim's name.[82] Until the effects of the crime are effectively remedied, property ownership is foreclosed to the victim. When an individual is victimized by identity theft, losses suffered include economic harms from being held responsible for transactions undertaken in the individual's name and potentially a negatively impacted credit score. Further, many individuals feel a dignitary harm arising from a perceived invasion of privacy. Thus, consumers victimized by information security-related crime suffer both economic integrity harms and the negative psychological feeling of helplessness frequently associated with crime.[83] For shareholders, corporate information vulnerability also means that their investment is impacted – the value of assets of the company in which they have invested diminishes.

Further, harms to social institutions occur. The social security system, for example, has been destabilized in part due to rampant social security number vulnerability.[84] A compromise of individuals' social security numbers can result in fraud, which then requires the expenditure of social resources. In addition to the costs of prosecution, such frauds further necessitate the incurring of transaction costs associated with issuing new social security numbers to victims and eliminating the old numbers from the social security rolls. Similarly, the integrity of social structures, such as law enforcement and the criminal justice system, is negatively impacted by information crime. Identity thieves may sometimes identify themselves using a victim's identity when being charged with a crime.[85] Discovering this misidentification of the criminal and clearing up the consequential damage to the victim's record similarly usurps both social and law enforcement resources. Lending practices are destabilized when identity thieves rather than consumers seek mortgages in consumers' names using data obtained through compromising a corporate database. As such, a duty to minimize harm to others includes minimizing damage to social systems caused by corporate information vulnerability.

This duty not to harm can be operationalized in corporate information security practices in at least two ways. First, it includes timely, fair, and accurate disclosure of the existence of security vulnerabilities that put consumers, partners, and the social system at risk to enable these impacted parties to mitigate their exposure to information risk. Second, it involves due care in updating information security practices to stay in step with the state of the art in best practices.

Duty to disclose existence of vulnerabilities and breaches to prevent further harm

A need for timely, fair, and accurate disclosure of the existence of corporate information security problems arises from the duty not to harm. Informing business partners and consumers of the existence of a vulnerability – even before it has been exploited by a malicious third party – and the affirmative steps underway to correct it buttresses commercial trust. Failure to disclose when harm was avoidable, conversely, diminishes commercial trust. Although the law varies on who must disclose information breaches and the permissible timeframe, the duty not to harm compels more aggressive disclosure than that required by law. By the time the disclosure is legally mandated, irreparable harms have usually occurred.

In Thomas Dunfee's research on optimal corporate disclosure practices, he found that the impetus behind many corporate disclosures may be a legitimacy-threatening event, such as a crisis involving negative press coverage. Second, argued Dunfee, when firms disclose information, it may be strategically oriented to repair lost goodwill.[86] Dunfee argued in favor of what he termed "Optimal Truthful Disclosure" where corporations should produce information up to the point where the marginal costs of production are equal to or less than the marginal benefit provided to society.[87] Dunfee asserted that it is not optimal to require stakeholders themselves to collect information when doing so would be significantly more costly than disclosure by the firm. He asserted that firms tend to provide less than optimal disclosure when liability rules and incentives are not aligned with the value of accurate information, on the one hand, and the cost of misleading information, on the other hand. These concerns raised by Dunfee fit the dynamics of corporate information security breach and vulnerability disclosure.

As the press and consumers become more sensitive to the risks of information breaches and identity theft, the costs of both of these dynamics will escalate for companies. Consumer behavior following recent data breaches indicates that a breach is perceived by consumers as a trust violating event.[88] For example, one internet jobseeker website that has suffered several data breaches in the last few years was the target of press and consumer backlash in response to a perceived lack of full disclosure. Although the company asserts it fully complied with any applicable data breach notification statutes, press reports indicate that, even assuming this compliance, the company took multiple days to inform the public of an ongoing breach, and during this time additional consumers may have been harmed.[89] Even though this type of delay was legally permissible, the press and consumer reaction to the perceived failure in timely disclosure was nevertheless strongly negative.[90] Information regarding corporate information security vulnerabilities and practices is costly or impossible for stakeholders to acquire. Simultaneously, however, it is valuable to stakeholders who want the information to make better decisions on investments, consumption purchases, employment choices, and the determination of public policy. Liability for information security breaches has been minimal and causes of action have been slow to emerge. Meanwhile, databases of aggregated consumer information are a key asset for many entities used to derive revenue streams through licensing. Just as most companies would recall a product known to poison their customers, companies should similarly take steps to warm of information security problems and to avoid knowingly exposing their business partners, shareholders, and customers to avoidable information risks. Vulnerable databases, websites, and business practices can result in information harms – compromised corporate information, stolen identities, and hijacked machines used for nefarious purposes.

