CYBER SECURITY AND DATA BREACHES: FIREWALLS & FIRESTORMS

by Sean J. Milano, Morrison Mahoney LLP, Stephen G. Troiano, Morrison Mahoney LLP and Cynthia Arends, Nilan Johnson Lewis PA

The recent explosion of cyber hacking and data breaches involving retailers and hospitality companies will undoubtedly lead to a commensurate rise in data breach litigation. Data breaches involving personal information and financial data, such as debit and credit card information, can be the basis for legal action on multiple fronts. The Federal Trade Commission (FTC) or state attorneys general may bring enforcement actions, which can carry significant fines and penalties. *See* In re Michaels Stores Pin Pad Litig, 830 F. Supp. 2d 518, 522 (N.D. Ill. 2011). Increasingly, consumer class actions are being filed seeking monetary damages for the data breach. In connection with such a consumer class action, financial institutions, such as banks and credit card companies, have also filed suit seeking to recover their costs arising out of the resulting fraudulent transactions and the need to replace the compromised cards. This paper will outline the types of actions that companies face from consumers, financial institutions and federal agencies. It also describes the applicable laws and regulations governing consumer data, along with resources available to businesses regarding consumer data issues. This paper concludes with a chronology of data breach incidents, at Appendix A.

Data Breach Litigation

The 2006 TJX cyber-attack and data theft resulted in litigation on several fronts. After TJX Companies disclosed that its data security had been compromised, numerous cases by allegedly affected consumers were filed. The U.S. District Court of Massachusetts consolidated these cases and the Multi-District Litigation Panel subsequently transferred all the cases, wherever located, into one action. *See* In re TJX Cos. Customer Data Sec. Breach Litig., 493 F. Supp. 2d 1382, 1383 (J.P.M.L. 2007). On a separate front, financial institutions brought suit against TJX, which was eventually consolidated with the consumer case, albeit proceeding on a different track.

A. Actions Brought Under Negligence Theory

Whether the litigation is brought by consumers or financial institutions, the causes of action asserted by plaintiffs are similar. In actions brought by consumers, negligence is frequently asserted. For instance, Supervalu, Inc. recently disclosed a data breach that occurred between June 22, 2014 and July 18, 2014. As of August 2014, consumer class actions have been filed in both Massachusetts and Illinois, despite the fact that little is known about the scope of the breach. The alleged common questions of fact or law for the consumer class include: 1) Whether defendants had a duty to disclose failures to comply with industry-standard cybersecurity practices; 2) Whether defendants complied with industry-standard cybersecurity practices; 3) Whether defendants concealed their noncompliance with industry-standard cybersecurity practices from their customers; 4) Whether the defendants' failure to comply with industry standard cybersecurity practices caused the beach. The plaintiffs' complaint further alleges that widely reported data breaches of point-of-sale systems at, among others, Target, Neiman Marcus, Michaels Stores, and P.F. Chang's, should have put Supervalu on notice that it

needed to ensure its own systems were not vulnerable to a similar attack. St. Pierre v. Supervalu, Inc., No. 1:14-cv-13539 (D. Mass. filed Aug. 29, 2014).

Financial institutions have also brought suits under a negligence theory against retail companies who have suffered a data breach. With respect to the 2013 Target Corporation breach, five banking institutions brought suit against Target individually, and on behalf of a class of all similarly situated financial institutions in the United States. On September 2, 2014, Target filed a motion to dismiss the plaintiffs' negligence claims. In its motion, Target argues the banks failed to plead that Target owed the banks any duty of care or that Target breached any such duty.

The Target case was brought in the United States District Court of Minnesota. With respect to the negligence claim, the banks argued that Target owed them a duty in obtaining, retaining, securing and deleting payment card information that Target collects from its consumers, providing security for that information consistent with industry standards, and thwarting intrusions routinely attempted by sophisticated hackers. *See* In Re Target Corporation Customer Data Security Breach Litigation, No. 014-md-02522 (D. Minn. 2014).

Target argued that no duty exists under Minnesota law to protect another from the harmful conduct, including criminal conduct, of a third person. Instead, a duty to protect against third party criminal harm arises only when (i) there is a special relationship between the defendant and the plaintiff (or the defendant and the third party) and (ii) the third-party harm is foreseeable. *See* Clark ex rel. H.B. v. Whittemore, 52 N.W.2d 705, 707 (Minn. 1996).

