Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Applying Information Security and Privacy Principles to Governance, Risk Management & Compliance

Corporate Governance, Risk Management & Compliance (GRC) is typically thought of in terms of adhering to particular compliance regimes (such as Sarbanes-Oxley) while addressing information security and privacy mandates (such as those found in HIPAA) is typically thought of as its own discrete task. This paper will bridge the gap between these two disciplines and identify how they interrelate and how efforts to comply with one regime can be leveraged to apply to the other. The topic is appropriate for GSEC because m...

Copyright SANS Institute

Author Retains Full Rights

AD

Applying Information Security and Privacy Principles to Governance, Risk Management & Compliance

GIAC (GSEC) Gold Certification

Author: Scott M. Giordano, giordanolaw@gmail.com
Advisor: Rodney Caudle

Accepted:

Abstract

Corporate Governance, Risk Management & Compliance (GRC) is typically thought of in terms of adhering to particular compliance regimes (such as Sarbanes-Oxley) while addressing information security and privacy mandates (such as those found in HIPAA) is typically thought of as its own discrete task. This paper will bridge the gap between these two disciplines and identify how they interrelate and how efforts to comply with one regime can be leveraged to apply to the other. The topic is appropriate for GSEC because much of InfoSec practice has legal implications, and many of them intersect with traditional GRC. This paper offers enterprises and government agencies the ability to minimize the duplication of total compliance efforts while improving InfoSec effectiveness. Perhaps more importantly, InfoSec professionals will have the ability to demonstrate their need for appropriate resources to upper management from a new perspective. Others will be interested in this paper for two reasons: (1) it demonstrates the many various applications of InfoSec to legal requirements and (2) it gives InfoSec professionals an importance to upper management that they previously did not possess. This paper will both build upon the legal aspects of InfoSec taught in class and add an entire new dimension to thinking about the implications of InfoSec as it applies to corporate GRC.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

1. Introduction

If there is a demarcation line for the start of the modern discipline of corporate governance, risk management and compliance (GRC) in the U.S., then perhaps the best candidate for that line is the handing down of the court's opinion in *In Re Caremark International Inc. Derivative Litigation* in 1996. *Caremark* stands for the principle that individual directors of a corporation's board may be held liable for failure to properly supervise the activities of that corporation. While the requirement for the creation of a corporate ethics program was promulgated in 1991 with the passage of the Federal Sentencing Guidelines for Organizations (FSGO), *Caremark* seems to have made a substantial impact on the resources dedicated to proper corporate governance. Completing this genesis period of corporate governance jurisprudence and guidelines was the legislative response to the Enron scandal and similar scandals at WorldCom and Adelphia, the enactment of Sarbanes-Oxley ("SOX") in 2002. Finally, extra-territorial governance regulation has become commonplace. The Foreign Corrupt Practices Act of 1977 (FCPA), a statute designed to combat bribery of foreign officials by U.S. companies, has seen unprecedented use in the past 6 years (Searcey, 2009). This combination of jurisprudence, guidelines, new legislation, and revitalization of statues subsequently precipitated a substantial volume of analysis by commentators. The result: a traditional discipline of law infused with new life and which has evolved ever since.

In a similar fashion, if there is a demarcation line for the start of the modern discipline of information security and privacy in the U.S., then perhaps the best candidate for that line is the passage of Senate Bill 1386 ("SB-1386") (Cal. Civ. Code §§ 1798.29, 1798.82 -1798.84) by the California legislature, the first "data breach notification" or "DBN" statute in the U.S. SB-1386 was passed by a unanimous vote in 2002 as a consequence of the intrusion into the Steven P. Teale data center in Sacramento, California, the state's capital. The Teale Data Center held, among other things, information about every employee in California, including members of the legislature. The statute requires timely notification of suspected

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

breaches of personally identifiable information (PII) of California residents, and in so requiring, effectively created a constantly-updated public listing of entities that have suffered a privacy breach nationwide, since entities in all states holding PII of California residents are subject to the statute (Privacy Rights Clearinghouse, n.d.). The result of the passage of SB-1386 was a flood of similar statutes, promulgated at the state (National Conference of State Legislatures, n.d.) and federal levels. Security requirements of private industry regulatory authorities gained similar strength (PCI Security Standards Council, n.d.).

During this time frame of roughly 1991-2002, governments in other parts of the world began promulgating regulations relating to corporate governance and information security and privacy as well. In 1995, the European union passed a strong directive addressing privacy of European citizens (E.U. Directive 95/46/EC), and that directive has had a profound impact on the way information is shared and where it is stored (The Cloud, 2009). In July of 2002 the European Union passed a directive addressing privacy of electronic communications (E.U. Directive 2002/58/EC). In December of 2003, Europe experienced its version of the Enron scandal with the revelation of massive accounting fraud by and collapse of Italian diary giant Parmalat, and new corporate governance regulations followed (George, & Lacey, 2006). Extra-territorial regulation of corporate governance has also begun in earnest with the enactment of the Bribery Act (2010) in the United Kingdom, an anti-corruption statute similar to the FCPA.

2. Legal GRC Principles

2.1. Introduction to GRC

The duties associated with corporate governance, risk management and compliance (GRC) have been important, if not especially remarkable, ones since the modern corporate age began in the U.S. after the end of the Second World War. Indeed, the idea of principles of, or best practices associated with, corporate governance are of relatively recent vintage (Somerville, 2009). The first step in

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

understanding the nature and scope of this discipline is that the concept of GRC is literally a contrivance by industry analysts that study the market for solutions to legal, regulatory and risk management obligations. While an enterprise may have legal, compliance and risk management departments, there is no GRC department or Chief GRC Officer. Gartner, an industry analyst firm with an emphasis on information technology (IT), acknowledges as much (Gartner Hype Cycle, 2010).

The definitions of the three GRC components can and do vary greatly; the following are offered for purposes of this analysis:

Governance. The means by which a corporation's board of directors steers or guides the corporate entity.

Risk Management. An operational-centric definition might be "the risk of loss resulting from inadequate or failed internal processes, people and systems, business relationships, or from external events." (Rasmussen, 2010) An information security-centric definition might be "the process of identifying, assessing, and reducing the risk to an acceptable level and implementing the right mechanisms to maintain that level of risk." (Harris, 2005)

Compliance. Bayer's 2008 Annual Report defines compliance this way: "Corporate compliance comprises the observance of statutory and company regulations on lawful and responsible conduct by the company, its employees and its management and supervisory bodies."