Duty to update information security practices to avoid harm

In *Ties that Bind*, Thomas Dunfee and Thomas Donaldson introduced the idea of a new approach to business ethics that exposed the implicit understandings or "contracts" that bind industries, companies, and economic systems into moral communities.[91] All particular or "micro" social contracts on the corporate level must comport with a hypothetical "macro" social contract that sets the moral boundaries for any social contracting. Framed another way, it might be said that for Dunfee and Donaldson, a moral "imagined community"[92] of contracting parties exists that shares a core group of moral rules. Dunfee and Donaldson's focus is on economic ethics, and they assume

that contracting parties are rational and knowledgeable. They recognize the importance of the existence of a framework of morality as a foundation for economic exchange. In the absence of these conditions, they argue that capital markets either become distorted or fail altogether owing to a fundamental lack of trust.[93]

In the context of information security issues, parties engaging in information exchanges – consumers buying goods online, shareholders visiting corporate websites for investor relations information, business partners licensing databases and the like – have an expectation that their information exchanges with a company will not harm them. As such, this expectation of safety entails trusting that the parties with whom they are transacting have updated the state of their information security to the state of the art. If merely doing business with someone causes harm through security compromise, trust is eroded. A complicating factor in this trust relationship is the difficulty of verifying the information security status of contracting parties. As such, parties are at an information disadvantage about each other's information security. Though their actions may be rational, their knowledge about information security may be deficient; nevertheless, they are reliant upon it. As Dunfee and Donaldson highlight, these are suboptimal conditions that may lead to market distortions and failures due to a lack of trust. Consequently, a company's role as a trusted member of the moral imagined community of information sharing parties necessitates preventing information security harm to others. A duty to update systems and maintain strong information security on an ongoing basis is the logical outgrowth.

Potentially a duty to exercise unique capabilities for the greater social good and to buttress development of stable institutions: developing good business norms

Thomas Dunfee argued that "[f]irms can play critical complementary role to government …when they exercise a core competency in responding to a social need."[94] A firm has a unique competency so long as no other firm has a greater competency.[95] Further, other ethicists argue that companies, particularly multinationals, have opportunities to support the development of well-ordered institutions through their normal business activities, through their internal activities and policies and through contributions to broad-based economic development.[96]

Combining these two insights with Dunfee and Donaldson's insights regarding the need for a shared framework of trust discussed in the previous section, we arrive at the argument that the widespread information security inadequacies in our economy and government perhaps trigger a duty for multinational corporations who specialize in information technology products and services to take the lead toward strong information security for all. Information technology companies with security expertise are uniquely situated to lead the way in crafting better information security practices in both the private and public sector. The development and stable functioning of our economic and social systems are being challenged by information security deficits. For example, the Government Accountability Office has repeatedly called for dramatic improvements in cybersecurity within the federal government, pointing out that even its most "secure" nuclear research facilities suffer from serious information security gaps.[97] Similarly, companies and individuals must report sensitive information to the IRS, but the IRS has struggled with its information security and continues to hire companies known for substandard information security.[98] A breach of the IRS that involves tampering with corporate tax filings could have serious repercussions of destabilizing the functioning of the IRS.

As discussed in previous sections, because of inherently transitive nature of information risk, the least secure company or government entity in possession of data determines the level of security for the whole system. The most careless possessor imposes negative effects in connection with the shared data on all other holders, similar to those that would have occurred if each other holder had been breached itself. Therefore, it is in companies' own interest to assist society in developing firm floors of adequate security, if for no other reason than to preserve the integrity of their own corporate information end to end. Expertise in information security matters is still an exclusive commodity that is just beginning to filter into the public and corporate consciousness. Companies in a position to use their inhouse expertise to help establish better information security

minimum standards to assist in buttressing our economy and social institutions should take the lead and do so as part of their corporate social responsibility programs. The greater social good needs corporate leadership in this area that is currently absent.