Negligence claims, as asserted in the Target case, have failed in other data breach cases. *See* In re Hannaford Bros. Co. Customer Data Sec. Breach Litig., 613 F. Supp. 2d 108, 124-25 (D. Me. 2009) (court dismissed negligent misrepresentation count where state's data breach notification statute left the court "wary of creating new state standards where the Maine Law Court had not already clearly provided a remedy").

However, at least one court has found such a duty to exist. *See* Sovereign Bank v. BJ's Wholesale Club, 395 F. Supp. 2d 183, 193-94 (M.D.P.A. 2005) (BJ's owed duty of care to issuer of credit and debit cards to prevent unauthorized disclosure of cardholder account numbers and information). In Sovereign, plaintiffs argued the nature of the relationship between a retail company and a credit card company established such a duty of care as a matter of law:

> there is a sufficient relationship between Plaintiff and BJ's because they both participate in the Visa network. BJ's as a merchant processes credit – and debit-card transactions for Sovereign as an issuing bank for the cards and, in the process, communicates with Sovereign before validating each transaction.

The court agreed with Sovereign's argument. The court held:

> A Sovereign cardholder uses the card at BJ's to buy a product. BJ's processes the transaction by electronically contacting Sovereign to approve it. The relationship is a direct one, with BJ's

knowing the issuing bank before initiating or completing the transaction.

At the time of this paper, the Target motion had not been ruled on. It is an emerging area of law, both with respect to actions brought by customers and those brought by financial institutions. However, even if plaintiffs are able to overcome this initial hurdle, many obstacles remain. Notably, in the Sovereign case, Sovereign's negligence claim was eventually dismissed under Pennsylvania's economic loss doctrine.

B. Breach of Fiduciary Duty

Another cause of action frequently asserted is breach of fiduciary duty. Courts have recognized the existence of a fiduciary duty to safeguard personal information. *See* Bell v. Michigan Counsel 25, 707 N.W.2d 597 (D. Mich. 2005); Cobell v. Norton, 391 F.2d 251 (D.D. C. 2004). Breach of implied contract and breach of implied warranty of fitness also frequently appear in consumer complaints. *See* In re Hannaford Bros. Co. Customer Data Security Breach Litig., 613 F. Supp. 2d 108, 119 (D. Me. 2009) (motion to dismiss breach of implied contract claim denied when court concluded that "in a grocery transaction where a customer uses a debit or credit card, a jury could find that there is an implied contractual term that Hannaford will use reasonable care in its custody of the consumers' credit card data").

In the case involving Hannaford, the plaintiffs argued that Hannaford owed a fiduciary duty to protect their credit and debit card data, which it allegedly breached. Under Maine law, to state a claim for fiduciary duty a plaintiff must: (1) allege the actual placing of trust and confidence in the defendant; (2) show that there is some disparity in the bargaining positions of the parties; and (3) show that the dominant party has abused its positions of trust. Leighton v. Fleet Bank of Me., 634 A.2d 453, 457-58 (Me. 1993).

The court held that plaintiffs did not show the "trust and confidence" contemplated by Maine confidential relationship cases. Under those cases, a fiduciary relationship was described as "something approximating a business agency, professional relationship, or family tie impelling or inducing the trusting party to relax the care and vigilance ordinarily exercised." Bryan R. v. Watchtower Bible & Tract Soc. of N.Y., Inc., 738 A.2d 839, 846 (Me. 1999).

Second, the Hannaford Court held that plaintiffs did not plead facts demonstrating disparate bargaining power between the plaintiffs and Hannaford. Finally, the court held that the plaintiffs failed to demonstrate that Hannaford abused a position of trust, because there was no evidence in the plaintiff's complaint that suggested Hannaford provided anything but a fair exchange of groceries in return for the customers' payments, or somehow took advantage of the system allowing customers to use cards.