2.2. GRC Categories

Industry analysts such as Gartner and Forrester Research have created categories or disciplines of GRC in order to assist in the analysis and evaluation of the offerings by vendors, including Enterprise GRC (E-GRC) (Gartner Enterprise Governance, 2008) and information technology GRC (IT-GRC) (Gartner Critical Capabilities, 2010). The GRC discipline that is the subject of this paper is a relatively new one called *Legal GRC (L-GRC)*. L-GRC represents GRC tasks or functions that have the most potential to result in litigation or regulatory scrutiny, and therefore require close and consistent collaboration with the corporate legal

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

department, outside counsel and subject matter experts (SMEs). Candidate departments include compliance, internal audit, risk management, loss prevention, human resources, and IT. L-GRC (hereinafter GRC) matters include: FCPA compliance, anti-trust, ethics management, policy & procedure management, export controls, internal investigations, information security and privacy, data loss prevention, e-discovery, and "horizontal" compliance practice that affects nearly every company, such as those that are HR-related, advertising/media and social media regulation.

2.3. GRC In Practice

The definitions of the respective GRC components described earlier, while accurate, do little to illuminate the practical role of GRC in the enterprise. Perhaps the best publicized aspect of corporate governance for enterprises that conduct business in foreign nations is the FCPA. The FCPA prohibits bribery of foreign government officials to assist in obtaining or retaining business (U.S. Dept. of Justice Overview, n.d.). Currently there are at least 120 active FCPA prosecutions and the statutes is noteworthy in particular because of its application not only to domestic firms operating overseas but to foreign corporations that have a presence in the U.S. (Urofsky, P., & Newcomb, D. 2010). Some recent FCPA-related settlements involving foreign corporations include Siemens AG (Germany), $800 million in 2008; KBR / Halliburton (United Arab Emirates), $579 million in 2009; and BAE (United Kingdom), $400 million in 2010 (FCPA Blog, 2010). The FCPA also addresses the financial integrity of corporations with a requirement of accurate record keeping which resembles an early incarnation of SOX.

With respect to financial integrity of a corporation, the promulgation of SOX has become iconic—this statute has become part of the fabric of the discipline of corporate governance and permeates the surrounding culture (Barnhizer, 2006). The significance of SOX goes far beyond its constituent parts addressing various practices of corporate boards. For example, section 806 (18 U.S.C. § 1514A)

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

contains protection for whistleblowers against retaliation by a corporation for participating in or assisting with an investigation by government authorities. Section 1107 (18 U.S.C. § 1513(e)) amended the obstruction of justice statute to protect whistleblowers who report *any* violation of federal law, not just of securities law. This is significant given the power of the obstruction statute as an independent means for prosecutors to obtain a conviction without having to obtain a conviction for the alleged underlying crime. The prosecution of Martha Stewart, for example, was for obstruction of justice (specifically, lying to investigators), not for insider trading, as publicity surrounding that matter implied. This is also significant because it applies to private corporations rather than merely public ones—in other words, every corporation is implicated (Kohn, n.d.). Finally, section 802 (18 U.S.C. § 1519) criminalizes intentional destruction of documents that could be involved in a government investigation or in a Chapter 11 bankruptcy.

Governance principles also apply to the physical and electronic integrity of a corporation. In March of 2007 retailer T.J. Maxx filed documents with the Securities and Exchange Commission (SEC) stating that the company experienced a breach of its computer network which resulted in the loss of some 45 million credit and debit card numbers, which, at the time, was the largest theft of such data. In the filing, the company admitted that the intrusion initially occurred in July of 2005 and continued until mid-January of 2007. The Federal Trade Commission (FTC) subsequently launched an investigation, and in March of 2008 reached a settlement with TJX (the parent company of T.J. Maxx). In the settlement documents the FTC alleged that the company "engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for personal information on its networks." Under the terms of the settlement TJX agreed to, among other things, "establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers" and that "[s]uch

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent's size and complexity, the nature and scope of respondent's activities, and the sensitivity of the personal information collected from or about consumers[.]" (FTC Settlement, 2008) The FTC's power to compel such a settlement did not come from any information security or privacy statute but rather from the FTC's power to prohibit unfair trade practices per Section 5(a) of the Federal Trade Commission Act, codified at 15 U.S.C § 45(a). Here, the FTC pursued the complaint under the theory that not protecting consumer privacy was an unfair trade practice. While this type of practice was not likely to have been considered when the Act was passed, the FTC has made the theory a consistent and successful means to combat poor information security and privacy practices at many corporations, and in doing so represents a major tool for promulgating corporate governance (Hiller, 2009).

3. Legal Principles of Information Security and Privacy

In determining the legal standards for which they will be held to account, InfoSec professionals (at least those without easy access to legal counsel) would, most likely, attempt to zero in on the section of the law that prospectively contains the requirements that must be completed in some algorithmic fashion, or what might be described as "The Information Security Statute." In practice, determining precisely what is expected of a particular professional, business unit manager, or company is not so easy and the amorphous nature of the law can be particularly frustrating to those trained to identify discrete answers or solutions to problems. Professionals soon discover that, yes, there are indeed applicable statutes, but also that the answers to their questions are more complex.

3.1. Common Law Liability

The common law system that is the foundation for the legal systems in the United Kingdom , the United States, and elsewhere was developed over hundreds of years in Great Britain by judges who determined questions of law with reference

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

to adjudication on similar matters by other judges (Plucknett, 1956) . That legal system was brought to the U.S. by British immigrants and built upon by succeeding generations of jurists and legislatures. One of the mainstays of the common law legal system is the adversarial nature of resolving disputes. Undoubtedly, most people have read or heard opinions on reforming the tort law system in the U.S. and associate that reform with matters that are commonly reported in the news media, such as medical malpractice or products liability. In the common law system, there are only two types of wrongs—crimes and torts. A crime committed against a person is considered committed against all of society. The criminal court system is designed primarily to punish those wrongs, and is done so by the state on behalf of society. The civil court system is designed to address just about everything else, and with respect to addressing wrongs, is designed primarily to compensate the aggrieved party. A tort is a civil wrong, and while all crimes are also torts, torts are not crimes. As a consequence, they can be resolved using the civil court system, which functions under a different standard of proof for resolving questions of fact—a "preponderance of the evidence" standard, i.e., it is more likely than not that an asserted allegation is true. This is in distinction to the standard for determining whether each element of a crime is proven—the "beyond a reasonable doubt" standard that most laypersons are familiar with. Understanding this distinction is important to InfoSec professionals for the following reasons:

1. There is no necessity to violate a law in order to be subject to a lawsuit in civil court. Lawsuits brought as a consequence of a security breach, e.g., occur regularly under the common law "theory" of negligence, the same theory used to bring the products liability, medical malpractice, and similar lawsuits mentioned earlier.
2. Tort law is used a matter of public policy as a means to "deputize" citizens to police the actions of others. Rather than have the government as the exclusive police agency, the civil legal system empowers citizens (usually through their attorneys) as a relatively economical way to seek redress against parties that are potentially committing some wrong. By demonstrating the scope of

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

potential liability, the civil law system is also a means to prevent decisions by people or companies that have the potential for harm to the public. The class action lawsuits that are commonly discussed in the media are examples of this, although a lawsuit does not have to achieve a class status in order to be effective at stopping or preventing potentially offensive actions.