Conclusion

Using the work of Thomas Dunfee, this article has conducted in-depth analysis of the relationship between law and business ethics in the context of corporate information security. It has debunked the two dominant arguments against corporate investment in information security – that legal compliance equals social responsibility and that shareholder earning maximization limits spending on information security. It has explained why socially responsible corporate conduct necessitates strong information security practices, which arise out of the moral duty not to harm. Further, this article has argued that potentially a duty exists for companies to exercise unique capabilities for the greater social good and to buttress development and functioning of social institutions.

Notes

[1] Pricewaterhouse Coopers (2009).

[2] Accounting practices have struggled to keep up (Caruso, 2007).

[3] Dunfee (2007).

[4] For example, goodwill frequently makes up over 15% of corporate assets in large companies (Get Out the Red Pen, 2009).

[5] Carr (2008).

[6] Time Magazine (1983).

[7] For example, most law firms use document management systems to centralize work product. For a discussion of document management software (Kennedy and Gelagin, 2003). This use of information technology serves to facilitate knowledge management, the sharing of institutional intellectual resources such as form contracts, and control over access to certain information.

[8] For a discussion of the risks that trade secret information faces from technology, see, e.g., Rowe (2007).

[9] The Gramm-Leach-Bliley Act specifically considers the implications of financial information being stored in corporate databases (Gramm-Leach-Bliley Financial Services Modernization Act, 1999).

[10] Consumers increasingly venture online to engage in information-sensitive activities, such as checking bank balances or transmitting credit card information in connection with purchases. Many consumers now view the purchasing of goods through the internet as a routine part of life (More Businesses Are Buying Over the Internet 2004). In the course of this routine, they leave a trail of information behind them.

[11] Winn and Wrathall (2000).

[12] H.R. Rep. No. 106-74, pt. 3, at 106-07 (1999).

[13] McDonald's Launches Fundraising Effort (2008).

[14] Shelvin (2007).

[15] King (2008).

[16] See, e.g., "I'm into Clippy" group (2009).

[17] Jewell (2007).

[18] Vijayan (2009).

[19] Pricewaterhouse Coopers (2008).

[20] See, e.g., Privacy Rights Clearinghouse (2009).

[21] The definition of stakeholder espoused here is consistent with that advocated by Dunfee. Dunfee defines stakeholders to be defined as a group of individuals determined in accordance with community norms and law whose interests are impacted by the activities of the company, consistent with hypernorms (Dunfee, 2002b).

[22] Fichera and Wenninger (2004).

[23] A further argument can be crafted that a positive duty to provide stakeholders the best possible information security. These ethical obligations are not absolute; they do not require unlimited expenditures. They simply require an entity to stay up to date in its knowledge and exercise reasonable care.

[24] Vamosi (2007).

[25] Dunfee (2007).

[26] Dunfee (2007).

[27] Matwyshyn (2007).

[28] In 1995, the European Union passed the E.U. "Data Directive," which went into effect in EU member states in 1998. The Data Directive contains provisions that prohibit transfer of the data of any European person outside the European Union without consent and require contractual imposition of a minimum level of care in handling on any third parties receiving the data. Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 38, art. 17.

[29] Salbu (2002).

[30] This statement does not contemplate any criminal statutes such as the Electronic Communications Privacy Act, 18 U.S.C. § 2701 (2000), which was passed in 1986.

[31] 15 U.S.C. §§ 6501–6506; 16 C.F.R. § 312.

[32] See, e.g., Schwartz (2007).

[33] Health Insurance Portability & Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936 (1996); (U.S. Department of Labor, Fact Sheet: Health Insurance Portability and Accountability Act, n.d.).

[34] 15 U.S.C. §§ 6801–6809 (2004).

[35] Children's Online Privacy Protection Act of 2000, 15 U.S.C. §§ 6501–6506 (2000). Children's Online Privacy Protection Rule, 16 CFR Part 312 (2006).

[36] For a list of state data breach notification statutes: National Conference of State Legislatures (n.d.).

[37] These state statutes vary in their definition of what constitutes a breach warranting notice, leaving discretion in some cases to the entity itself to determine whether the breach triggers the statute. For a discussion of state data breach notification statutes (Schwartz, 2007).

[38] Schwartz (2007).

[39] Privacy Rights Clearinghouse (2009).

[40] For example, CVS/Caremark recently paid $2.25 m to settle charges brought in connection with its dumping of medical records and patient social security numbers into garbage cans outside its stores (Pereira, 2009).