C. State Data Breach Laws

Almost every state has enacted a statute regarding data breaches. *See* e.g. Mass. Gen. Laws c. 93H; Cal. Civ. Code §1798. The laws generally apply to all persons and entities that maintain or store personally identifiable information about a resident of that state. Under such statutes, there is a statutory duty to report a known security breach. Many such statutes do not provide for a private right of action. Further, some have a safe harbor provision for encrypted

data. Under such a safe harbor provision, no notice is required as long as data acquired or used is encrypted. For instance, the first state to pass such a statute was California. California Civil Code 1798.82 states:

> Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measure necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

The statute also requires the business to issue a security breach notification in the following manner:

> (1) The security breach notification shall be written in plain language.
>
> (2) The security breach notification shall include, at a minimum, the following information:
>
> (A) The name and contact information of the reporting person or business subject to this section.
>
> (B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
>
> (C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.
>
> (D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.
>
> (E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

> (F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

Cal Civ. Code 1798.84 also provides a private right of action and penalties. It also prohibits waiver:

> (a) Any waiver of a provision of this title is contrary to public policy and is void and unenforceable.
>
> (b) Any customer injured by a violation of this title may institute a civil action to recover damages.
>
> (c) In addition, for a willful, intentional, or reckless violation of Section 1798.83, a customer may recover a civil penalty not to exceed three thousand dollars per violation; otherwise, the customer may recover a civil penalty of up to five hundred dollars ($500) per violation for a violation of section 1798.83.

While almost every state has a similar data breach notification statute, not every state's statute expressly provides a private right of action. *See e.g.*, Mass. Gen. Laws. c. 93H (Massachusetts Attorney General can bring action and seek penalties, however there is no express private right of action). In one such action asserted by a consumer in Louisiana, the court dismissed the plaintiff's claim under the Louisiana Database Security Breach Notification law because the plaintiff failed to allege cognizable damages suffered from any breach. The court found that the plaintiff's damages were not based on an actual injury, but the speculative future injury of identity theft. Pinero v. Jackson Hewitt Tax Service, Inc., 594 F. Supp. 2d 710, 717 (E.D. La. 2009).

D. State Consumer Protection Laws

Consumers and financial institutions alike have asserted claims under state consumer protection laws in data breach litigation. Such claims allege defendants have engaged in unfair or deceptive trade practices. *See* In re TJX Companies Retail Security Breach Litigation, 524 F. Supp. 2d 83, 92 (2007); In re Hannaford Bros. Co. Customer Data Security Breach Litig., 613 F. Supp. 2d 108, 129 (D. Me. 2009).

In the Hannaford case, the court denied Hannaford's motion to dismiss the plaintiffs' unfair trade practices claim. Under Maine law:

> an act or practice is deceptive if it is a material misrepresentation, omission, act or practice that is likely to mislead consumers acting reasonably under the circumstances. A material representation, omission, act or practice involves information that is important to consumers and, hence, likely to affect their choice of, or conduct regarding, a product. An act or practice may be deceptive, within

> the meaning of Maine's Unfair Trade Practices Act, regardless of a defendant's good faith or lack of intent to deceive.

The court then found that such a data breach gives rise to a cognizable claim under Maine's UTPA. In its reasoning, the Maine court relied heavily on the First Circuit's decision in the TJX case. In that case, the plaintiffs asserted a claim under Chapter 93A, Massachusetts' consumer protection statute. The Maine court compared the language of both the Maine UTPA and Massachusetts statute and found them to be similar. *Compare* 5 M.R.S.A. §207 ("Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are declared unlawful."), *with* Mass. Gen. Laws. c. 93A, §2(a) ("Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful.").

In the TJX case, the court noted that to bring conduct within the "unfairness rubric of chapter 93A does not require that it have been specifically condemned by the FTC which has itself identified general factors to consider in identifying unfairness." In re TJX Companies Retail Sec. Breach, 564 F.3d 489 (2009). Rather, under Massachusetts law:

> Relying on FTC interpretations . . . the following are considerations to be used in determining whether a practice is to be deemed unfair: (1) whether the practice . . . is within at least the penumbra of some common-law, statutory, or other established concept of unfairness; (2) . . . is immoral, unethical, oppressive, or unscrupulous; (3) . . . causes substantial injury [to] . . . competitors or other businessmen.

Id. The court then found that using this criteria, if the charges in the plaintiffs' complaint are true, it could be found in the TJX case "inexcusable and protracted reckless conduct, aggravated by failure to give prompt notice when lapses were discovered internally, and causing very widespread and serious harm to other companies and to innumerable consumers. And such conduct, a court might conclude, is conduct unfair, oppressive and highly injurious – and so in violation of chapter 93A." Id.