3. Criminal statutes may contain a "private right of action" section or clause that offers citizen-victims the ability to pursue redress in civil court. The Computer Fraud and Abuse Act (1986) (CFAA), the federal "anti-hacking" statute, is one such example. Again, such right of action is created as a means to utilize citizens to police particular types of offensive behavior.
4. Conviction of a crime has potentially substantial civil implications. When a person (including a corporation, which is a fictional person) is convicted of a crime, the question of that person or entity's liability in civil court is considered already resolved under a principle known as *res judicata*, literally, "the thing has been adjudicated." This means that a crime victim can take that conviction into a civil court without the need for a jury trial on the merits of the matter, and request damages.

The importance of the foregoing discussion to InfoSec professionals is that civil liability can accrue for actions taken or not taken without a particular law being implicated. Rather, only the following is required: (1) a duty by the professional or entity in question to the complaining party; (2) a breach of that duty; (3) causation; and (4) damages (Schneider, 2009). When filing lawsuits relating to privacy or security violations, plaintiffs will not only rely on potential statutory violations in their pleadings (assuming they are available), they will almost without exception include common law theories, such as negligence. In July of 2010, a reporter for cable sports network ESPN, Erin Andrews, filed a lawsuit against hotel chain Marriott International, the Ohio State University, and others for a privacy breach that occurred when an individual surreptitiously videotaped her while undressing in her hotel room and subsequently posted the video on the Internet. In the lawsuit, she pleaded using only common law theories, including negligence (*Andrews v. Marriott*, 2010). The kernel of her theories was that the

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

defendants had a duty to protect guests from privacy breaches by taking due care to not give information helpful to potential stalkers, such as room numbers (the suit is pending as of this writing). In September of 2010, search engine provider Google settled a privacy lawsuit for $8.5 million that stemmed from the introduction of a feature into the company's email service, Google Mail, called "Buzz." Buzz was an attempt by Google to compete with social networking provider Facebook by capturing and distributing a subscriber's contacts list to all of the contacts in that list, effectively creating a virtual network. Google did so, however, without the consent of subscribers. The result was a lawsuit filed on behalf of seven subscribers that eventually achieved class action status. The settlement, filed in U.S. District Court in San Jose, California, citied a variety of theories, including violations of: the Electronic Communications Privacy Act, the Stored Communications Act, the Computer Fraud and Abuse Act, and the common law tort of Public Disclosure of Private Facts as recognized by California common law (Buzz Settlement, 2010). The settlement did not go to plaintiffs, however, but rather went to a fund designed to educate the public about the privacy aspects of Buzz (approximately $2 million went to plaintiffs' attorneys (Efrati, 2010)). The decision by Google to settle is not surprising. Defendants tend to settle out of fear of the potential scope of jury award and, as a practical matter, the vast majority of lawsuits settle before trial is complete—perhaps as many as 99%.

While the requirements for a lawsuit utilizing common law theories might seem relatively simple in an academic sense, in practice they sometimes represent a steep hill to climb for plaintiffs who have suffered as a result of poor information security practice by business and government entities. With respect to litigation precipitated by security breaches, often the biggest challenge for plaintiffs is the final element, articulating damages. TJX, for example, settled the consumer class action lawsuit that resulted from its breach in exchange for offering credit monitoring services valued by TJX at $166 million (though only valued by plaintiffs at $6.1 million) and $6.5 million in plaintiffs attorneys' fees but no cash

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

payments to plaintiffs. The presiding judge did question the disparity in valuation of the credit monitoring services but ultimately approved the settlement. While there is a dearth of analysis as to why the settlement did not provide a cash payment, almost certainly the cause was a lack of discernable damages on the part of the plaintiffs. This phenomenon is not the exception in data privacy breach litigation, but rather the rule. The dismissal of the privacy breach lawsuit against Hannaford stores is particularly instructive. Hannaford Brothers is a supermarket chain headquartered in Portland, Maine that suffered a security breach between Dec. 7, 2007 and March 10, 2008. According to a letter sent by Hannaford to the Massachusetts' Attorney General's office, malware was loaded into the company's servers that captured transaction data from the company's point-of-sale terminals and forwarded that data to an overseas destination (Messmer, 2008). Information from approximately 4.2 million payment cards was captured, resulting in 1,800 fraudulent charges (Privacy Rights Clearinghouse, n.d.). Lawsuits followed that utilized a variety of theories and the matter was ultimately heard before the Supreme Court of Maine. The Court rejected the suits because all losses had been reimbursed by the payment card issuers (with the exception of one unreimbursed loss; that case was allowed to go to trial). In rejecting the victims' request for damages based upon their expenditure of time and effort to address the breach, the justices stated that

> it must still be established that the time and effort expended constitute a legal injury rather than an inconvenience or annoyance. Unless the plaintiffs' loss of time reflects a corresponding loss of earnings or earning opportunities, it is not a cognizable injury under Maine law of negligence. [citations omitted] (*In Re Hannaford* at 12-13).