[41] In re Caremark Int'l Inc. Deriv. Litig., 698 A.2d 959, 967 (Del. Ch. 1996), the Delaware court held that sustained or systematic failure of the board to exercise oversight constitutes a breach of the duty of loyalty and thus a failure to act in good faith. In Stone v. Ritter, the Supreme Court of Delaware again discussed the role of good faith in the context of directors' fiduciary duties in holding that a failure to act in good faith is not in itself a reason for a finding of fiduciary liability. Instead, the requirement to act in good faith is an element of the duty of loyalty, and a failure to act in good faith may result in liability if the director's conduct violates the duty of loyalty. Stone v. Ritter, 911 A.2d 362, 369–370 (Del. 2006).

[42] 698 A.2d 959, 967 (Del. Ch. 1996).

[43] In re Caremark Int'l Inc. Deriv. Litig., 698 A.2d 959, 971 (Del. 1996).

[44] Stone v. Ritter, 911 A.2d 362 (Del. 2006).

[45] Miller v. McDonald (In re Health Alternatives, Inc.) (2008).

[46] Miller (2008).

[47] Sarbanes–Oxley Act, Section 404, Pub. L. No. 107–204, 116 Stat. 745 (codified in scattered sections of 11, 15, 18, 28 and 29 U.S.C. (Supp. III 2003)).

[48] Schwartz et al. (2005).

[49] Claburn (2007a, b).

[50] Wilson (2009).

[51] For example, Acxiom Corporation derives revenue principally from selling aggregated information. If this information is stolen and becomes available cheaply on the information black market, it is highly unlikely that Acxiom will be able to maintain the value of this intangible asset at previous levels (Acxiom Inc. 2009).

[52] Wright (2004). In the tax context, entities frequently argue that they should be allowed to amortize the value of their customer lists (Charles Schwab Corp. v. Comm'r, 2004).

[53] In the biggest incidence of identity theft known to date, a help desk worker at Teledata Communications, Inc., which provides credit reports on consumers to lenders, is estimated to have stolen 30,000 consumers' credit reports which he shared with around 20 compatriots who leveraged the data to cause significant financial damage to the consumers in question. He was paid approximately $30 per credit report, or a total of $900,000 (Neumeister, 2003; Reuters, 2004).

[54] It can be argued that any data leakage is demonstrative of inadequate measures to keep the information secret, thereby putting it outside the scope of trade secret protection of most states' trade secret statutes. Trade secret statutes vary state by state, but most define a "trade secret" as information that an entity has used due care in protecting from disclosure. If it can be demonstrated that information security practices of an entity were suboptimal during any point in the lifetime of the information, it can frequently be successfully argued that the information in question is no longer a trade secret (Soma et al., 1996).

[55] One of the newest brand-building techniques is for each entity to make its own corporate cyborg/avatar to provide a friendly face to internet visitors (Vhost Sitepal, 2004).

[56] Pereira (2009).

[57] For example, some professional spammer employees earn salaries in excess of $100,000 per year while professional spammer entity owners earn millions of dollars per year (Comments of Simple Nomad, 2003).

[58] Chapman (2007). In particular, the involvement of organized crime in identity theft has brought an additional level of professionalization.

[59] Menn (2004).

[60] According to Dunfee, the multiple sources of standards that exist or potentially exist complicate the process of determining which ethical principles are relevant for a particular board and its constituent directors. The potential sources for ethical obligation for directors and/or boards include: (a) corporate codes of ethics; (b) director-specific corporate codes of ethics; (c) company corporate governance principles; (d) ethical codes for members of national director association; (e) international and national corporate governance principles; and (f) generally recognized principles of business ethics.

Each has its own focus and purpose. Taken together they point the way toward core principles for directors' ethical obligations. Corporate codes of ethics Directors of companies having a code of ethics for their employees may be explicitly required to comply with relevant portions of their corporation's code of ethics.

[61] Bowie and Dunfee (2002). See also Dunfee (1998, 1999).

[62] Pricewaterhouse Coopers (2008).

[63] For example, in one study of the banking industry in the United States, an industry currently plagued with instability and holds in excess of $7.17 trillion in loans, 36% of customer emails went unanswered. 96% did not offer live chat as a communication channel, and 94% of banks did not offer a website with a dynamic, flexible knowledge base allowing customers to have the most updated account information (Talisma, 2008).

[64] Leyden (2006).

[65] Ex-AOL Man jailed For E-mail Scam (2005).