E. Breach of Implied Contract

Plaintiffs also assert claims for breach of implied contract. In Hannaford, the court denied the defendant's motion to dismiss the plaintiffs' breach of implied contract claim. Both plaintiffs and defendants agreed that at the point of sale (the cash register), there exists a contract for the sale of groceries. The consumer bought groceries from Hannaford and, in exchange, paid Hannaford for those groceries. The court agreed that such a transaction was a contract for the sale of goods under Article 2 of Maine's Uniform Commercial Code. However, the parties disagreed over whether such a contract included an implicit agreement that, at the point of sale, the merchant will guaranty the consumer's electronic data against all intrusion.

The Hannaford Court found that such an implied term is a question of fact for a jury to decide. The court compared the obligation to safeguard electronic data to that of cash, coupons or checks. "If the consumer presents a check, Article 3 of Maine's Uniform Commercial Code

imposes various obligations and expectations as a matter of law. If the consumer tenders cash or coupons, a jury could reasonably find that the merchant is entitled to expect the currency or coupons to be authentic, not counterfeit, as an implied term of the contract of sale." In re Hannaford Bros. Co. Customer Data Security Breach Litig., 613 F. Supp. 2d 108, 119 (D. Me. 2009). Thus, the Court concluded:

> If a consumer tenders a credit card or debit card as payment, I conclude that a jury could find certain other implied terms in the grocery purchase contract: for example, that the merchant will not use the card data for other people's purchases, will not sell or give the data to others (except in completing the payment process), *and will take reasonable measures to protect the information (which might include meeting industry standards)*, on the basis that these are implied commitments that are absolutely necessary to effectuate the contract and indispensable to effectuate the intention of the parties. A jury could reasonably find that consumers would not tender cards to merchants who undertook zero obligation to protect customers' electronic data. But in today's known world of sophisticated hackers, data theft, software glitches, and computer viruses, a jury could not reasonably find an implied merchant commitment against every intrusion under any circumstances whatsoever.

Notably, despite the court's allowance of the plaintiffs' breach of implied contract claim to proceed as outlined above, it dismissed the plaintiffs' breach of implied warranty of fitness claim finding that Maine law did not apply an implied warranty of fitness to a grocery store's electronic payment processing systems.

Given the millions of consumers possibly impacted by the reported recent data breaches involving retailers and hospitality companies, the potential monetary exposures to those businesses in terms of costs, fines and damages may be substantial. At a minimum, consumer plaintiffs can be expected to seek the cost of credit monitoring, which may be a significant expense given the large number of plaintiffs. Far more ominous, however, are the potential claims of consumer plaintiffs and financial institutions for actual, statutory and punitive damages based on the theories outlined above. In the TJX case, the costs reached over $250m. Claims for damages of such magnitude will no doubt only serve to encourage the commencement of data breach litigation in ever increasing numbers in the future.

Data Security Legislation

There are well over 50 federal laws, in addition to state counterparts, that address issues related to cybersecurity. *Federal Laws Relating to Cybersecurity*, Eric A. Fischer, Congressional Research Service, June 20, 2013, Table 2. Some of those laws, including the Sherman Antitrust Act, were originally enacted in the 1800s. Id. Because many of the laws at issue were crafted long before the birth of internet, their use to protect information on the internet is often cumbersome. Moreover, the legislation that does exist tends to focus on an industry (such as health data), rather than data collection or storage more generally. However, while the heads of most federal agencies have pushed Congress for comprehensive legislation addressing cybersecurity, to date businesses need to continue to adhere to the hodgepodge of laws in existence. Some of the more prominent laws that regulate data maintained by businesses include the following:

Gramm-Leach-Bliley Act ("GLB Act") 15 U.S.C. §§ 6801-6809, which provides data security requirements for non-bank financial institutions. The dual focus of the Act, both requiring companies to protect sensitive data and to inform consumers as to how the data will be used, is monitored by multiple federal agencies including the FTC, FRB, OCC, SEC, NCUA, OTS and CFTC.

Fair Credit Reporting Act ("FCRA") 15 U.S.C §§ 1681-1681x, requires credit reporting agencies to use reasonable procedures to ensure only proper disclosure of consumer information and also imposes limitations on the use and disposal of consumer credit information.

Children's Online Privacy Protection Act (COPPA) 15 U.S.C. §§ 6501-06, places limitations and requires reasonable security measures for data about children collected online.