This decision illustrates the limitation of common law theories in privacy breach litigation—the disruption to the lives of victims can be substantial yet not subject to indemnification. This problem is especially acute for business owners, professionals, and the self employed who cannot point to lost wages because they do not receive a paycheck but still have to maintain their businesses while addressing the breach. Even when plaintiffs articulate theories based on statutes

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

in privacy breach lawsuits, the track record has been poor. Two examples demonstrate why lawsuit theories are less important than cognizable damages:

Ruiz v. Gap. Joel Ruiz, a job applicant at clothing retailer Gap, sued when a contractor to Gap, Vangent, was burglarized and suffered the loss of two laptops containing application information for approximately 750,000 Gap job applicants (Gantz, 2010). His theories included alleging negligence, breach of contract, unfair competition, invasion of privacy, and violation of Cal. Civ. Code § 1798.85, which provides for the protection of Social Security Numbers (SSNs). The U.S. District Court in San Jose granted summary judgment for the defendants (i.e., a determination that the allegations are without merit and the case should not proceed to trial) given that he could show no damages stemming from the theft, only the potential for such damages. Ruiz appealed and Ninth Circuit Court of Appeals upheld the lower court's decision, stating that, with respect to the negligence claim, the lower court correctly concluded "that Ruiz had failed to establish sufficient appreciable, nonspeculative, present harm to sustain a negligence cause of action under California law." (*Ruiz* at 3). With respect to the statutory claim, the Court of Appeals again upheld the lower court's decision, based on the interpretation of the statute as only preventing the use of an SSN as an identifier for logging into a website, rather than protecting the SSN from misuse after a person logs in.

Pisciotta v. Old National Bancorp. Defendant, a bank, suffered a privacy breach when an intruder broke into the bank's network and obtained access to the confidential information of tens of thousands of their customers. Plaintiffs brought a class action lawsuit in the U.S. District Court for the Southern District of Indiana against the bank and NCR, the bank's IT contractor, alleging negligence, breach of contract, and breach of implied contract. In their pleadings, plaintiffs sought relief for expenses related to purchasing credit monitoring services in order to warn of potential identity theft but did not cite any actual monetary losses. After reviewing other litigation that had similarly requested payment for credit monitoring services without underlying losses, the court dismissed the suit, given the absence of an allegation of cognizable damages.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Plaintiffs appealed using a variety of arguments, but the Seventh Circuit Court of Appeals ultimately disagreed, and after reviewing similar cases in other jurisdictions stated that

> [a]lthough some of these cases involve different types of information losses, all of the cases rely on the same basic premise: Without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy. (*Pisciotta* at 639).

Indiana has a privacy breach notification statute but plaintiffs did not cite it as part of the suit, most likely since it does not provide a private right of action and only requires notification of the breach, not subsequent remedial measures, such as providing credit monitoring services.

The long list of lawsuits resulting from electronic privacy breaches that were ultimately unsuccessful begs the question of why did plaintiffs' counsel initiate such actions knowing of the missing element of damages and poor track record of so many cases? The answer most likely lies in counsels' gamble that defendants would settle out of court rather than risk a large award from a hostile jury or litigation expenses that may drag on for years. All or nearly all of the privacy breach litigation involved class actions, whereby one plaintiff acts as a representative for others similarly aggrieved. Settlements in such matters are often very generous to plaintiffs' counsel (such as in the TJX and Google settlements) and counsel may well have been hoping to repeat such success in the matters just cited.

3.2. Common Law and Statutory Liability

In the United States, the legal principles that form the bedrock of information security and privacy obligations can be placed into two categories: (1) obligations that protect the integrity of the corporation; and (2) obligations that protect everyone else.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

3.2.1. The Caremark Decision

Obligations that protect the integrity of the corporation are based upon the principle that the directors of the corporation owe a fiduciary duty of due care with respect to giving appropriate attention to the operation of the corporation, and the failure to uphold that duty can result in the direct imposition of liability upon directors by the corporation's shareholders. The landmark case that is articulated this principle, *Caremark*, addressed that potential liability in the context of the integrity of a corporation's information and reporting systems. *Caremark* involved the settling of a lawsuit by the corporation's shareholders against the directors (a "derivative" lawsuit) for failure to supervise employee activities, specifically, activities that involved violations of federal healthcare law. Those violations resulted in an investigation by the Office of Inspector General (OIG) of the U.S. Department of Health and Human Services (HHS), the U.S. Department of Justice, and state regulators. Subsequently, indictments were issued by a federal grand jury against Caremark and two of its officers. The matter was ultimately settled, with Caremark agreeing to (1) plead guilty to a single count of mail fraud; (2) the payment of a criminal fine; (3) the payment of substantial civil damages; and (4) cooperate on further federal investigations on matters relating to the OIG investigation (*Caremark* at 18-19). Caremark proposed to settle the derivative action with the shareholders, and such settlement required review and consent by a Delaware state court judge. In reviewing the proposed settlement, the judge noted that plaintiffs were not alleging that the directors knew of the violations, but rather that they should have known, which is a higher standard to meet. In determining whether the proposed settlement was a fair one, the judge further noted that "relevant and timely information is an essential predicate for satisfaction of the board's supervisory and monitoring role" and that

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

> it is important that the board exercise a good faith judgment that the corporation's information and reporting system is in concept and design adequate to assure the board that appropriate information will come to its attention in a timely manner as a matter of ordinary operations, so that it may satisfy its responsibility. (*Caremark* at 38)**.**

The judge concluded that

> a director's obligation includes a duty to attempt in good faith to assure that a corporate information and reporting system, which the board concludes is adequate, exists, and that failure to do so under some circumstances may, in theory at least, render a director liable for losses caused by non-compliance with applicable legal standards[.] (citations omitted) (*Id).*

The importance of this holding to a corporation's directors is that they now must include, as part of their duties, a process to ensure that a proper corporate information and reporting system exists and that it is functioning according to principles that are generally accepted by the relevant governing bodies.

3.2.2. The Federal Sentencing Guidelines for Organizations

The Federal Sentencing Guidelines for Organizations (FSGO) is another source of obligations that address the integrity of a corporation's information system. The original Federal Sentencing Guidelines were issued in 1987 as a result of the Sentencing Reform Act of 1984. The Act sought to prevent disparate sentences for the same crime by introducing a standardized process by which the circumstances surrounding the offense(s) in question could be analyzed and a resulting sentence could be computed that would be consistent across courts. The FSGO was adopted by the United States Sentencing Commission (USSC) in 1991 pursuant to the Act and features as a key component "powerful incentives for corporations today to have in place compliance programs to detect violations of law, promptly to report violations to appropriate public officials when discovered, and to take prompt, voluntary remedial efforts." (*Caremark* at 33) Those incentives include a substantial reduction in the potential penalties that the

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

corporation might otherwise face as a result of criminal prosecution. The compliance programs cited is referred to in Section 8 of the Guidelines as a "corporate ethics program" and requires that every corporation have a program that contains the following seven elements:

1. Establish standards and procedures to prevent criminal conduct
2. Management oversight: (a) Upper management has knowledge and oversight of the compliance and ethics program; (b) The organization has an effective program with responsible individuals assigned; and (c) Those individuals have day-to-day operational responsibility for the program
3. Screen prospective or existing employees
4. Standards and training: (a) Communicate standards and procedures and (b) Conduct effective training programs.
5. Controls: (a) Establish controls to ensure that program is followed; (b) Conduct periodic evaluations; and (c) Establish a confidential reporting system.
6. Offer incentives to follow and controls to enforce the program
7. Respond to criminal conduct and improve the program accordingly

InfoSec professionals will immediately recognize that the ethics program elements are simply a set of preventative, detective, and corrective controls that have the following implications for information security and privacy practice:

1. Many, if not most, requirements of specific security statutes and regulations, such as the HIPAA Security Rule, can also be fulfilled simultaneously with FGSO requirements.
2. Because a FSGO-mandated compliance and ethics program draws direct sponsorship from upper management, the controls created pursuant to it are going to receive the necessary resources to make them effective in a way that information security controls seldom receive.
3. The general counsel (GC) or outside counsel of the corporation is going to be intimately involved in the creation of the program. Neither type of counsel

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

will probably appreciate the InfoSec implications and proactively involve the appropriate security team members.

4. Chief Compliance Officers (CCOs), if a corporation has one, often come from the legal department and consequently suffer the same lack of cognizance to reach out to those charged with information security.
5. It is incumbent upon InfoSec professionals to reach out to GCs, CCOs, and others charged with instituting corporate compliance programs in order to prevent the creation of duplicative controls and to give input into the overall protection strategy.

Corporate ethics programs established pursuant to FGSO or NYSE rules do not merely have the goal of preventing or remediating corporate malfeasance. Rather, there is a substantial body of commentary that argues that corporate ethics also implicates protecting the integrity of corporate property. That property includes intellectual property (IP) such as trade secrets. In order to take advantage of federal and state laws protecting trade secrets, corporations must demonstrate "reasonable" measures taken to protect the secret(s) in question. Many of those measures will relate to preventing unauthorized access to electronic data, and once again, information security strategy, personnel, and technology will be implicated.

3.2.3. Sarbanes-Oxley

The passage into law of Sarbanes-Oxley Act of 2002— SOX, was truly a watershed moment in the history of corporate regulation. Not since the aftermath of the Great Depression had so sweeping a set of corporate integrity regulations been promulgated by the federal government. Those regulations were passed in the wake of the bankruptcies of such corporate giants such as Enron, WorldCom, and Adelphia, and revelations of corporate malfeasance at companies such as Tyco International. Commentary and literature relating to SOX is legion— thousands, if not tens of thousands, of articles have been written about the statute and its implications. The costs to implement SOX are also stunning. Estimates for the average cost of Section 404 compliance for fiscal year 2004 ranged from

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

$2.2 to $2.6 million (Insurance Journal, 2005), while an estimate for fiscal year 2007 was $1.7 million (FEI Survey, 2008). The fundamental problem addressed by SOX is the integrity of corporate financial statements. Many of the problems relating to Enron, for example, stemmed from the proceeds of financial transactions that appeared on income statements but whose details remained hidden, or "off balance sheet," and therefore not subject to scrutiny by securities market participants and regulators. As a consequence, Section 302 of SOX set forth the requirement that both a publicly-traded corporation's CEO and CFO certify that veracity of the financial statements submitted to the SEC under penalty of criminal sanctions. For the InfoSec professional, several sections have indirect applicability to infrastructure protection, and, like FGSO, have the potential to create controls that are either duplicative or unnecessarily consume resources:

1. Section 404—Internal Financial Controls. Perhaps the most-cited section of the statute, 404 requires establishment of internal financial controls. Since financial data and systems are hosted on the corporation's network or one that the corporation has authority over, the requirement necessitates infrastructure protection and as a result is sometimes referred to as an "implied information security controls" requirement.
2. Section 409—Interim Reporting. Under this section, corporations that have discovered material weaknesses in their internal financial controls must issue an interim report to the SEC. This also has indirect applicability to InfoSec professionals since corporations such suffer a security breach such as an intruder into the network, loss of laptops or backup media, or other breach arguably have a potential weakness over internal financial controls.
3. Section 802—Records Management. This section provides criminal sanctions for intentional destruction of records relating to an investigation by government officials or to a Chapter 11 bankruptcy. Like the other sections of the statute, this section implies a role for information security staff members in the creation and promotion of controls that address the unauthorized destruction of corporate records.

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

3.2.4. The Federal Rules of Civil Procedure

The Federal Rules of Civil Procedure (FRCP) are the rules which govern most aspects of civil litigation in U.S. federal courts. The Rules, in conjunction with the Federal Rules of Evidence (FRE), govern the admission of evidence into legal proceedings. The process of requesting documents from an opposing party that are both relevant to the instant litigation and are not otherwise privileged is referred to as "discovery." Historically, discovery potentially involved copying tens, if not, hundreds, of thousands of documents, reviewing them for relevance and privilege, and then turning them over to the opposing party, or "producing" them. The opposing party would then assign junior attorneys to pore over those documents looking for evidence to support their client's claims. In the 1990's, attorneys realized that relevant and particularly very inculpatory data was stored on the hard drives of opposing parties and requested that such electronic data be produced. This led to a long litany of court decisions addressing the extent to which such data was admissible and what lengths the producing party had to go in order to fulfill the discovery request (traditionally, the party receiving the discovery request had to bear the full cost of production). Over time, commentators began referring to this process as "electronic discovery" or "e-discovery." As the number of cases addressing e-discovery grew, it became apparent that the FRCP would need to be amended in order to address the many aspects that are implicated by the intersection of IT and the U.S. legal system. Those amendments were promulgated in December of 2006, and have had a substantial impact on the discovery process in all or nearly all cases, since just about anything powered by electricity can produce electronic data, directly or indirectly (referred to by the amended Rules as "electronically stored information" or ESI). While the individual States are not subject to the FRCP relating to litigation in state court, many of them developed their own e-discovery rules, and undoubtedly the FRCP amendments have influenced them.