[66] For example, TJX Companies recently experienced a large data breach due to a failure to update security (Gaudin, 2007; Massachusetts, Connecticut Bankers Associations and the Maine Association of Community Banks and Individual Banks File Class Action Lawsuit Against TJX Companies Inc., 2007).

[67] Schwartz et al. (2005).

[68] See endnote 48.

[69] Trevino and Weaver (2003).

[70] Pricewaterhouse Coopers (2009, p. 10).

[71] Pricewaterhouse Coopers (2009).

[72] Ford and Richardson, (1994). Although this relationship is not universally true, its presence a portion of the time makes it a worthwhile step toward building a corporate culture of security.

[73] See endnote 48.

[74] See endnote 48.

[75] The Sentencing Guidelines require organizations to "…promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law" and require that the organization's "governing authority" be "…knowledgeable about the content and operation of the compliance and ethics program and…exercise reasonable oversight with respect to the implementation and effectiveness of the compliance and ethics program" (Schwartz et al., 2005).

[76] For a recent exchange on the concept of corporate citizenship, see (Néron and Norman, 2008) and the responses published in the same issue of *Business Ethics Quarterly*.

[77] See endnote 48.

[78] See endnote 48.

[79] See endnote 48.

[80] Identity Theft Resource Center (2009).

[81] The banks impacted by the TJX breach argued that as corporate data breaches such as the TJX breach become more frequent and larger in scale, banks cannot continue to absorb the downstream costs of other companies' information security mistakes (Gaudin, 2007). As the TJX suits demonstrate, data breaches never occur in a corporate vacuum.

[82] Utah Attorney General (2004).

[83] For example, victims frequently feel residual psychological trauma for as long as 5 years after a crime (see Herek et al., 1999).

[84] For a discussion, see, e.g., Matwyshyn (2005).

[85] Approximately 15% of identity theft victims' personal information is fraudulently used in nonfinancial ways, particularly in connection with the thief being charged with a crime and passing himself off as the victim. Four percent of victims reported that their information was misused in this way (McCullagh, 2003).

[86] Hess and Dunfee (2002) citing Deegan et al. (2002).

[87] Hess and Dunfee (2002) citing Franco (2002). Dunfee further argued that in such circumstances, a single standardized format should be established by a government body to overcome the problem of strategic (non)disclosure by firms. The goal is to permit comparability with other firms. It seems that law is indeed evolving in this direction, as discussions of national data breach legislation commence.

[88] Abelson (2009).

[89] Monster.com Admits Keeping Data Breach Under Wraps (2007).

[90] See endnote 89.

[91] "It is in economic communities, and in the often unspoken understandings that constitute their ethical glue, that we believe many of the answers to business ethics quandaries lie. We think that answering ethical questions… requires understanding both the extant but often unspoken "contracts' that pervade business and also a yet deeper, universal "contract" that supersedes even individual ones, thus resulting in an approach to business ethics that integrates deep and shallow social contracts."

[92] Anderson (1991).

[93] Donaldson and Dunfee (2002).

[94] For Dunfee, successful corporate humanitarian interventions should be: (1) connected to the organization's core values, (2) based on special competencies, (3) done in a manner consistent with the company's responsibility to generate profits, and (4) based on specific goals and performance measurement (Dunfee, 2002a, b).

[95] Dunfee (2006).

[96] Hsieh (2004).
[97] Lipowicz (2008).
[98] IRS Freely Gives Out Employee User Name/Password Info (2007), Goodin (2009).

Acknowledgment

The author thanks the Zicklin Center for Business Ethics Research for the continued support of her research.

References

Abelson, J.: 2009 'TJX holds sale related to breach of consumer data', *Boston.com*. http://www.boston.com/business/articles/2009/01/22/tjx_holds_sale_related_to_breach_of_consumer_data/. Accessed 22 Jan 2009.

Acxiom, Inc.: 2009, http://www.acxiom.com/. January 20.

Anderson, B.: 1991, *Imagined Communities* (Verso, London).

Bowie, N. E. and T. W. Dunfee: 2002, 'Confronting Morality in Markets', *Journal of Business Ethics* **38**(4), 381–393.

Carr, J.: 2008, *SC Magazine*, April 10. http://www.scmagazineus.com/From-RSA-Financial-services-companies-struggling-with-multichannel-authentication/article/108906/. Accessed 3 Jan 2009.