The applicability of GRC to information security occurs in two contexts: (1) the ability of the producing party's IT infrastructure to produce the data according to

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

the specific parameters of the requesting party and (2) the integrity of the process used to preserve and capture the requested ESI. The first requirement is sometimes referred to by e-discovery vendors as "FRCP compliance," which is a bit of a misnomer since the 2006 amendments never use the words "comply" or "compliance" in describing obligations related to e-discovery. The second requirement falls squarely on the shoulders of InfoSec professionals and is concerned with the authenticity of the ESI that is being offered into evidence. Early in e-discovery jurisprudence, trial court judges appeared not to offer especially intense scrutiny to ESI offered into evidence, only requiring that there be a "reasonable likelihood" that the evidence is what the party purported it to be (*U.S. v. Tropeano*, 2001). Over time, that scrutiny increased, and some trial court judges required a demonstration of the integrity of the process used to preserve, capture and process the ESI into the particular form that was being offered (or "proffered") into evidence. Two cases in particular have been cited for this proposition. The first is *American Exp. Travel Related Servs. v. Vinhnee (In re Vinhnee)* (2006), a bankruptcy matter, where a creditor sought to demonstrate that debts owed to it were not dischargeable and submitted electronic records in support. The bankruptcy court rejected the records as not properly authenticated and that rejection was upheld on appeal. With respect to the integrity of the process used to produce the ESI and offered into evidence pursuant to FRE 901(a), the appeals court found that

> The logical questions extend beyond the identification of the particular computer equipment and programs used. The entity's policies and procedures for the use of the equipment, database, and programs are important. How access to the pertinent database is controlled and, separately, how access to the specific program is controlled are important questions. **How changes in the database are logged or recorded, as well as the structure and implementation of backup systems and audit procedures for assuring the continuing integrity of the database, are pertinent to the question of whether records have been changed since their creation.** [emphasis added] (*Vinhee* at 445).

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

The second case is *Lorraine v. Markel Am. Ins. Co.* (2007). The matter related to an arbitration award, and both sides submitted a motion for summary judgment without bothering to authenticate their supporting electronic documents. Judge Paul Grimm rejected both submissions as a consequence. In his analysis, he discussed the process of authentication of computer-based evidence under FRE 901(a), stating that "[f]actors that should be considered in evaluating the reliability of computer-based evidence include the error rate in data inputting, and the security of the systems." He went further to state that

> The primary authenticity issue in the context of business records is on what has, or may have, happened to the record in the interval between when it was placed in the files and the time of trial. In other words, the record being proffered must be shown to continue to be an accurate representation of the record that originally was created . . . . Hence, the focus is not on the circumstances of the creation of the record**, but rather on the circumstances of the preservation of the record during the time it is in the file so as to assure that the document being proffered is the same as the document that originally was created**. [emphasis added] *(Markel* at 573).

In both cases, the threshold question as to the admissibility of the proffered evidence under FRE 901(a) focused on demonstrating the integrity of the logical and technological aspects of the entire duration of the evidentiary record's existence, from post-creation to the time it was offered into evidence. InfoSec professionals are uniquely qualified to address this process and, as a consequence, can expect this task to be added to their (arguably) already long list of duties.

4. Convergence

Over time, InfoSec and GRC professionals will see a convergence of laws and regulations addressing the integrity of IT systems and of the integrity of actions taken by corporate directors and officers. By necessity, they will be required to work closely together in order for their respective organizations to meet the long and growing list of obligations imposed upon them. This is so for the following reasons:

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

1. Mutual Dependency. The modern organization cannot function without the use of IT. The current migration to Cloud-based IT infrastructure and services does not vitiate this—in fact, it exacerbates the problem because there is an inherent distrust of data being held by another party. The fact that outsourced service providers probably are more security conscious than the average enterprise does not change this, since the perception of regulators and jurists is what matters. Directors and officers of a corporation are participants in and consumers of electronic networks and data, and corporate governance requires that their actions, insofar as they are evidenced by those networks and data, are captured for purposes of personal and corporate accountability. Thus, the goals of regulations that govern the integrity of personal and corporation actions and of electronic networks are tightly coupled.
2. Operational necessity. The emergence of post-Enron and post-financial crisis legislation addressing corporate integrity created an implied list of operational requirements needed to effectuate compliance with those laws. Other statutes already in existence, such as HIPAA, grew in scope in complexity over time as well, and in the same fashion, necessitated corresponding operational integrity requirements. Previous to these statutes, organizations could conceivable function internally using departmental silos, without much need for cross-departmental cooperation. Those days are over. Now, organizations have to break down those silos and mandate cooperation among departments if compliance is to be achieved. This is so because so many functions are implicated by GRC and information security requirements that trying to function independently would not only be duplicative and expensive, it would ultimately fail.
3. Globalization. The advent of globalization has produced its own legion of commentary, and the dangers of a world that is so tightly connected has been examined in depth by a variety of authors. Other countries are promulgating corporate governance and information privacy statutes, and there is every reason to believe that this phenomena will continue. Examples include (1) the U.K.'s Bribery Act, which will come into effect in April of 2011, and will address a greater range of corporate malfeasance than does the FCPA; and (2) EU Directive 2009/136/EC, which requires telecommunication providers to notify government authorities and

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

affected individuals of privacy breaches. Corporations that have European employees are subject to the EU Privacy Directive, and have found that conducting e-discovery that involves those employees directly or indirectly to be particularly difficult, since employee e-mail is considered personal information and its transfer outside of the EU is subject to a host of restrictions. Some European nations even have gone so far as to promulgate so-called "blocking statutes" that prevent any cooperation by resident companies with discovery requests from common law nations.

The result of these factors is that GRC and InfoSec professionals will have create a single set of policies that address the multitude of requirements, identify the expectations that are explicitly and implicitly imposed as a consequence, and create physical, technical, and administrative controls that enforce those expectations. The only way this can be achieved is with the unqualified support of the directors and management of the organization, including the resources that they can assign.

Below is a list of selected GRC statutes and regulations that have a direct or indirect InfoSec application:

Functional Area	GRC	Information Security & Privacy
Protection of consumer privacy, including personally identifiable information (PII), non-public information (NPI), and payment cardholder information	• SOX 404 and 409 • FSGO ethics program • Fair Credit Reporting Act (FCRA) • FACTA secure destruction rule • FTC Red Flags rule • Federal Trade Commission Act, §5 • Electronic Communications Privacy Act (ECPA) • E.U. Privacy Directives 1995/46/EC and 2002/58/EC	• HIPAA Security Rule • HIPAA Privacy Rule • State database breach notification statutes • MA 201 CMR 17.00 • GLBA • E.U. Directive 2009/ 136/EC • PCI-DSS
Protection of intangible assets, such as trade secrets, confidential information, brand, reputation, and	• SOX 404 and 409 • Uniform Trade Secrets Act (UTSA) • Economic Espionage	• Incident response protocols • FSGO-compliant physical, technical, and

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

goodwill	Act (EEA) • FSGO ethics program • NYSE Rule 303A • Business associate agreements	administrative controls
Electronic discovery obligations under the FRCP	• EDRM Information Management, Identification, and Preservation phases • SOX 809 • E-discovery blocking statutes (Europe)	• EDRM Collection phase • FRE 901(a)
Anti-bribery/anti-corruption	• FSGO compliance program • Foreign Corrupt Practices Act (FCPA) • Bribery Act (United Kingdom)	• FSGO-compliant physical, technical, and administrative controls

5. Conclusions

Everything that InfoSec professionals do (and fail to do) in the course of their duties has relevance to, and is impacted by, the laws and legal system of the United States and potentially other nations, depending on the scope of the relevant organization. Such duties will address a variety of events: responding to criminal activity, such as network intrusions; responding to requests for electronically stored information (ESI) from litigants, regulatory agencies, and law enforcement; gathering evidence for internal investigations; installing logical and technical controls; and proactively defending the enterprise through traffic analysis and other measures. This intersection of law, technology, and business requirements requires professionals for a variety of departments to work closely together, yet this is often not the case. Translating regulatory and judicial mandates into organization-wide policies is a task that is often done with little or no input from InfoSec professionals. Furthermore, those mandates and policies create expectations that, in order to be met, must be simple, measurable, achievable, and amenable to effective controls. Unfortunately, organizations tend to engage such professionals at the point when controls are to be put into place, which is long after strategic and budgetary decisions have already been made. At this point there is a real

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

risk of upper management looking at InfoSec as just a group of firewall installers and virus eradicators or worse, a group that is preventing business from being done because they are preventing people from going to their favorite websites. The challenge for InfoSec professionals in addressing the many security and privacy implications from global GRC mandates is having their perspective being taken into account by business unit managers and the General Counsel. CIOs often seem to view InfoSec as just another IT-related task, not unlike records management, and spend the bulk of their time on "big picture" matters such as vendor sourcing and IT projects. In their defense, they are charged with demonstrating yearly ROI and reduced costs, and many are now being asked to also demonstrate that they are providing the enterprise with a distinct competitive advantage. The larger problem is convincing the corporation's General Counsel. Unfortunately, attorneys only listen to other attorneys, and are going to take unsolicited advice from InfoSec professionals reluctantly. All of the white papers offered by vendors on the intersection of IT and law are going to be viewed with the same suspicion as well. The task of convincing the GC and other attorneys rests on InfoSec professionals' selling their proposals using language that attorneys appreciate. If a corporation has a CCO, that person should be the first person that the InfoSec professional visits to strategize on proper language and positioning. This is so since many CCOs and compliance officers are also attorneys but whose duties often touch upon InfoSec. One approach would be to use a legal research database (such as LexisNexis, Westlaw, or Google Scholar) to create a table that cross-references regulatory actions and legal case citations to IT-specific laws and guidelines. The FTC and state attorneys general routinely sanction corporations who have violated information security and privacy expectations of consumers, and issue press releases that provide a wealth of information that can be cited. That table, along with a presentation of the resulting costs and business disruption will go a long way to demonstrating the necessity and value of combined GRC-InfoSec compliance efforts. Finally, the organization's CFO has seen their role expand over the past decade to include protection of the organization's brand, stock price, and shareholder value, and will be very receptive to the economies of scale, increased overall protection, and reduction in potential organizational liability that a combined compliance effort offers.

Scott M. Giordano, giordanolaw@gmail.com

© 2010 SANS Institute, Author retains full rights.

6. References

$6.5 million fees in class action settlement between consumers and retailer approved; in re tjx co. retail sec. breach litig., no. 07-10162 (d. mass. nov. 3, 2008). *Class Action Law Monitor*, November 30, 2008, at p. 28.

American Exp. Travel Related Servs. v. Vinhnee (In re Vinhnee), 336 B.R. 437 (9th Cir. 2006).

Barnhizer, D. (2006). Waking from sustainability's 'impossible dream': the decision-making realities of business and government. *Georgetown International Environmental Law Review, 18,* 662.; Cleveland-Marshall Legal Studies Paper No. 06-123. Available at SSRN: http://ssrn.com/abstract=878405

Basri, C. (Ed.). (2008). *Ediscovery for corporate counsel, 2008 ed*. Eagan, MN: Thompson West.

Bayer, *2008 Annual Report*, Retrieved August 11, 2010, from http://www.annualreport2008.bayer.com/en/glossary.aspx

Biegelman, M., & Bartow, J. (2006). *Executive roadmap to fraud prevention and internal control.* Hoboken, N.J.: John Wiley & Sons, Inc.

California Civil Code §§ 1798.29, and 1798.82 through 1798.84.

Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, § 2, 100 Stat. 1213 (1986), codified at 18 U.S.C. § 1030.

Efrati, A. (2010). Google settles privacy lawsuit for $8.5 million [Electronic Version]. *The Wall Street Journal.*

Erin Andrews vs. Marriott International, Inc., et. al., No. 2010-L-008186, Ill. Cir., Cook Co. (2010).

European Parliament and Council. *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*, 2002 O.J. (L 201/37).

European Parliament and Council. *Parliament and 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 281/31).

Scott M. Giordano, giordanolaw@gmail.com

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Federal Sentencing Guidelines, 18 U.S.C. §§ 3551-3742 (2006); 28 U.S.C. § 991-98 (2006).

Financial Executives Institute. *FEI Survey: Average 2007 SOX Compliance Cost $1.7 Million* (April 30, 2008). Retrieved September 18, 2010 from http://fei.mediaroom.com/index.php?s=43&item=204

Fleischer, P. (2000, April 16). Privacy…? *The cloud: policy consequences for privacy when data no longer has a clear location.* Retrieved August 9, 2010 from http://peterfleischer.blogspot.com/2009/04/cloud-policy-consequences-for-privacy.html

FCPA Blog (2010, July 20). *The fcpa's top ten.* Retrieved August 15, 2010 from http://www.fcpablog.com/blog/2010/7/20/the-fcpas-top-ten.html

Foreign Corrupt Practices Act of 1977, 15 U.S.C. §§78dd-1 to 78dd-3.