Caruso, D.: 2007, 'When Balance Sheets Collide With the New Economy', *New York Times*, September 9. http://www.nytimes.com/2007/09/09/business/09frame.html?_r=1&oref=slogin. Accessed 3 Jan 2009.

Chapman, M.: 2007, 'Monster.com suffers job lot of data theft', *vnunet.com*, August 21. http://www.itweek.co.uk/vnunet/news/2197133/monster-suffers-job-lot-theft.

Charles Schwab Corp. v. Comm'r: 2004, U.S. Tax Ct. LEXIS 10 (T.C. Mar. 9, 2004).

Claburn, T.: 2007a, 'Facebook and MySpace Monetize Friendship with Targeted Ads', *ITNews.com*, November 7. http://www.itnews.com.au/News/64502,facebook-and-myspace-monetize-frienship-with-targeted-ads.aspx.

Claburn, T.: 2007b, 'The Cost of Data Loss Rises', *Information Week*, November 28. http://www.informationweek.com/management/showArticle.jhtml?articleID=204204152.

Comments of Simple Nomad: 2003, *Stanford University, Cybersecurity, Research and Disclosure Conference*.

Donaldson, T. J. and T. W. Dunfee: 2002, 'Ties that Bind in Business Ethics: Social Contracts and Why They Matter', *Journal of Banking & Finance* **26**, 1853–1865.

Dunfee, T.: 1998, 'The Marketplace of Morality: Small Steps Toward a Theory of Moral Choice', *Business Ethics Quarterly* **8**(1), 127–145.

Dunfee, T. W.: 1999, 'Corporate Governance in a Market with Morality', *Law and Contemporary Problems* **62**(3), 101–129.

Dunfee, T. W.: 2002a, 'Don't Compel but Encourage', *Across the Board*. January–February, p. 23.

Dunfee, T. W.: 2002b, 'Stakeholder Theory: Managing Corporate Social Responsibility in a Multiple Actor Context', in A. Crane, A. McWilliams, D. Matter, J. Moon and D. Siegel (eds.), *The Oxford Handbook of Corporate Social Responsibility* (Oxford University Press, Oxford), pp. 346–362.

Dunfee, T. W.: 2006, 'Do Firms with Unique Competencies for Rescuing Victims of Human Catastrophes Have Special Obligations', *Business Ethics Quarterly* **16**(2), 185–210.

Dunfee, T. W.: 2007, 'The World is Flat in the Twenty-First Century: A Response to Hasnas', *Business Ethics Quarterly* **17**(3), 427–431.

Ex-AOL Man Jailed For E-mail Scam: 2005, *BBC*, August 18. http://news.bbc.co.uk/2/hi/technology/4162320.stm. Accessed 30 Jan 2009.

Fichera, R. and S. Wenninger: 2004, 'Islands of Automation are Dead—Long Live Islands of Automation', *Forrester*, August 13. http://www.forrester.com/Research/Document/Excerpt/0,7211,35206,00.html.

Ford, R. C. and W. D. Richardson: 1994, 'Ethical Decision Making: A Review of the Empirical Literature', *Journal of Business Ethics* **13**, 205.

Gaudin, S.: 2007, 'Banks Hit T.J. Maxx Owner With Class-Action Lawsuit', *Information Week*, April 25. http://www.informationweek.com/news/showArticle.jhtml?articleID=199201456.

Get Out the Red Pen: 2009, *Barrons*, February 17. http://online.barrons.com/article/SB123457702581886857.html?mod=wsjcrmain. Accessed 20 Feb 2009.

Goodin, D.: 2009, 'After Mass Security Lapse, RBS Worldpay Gets IRS Contract', *The Register*, April 24. http://www.facebook.com/ext/share.php?sid=76662123957&h=41EbF&u=LSKn1&ref=mf.

Gramm-Leach-Bliley Financial Services Modernization Act: 1999, *Pub. L. No. 106–102, 113 Stat. 1338*.

Herek, M., J. R. Gillis and J. C. Cogan: 1999, 'Psychological Sequelae of Hate-Crime Victimization Among Lesbian, Gay, and Bisexual Adults', *Journal of Consulting and Clinical Psychology* **67**, 945.

Hess, D. and T. W. Dunfee: 2002, 'The Kasky-Nike Threat to Corporate Social Reporting: Implementing a Standard for Optimal Truthful Disclosure as a Solution', *Business Ethics Quarterly* **17**(1), 3–30.

Hsieh, N.: 2004, 'The Obligations of Transnational Corporations: Rawlsian Justice and the Duty of Assistance', *Business Ethics Quarterly* **14**, 643–661.

Identity Theft Resource Center: 2009, *2008 Data Breach Total Soars*. January 5. http://www.idtheftcenter.org/artman2/publish/m_press/2008_Data_Breach_Totals_Soar.shtml. Accessed 30 Jan 2009.

''I'm into Clippy'' group. *Facebook*: 2009, http://www.facebook.com/s.php?init=q&q=clipp&ref=ts&sid=ce08cec5d72135ff10e279eaecda4355#/group.php?sid=0&gid=33916191574. Accessed 3 Jan 2009.

IRS Freely Gives Out Employee User Name/Password Info: 2007, *Slashdot*, August 5. http://it.slashdot.org/article.pl?sid=07/08/05/1834201&tid=172. Accessed 3 Jan 2009.

Jewell, M.: 2007, 'TJX Breach Could Top 94 Million Accounts', *MSNBC*, October 24. http://www.msnbc.msn.com/id/21454847/.

Kennedy, D. and J. Gelagin: 2003, 'Want to Save 16 Minutes Every Day?', *Findlaw*. February. http://practice.findlaw.com/archives/worldbeat_0203.html.

King, R.: 2008, 'Building a Brand with Widgets', *Businessweek*, March 3. http://www.businessweek.com/technology/content/feb2008/tc20080303_000743_page_2.htm. Accessed 3 Jan 2009.

Leyden, J.: 2006, 'Acxiom database hacker jailed for 8 years', *The Register*, February 23. http://www.theregister.co.uk/2006/02/23/acxiom_spam_hack_sentencing/. Accessed 3 Feb 2009.

Lipowicz, A.: 2008, *GAO: Los Alamos Lab has Cybersecurity Gaps*, September 26. http://fcw.com/Articles/2008/09/26/GAO-Los-Alamos-Lab-has-cybersecurity-gaps.aspx. Accessed 3 Feb 2009.

Massachusetts, Connecticut Bankers Associations and the Maine Association of Community Banks and Individual Banks File Class Action Lawsuit Against TJX Companies Inc.: 2007, *Massachusetts Bankers Association*, April 24. https://www.massbankers.org/pdfs/DataBreachSuitNR5.pdf.

Matwyshyn, A. M.: 2005, 'Material Vulnerabilities: Data Privacy, Corporate Information Security and Securities Regulation', *Berkeley Business Law Journal* **3**, 129.

Matwyshyn, A. M.: 2007, 'Technoconsen(t)sus', *Washington University Law Review* **85**, 529.

McCullagh, D.: 2003, 'Study: Millions Hit by ID Fraud', *News.com*. September 3. http://news.com.com/Study+Millions+hit+by+ID+fraud/2100-1029_3-5071060.html?tag=st.rc.targ_mb. Accessed 3 Jan 2009.

McDonald's Launches Fundraising Effort: 2008, November 18. http://www.philanthropyjournal.org/news/mcdonalds-launches-fundraising-effort. Accessed 3 Jan 2009.

Menn, J.: 2004, 'Deleting Onling Extortion', *LA Times*, October 25. http://www.josephmenn.com/other_delete_online_extortion.php.

Miller, R. T.: 2008, 'Wrongful Omissions by Corporate Directors: Stone v. Ritter and Adapting the Process Model of the Delaware Business Judgment Rule', *University of Pennsylvania Journal of Business and Employment Law* **10**, 911.

Miller v. McDonald (*In re Health Alternatives, Inc*).: 2008 B.R., Adv. No. 07-51350, WL 1002035 at *1 (Bankr.D.Del., April 9, 2008).

Monster.com Admits Keeping Data Breach Under Wraps: 2007, August 24. http://www.foxnews.com/story/0,2933,294471,00.html. Accessed 3 Jan 2009.

Néron, P.-Y. and W. Norman: 2008, 'Corporations as Citizens: Political not Metaphorical, A Reply to Critics', *Business Ethics Quarterly*.

Neumeister, L.: 2003, 'Guilty Plea in Huge ID Theft Case', *CBS*, September 14. http://www.cbsnews.com/stories/2004/09/15/tech/main643714.shtml.