George, B., & Lacey, K. (2006). *A comparative analysis of post-sarbanes-oxley corporate governance developments in the us and european union: the impact of tensions created by extraterritorial application of section 404.* The American Journal of Comparative Law, 52(2), 460. Available at SSRN: http://ssrn.com/abstract=1150365.

Gartner (2010, April 30). *Critical capabilities for it governance, risk and compliance management.* [Gartner ID Number: G00175673] Retrieved August 11, 2010, from http://www.gartner.com

Gartner (2008, February 19). *The enterprise governance, risk and compliance platform defined*. [Gartner ID Number: G00155196] Retrieved August 11, 2010, from http://www.gartner.com

Gartner (2010). *Hype cycle for governance, risk and compliance technologies, 2010*. Retrieved August 8, 2010 from http://www.gartner.com

Harris, S. (2005). *Cissp all-in-one exam guide, third edition*. New York, NY: McGraw-Hill Osborne Media.

Hiller, S. (2009). Due diligence on the run: business lessons derived from ftc actions to enforce core security principles. *Idaho Law Review, 45,* 283.

In Re Caremark International Inc. Derivative Litigation, 698 A.2d 959 (Del. Ch. 1996).

Scott M. Giordano, giordanolaw@gmail.com

© 2010 SANS Institute, Author retains full rights.

In Re Google Buzz User Privacy Litigation, Case No. 5:10-CV-00672-JW (N.D. Cal., Sept. 3, 2010), at p. 2.

In re Hannaford Bros. Co. Customer Data Sec. Breach Litig., 2010 ME 93 (Me. Sept. 21, 2010).

In re TJX Co. Retail Sec. Breach Litig., No. 07-10162 (D. Mass. Nov. 3, 2008).

K & L Gates LLP (2008, October 10). *Current listing of states that have enacted e-discovery rules*, Retrieved September 18, 2010 from http://www.ediscoverylaw.com/2008/10/articles/resources/current-listing-of-states-that-have-enacted-ediscovery-rules/

Kohn, S. (n.d.). *Sarbanes-oxley act: legal protection for corporate whistleblowers,* Retrieved August 15, 2010 from http://www.whistleblowers.org/index.php?option=com_content&task=view&id=27

Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534 (D. MD.) (May 4, 2007).

Matwyshyn, A.M. (2009). *Harboring data: information security, law, and the corporation.* Stanford, CA: Stanford Law Books.

Messmer, E. (2008). Details emerging from hannaford data breach. *Network World*, March 28, 2008.

Paz v. State of California, 22 Cal. 4th 550 (Cal. 2000).

PCI Security Standards Council, n.d. *About the pci data security standard (pci dss).* Retrieved August 8, 2010, from https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

Photopoulos, C. (2008). *Managing catastrophic loss of sensitive data: a guide for it and security professionals*. Burlington, MA: Syngress Publishing.

Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629 (7th Cir. Ind. 2007).

Plucknett, T. F.T. (1956). *A concise history of the common law. fifth edition.* Boston: Little, Brown and Company. Reprinted 2001 by The Lawbook Exchange, Ltd.

Privacy Rights Clearinghouse, n.d. *Chronology of data breaches*. Retrieved August 8 and October 9, 2010, from http://www.privacyrights.org/data-breach/new

National Conference of State Legislatures, n.d. *State Security Breach Notification Laws*. Retrieved August 8, 2010 from http://www.ncsl.org/default.aspx?tabid=13489

Scott M. Giordano, giordanolaw@gmail.com

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Rasmussen, M. (2010, July 26). Corporate Integrity. *Managing risk & compliance across extended business relationships*. Retrieved August 11, 2010 from http://corp-integrity. blogspot.com/2010/07/managing-risk-compliance-across.html

Ruiz v. Gap, Inc., 2010 U.S. App. LEXIS 10984 (9th Cir. Cal. May 28, 2010) (unpublished).

Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745, codified in scattered sections of 11, 15, 18, 28, and 29 U.S.C.

Sarbanes Oxley Drives Up Large Companies' Audit Costs by $1.4 Billion. *Insurance Journal*, April 28, 2005. Retrieved September 18, 2010 from http://www.insurancejournal.com/news/national/2005/04/28/54393.htm

Schneider, J. (2009). Preventing data breaches: alternative approaches to deter negligent handling of consumer data. *Boston University Journal of Science and Technology Law, 15,* 286.

Searcey, D. (2009). U.s. cracks down on corporate bribes [Electronic Version]. *The Wall Street Journal*, *A1*.

Sentencing Reform Act of 1984, part of the Comprehensive Crime Control Act of 1984, ch. 2, Pub. L. No. 98-473, 98 Stat. 1837, 1987 (1984), codified as amended in scattered sections of 18 U.S.C.

Somerville, M. (July 20, 2009). Getting serious about compliance the evolving role of the chief compliance officer. *Corporate Compliance Insights*. Retrieved August 8, 2010 from http://www.corporatecomplianceinsights.com/2010/evolving-role-definition-history-of-cco-chief-compliance-officer/

The T. J. Hooper, 60 F.2d 737 (2d Cir. N.Y. 1932).

United Kingdom Ministry of Justice. *Bribery act 2010*, Retrieved August 16, 2010, from http://www.justice.gov.uk/publications/bribery-bill.htm

United States Department of Justice. *Foreign corrupt practices act, an overview*, Retrieved August 15, 2010 from http://www.justice.gov/criminal/fraud/fcpa/

United States Federal Trade Commission. *In the matter of the tjx companies, inc., a corporation. agreement containing consent order. file no. 072 3055*, Retrieved August 16, 2010 from http://www.ftc.gov/os/caselist/ 0723055/ 080327agreement.pdf

Scott M. Giordano, giordanolaw@gmail.com

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

United States v. Tropeano, 252 F.3d 653 (2nd Cir. 2001).

Urofsky, P., & Newcomb, D. (2010, March 4). *Recent trends and patterns in fcpa enforcement*, Retrieved August 15, 2010 from http://www.shearman.com/FCPA-Digest-Reports-Increased-Prosecutions-of-Individuals-Emphasis-on-Industry-Compliance-03-29-2010/

© 2010 SANS Institute, Author retains full rights.

Scott M. Giordano, giordanolaw@gmail.com

© 2010 The SANS Institute As part of the Information Security Reading Room Author retains full rights.

Last Updated: June 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**