Pereira, J.: 2009, *CVS to Pay $2.25 Million in Privacy Case*, February 19. http://www.wsj.com. Accessed 20 Feb 2009.

Pricewaterhouse Coopers: 2008, *Global State of Informaiton Security*. http://www.pwc.com/extweb/insights.nsf/docid/0E50FD887E3DC70F852574DB005DE509/$File/PwCsurvey2008_cio_reprint.pdf. Accessed 20 Jan 2009.

Pricewaterhouse Coopers: 2009, *Safeguarding the New Currency*, October. http://www.pwc.com/extweb/insights.nsf/docid/0E50FD887E3DC70F852574DB005DE509/$File/Safeguarding_the_new_currency.pdf. Accessed 2 Jan 2009.

Privacy Rights Clearinghouse: 2009, *Chronology of Data Breaches*. http://www.privacyrights.org/ar/ChronDataBreaches.htm. Accessed 30 Jan 2009.

Reuters: 2004, 'Man Pleads Guilty in Massive Identity Theft', *CNET*, September 15. http://news.com.com/Man+pleads+guilty+in+massive+identity+theft/2100-1029_3-5367658.html?tag=st.rc.targ_mb.

Rowe, E.: 2007, 'Saving Trade Secret Disclosures on the Internet Through Sequential Preservation', *Boston College Intellectual Property and Technology Forum*: 091101.

Salbu, S. R.: 2002, 'The European Union Data Privacy Directive and International Relations', *Vanderbilt Journal Transnational Law* **35**, 655–691.

Schwartz, P. M.: 2007, 'Notifications of Data Security Breaches', *Michigan Law Review* **105**, 913.

Schwartz, M. S., T. W. Dunfee and M. J. Kline: 2005, 'Tone at the Top: An Ethics Code for Directors?', *Journal of Business Ethics* **58**(1), 79–100.

Shelvin, R.: 2007, *ING Direct's Emotional Connection with Customers*, February 9. http://marketingroi.wordpress.com/2007/02/09/ing-directs-emotional-connection-with-customers/. Accessed 3 Feb 2009.

Soma, J. T., S. K. Black and A. R. Smith: 1996, 'Antitrust Pitfalls in Licensing', *Practicing Law Institute – Patent* **449**, 349.

Talisma: 2008, *Online Banking Audit Reveals Major Opportunities for Customer Service Improvement*, February 21. http://www.talisma.com/tal_news/press_release.aspx?id=1448. Accessed 3 Jan 2009.

Time Magazine: 1983, *Cover*, January 3. http://www.time.com/time/covers/0,16641,19830103,00.html. Accessed 3 Jan 2009.

Trevino, L. and G. R. Weaver: 2003, *Managing Ethics in Business Organizations: Social Scientific Perspectives* (Stanford University Press, Stanford, CA).

Utah Attorney General: 2004, *ID Theft + Mortgage Fraud = Utah's Newest Scam*, May 19. http://attorneygeneral.utah.gov/PrRel/prmay192004.htm. Accessed 30 Jan 2009.

Vamosi, R.: 2007, *Monster Defends Delay in Notifying Users of Data Breach*, August 30. http://news.cnet.com/8301-10784_3-9769438-7.html. Accessed 3 Jan 2009.

''Vhost Sitepal'': 2004, *Oddcast*. http://www.oddcast.com/sitepal/?promotionId=235&bannerId=128. Accessed 26 Nov 2004.

Vijayan, J.: 2009, *Heartland Data Breach Could be Bigger Than TJX's*, January 21. http://www.infoworld.com/article/09/01/21/Heartland_data_breach_could_be_bigger_than_TJXs_1.html. Accessed 30 Jan 2009.

Wilson, T.: 2009, *Data Breach Costs Rose Significantly In 2008, Ponemon Study Says*, February 2. http://www.darkreading.com/security/attacks/showArticle.jhtml?articleID=213000466&cid=RSSfeed. Accessed 1 Mar 2009.

Winn, J. K. and J. R. Wrathall.: 2000, 'Who Owns the Customer?', *Business Lawyer* **56**, 213–233.

Wright, B.: 2004 'IT Security Law', *Tax Administration*. http://www.taxadmin.org/fta/meet/04tech_pres/wright.pdf.

Department of Legal Studies and Business Ethics,
The Wharton School,
Philadelphia, PA 19104-6340, U.S.A.
E-mail: amatwysh@wharton.upenn.edu