Health Insurance Portability and Accountability Act (HIPAA), 42 CFR Part 2, contains provisions that define and govern the use and disclosure of Personal Health Information (PHI). Importantly HIPAA rules do not only apply to health entities, for example, law firms that receive PHI as part of litigation matters are subject to HIPAA limitations.

In addition to these federal statutes, most states have data collection and privacy statutes as well, applying to the states themselves, their residents and businesses operating within their borders. While the scope of these statutes are similar, the specifics vary widely. State statutes outline the specific data types that the state law covers, from name and social security numbers in most, to retina and fingerprint data in others. Some states, such as North Dakota, include date of birth and mother's maiden name as protected information, *see* N.D. Cent. Code § 51-30-01, while most others do not. Many of the statutes also describe the type of investigation into a breach that is required, and the type and timing of notice to affected consumers following a data breach. Even the notice provisions themselves vary – while many states merely require notice in a reasonable period of time or "expeditiously," some states describe specific required language, which hampers a one-size-fits-all approach to notice. *See, e.g.*, Cal. Civ. Code §1798.82. The

myriad of laws certainly poses difficulty for businesses operating in multiple states and further highlights the importance of preparing your breach notice strategy long before a breach occurs.

Federal Agency Action

While the media focus surrounding data breach issues tends to focus on the consumers affected and resulting litigation, federal enforcement actions are also an increasing risk and business cost associated with data breaches. The FTC has been the most active federal agency in the area of cybersecurity, molding businesses' behavior under the guise of consumer protection. §5 FTC Act, 15 U.S.C.45(a), generally regulates unfair trade practices and is frequently used by the FTC to initiate enforcement actions against companies that the FTC maintains have failed to reasonably protect consumer data. The FTC focus has been quite broad, ranging from pursuing companies failing to limit data collection activities as described within their own privacy policies, to sanctioning companies for "unreasonably" failing to securely handle consumer data. Unfortunately, the reasonableness standard does not on its own provide much guidance for businesses, although the FTC's published consent decrees do outline business practices which it deems to be unreasonable.

Looking at the FTC's recent consent decree signed with Fandango provides a good illustration of the risks businesses face if they are subject to an FTC action. On March 28, 2014, the FTC announced that it had reached a settlement with Fandango related to Fandango's failure to reasonably protect consumer data in its mobile app. The FTC alleged that from 2009-2013, despite reassuring consumers that their data was secure, Fandango disabled the SSL certificate which would have verified that the communications were secure. On August 14, 2014, the FTC approved the final consent decree in the Fandango matter and outlined the steps that Fandango agreed to undertake. As part of the consent decree, Fandango agreed to take a number of steps to ensure the security of its consumer data and agreed to 20 years of monitoring by the FTC, with biennial third-party security audits. *See* FTC Enforcements, Cases and Proceedings, Fandango, LLC. http://www.ftc.gov/enforcement/cases-proceedings/132-3089/fandango-llc; Fandango consent decree, http://www.ftc.gov/system/files/documents/cases/140328fandangoorder.pdf. The Fandango agreement is typical and most of the FTC consent decrees require the affected entity to agree to the twenty years of auditing and monitoring by the FTC, in addition to additional recordkeeping requirements related to the monitoring.

The FTC's authority to undertake the enforcement actions, which at times appear to be an additional kick in the teeth to an entity already facing consumer suits related to a data breach, was recently affirmed by a federal district court in New Jersey. There, Wyndham Hotels challenged the FTC's authority under § 5 after the FTC filed a complaint against Wyndham following an incident in which Russian hackers stole consumer credit data from Wyndham's system. In denying Wyndham's motion to dismiss, the court affirmed both the FTC's authority under § 5 and concluded that the fact the FTC had not issued regulations outlining the standards it expected did not undermine its authority to act. FTC v. Wyndham Worldwide Corp., No. Civ. 13-1887, --F.Supp.2d--, 2014 WL 1349019 (D.N.J. April 7, 2014).

Executive Order 13636 and the NIST Cybersecurity Framework

On February 12, 2013, President Obama issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity." That order directed the National Institute of Standards (NIST) to develop a voluntary risk-based Cybersecurity Framework in conjunction with both public and private entities. The goal of the order and the standards was to develop a process through which entities could assess and manage cybersecurity risks that was both cost-effective and universally applicable, regardless of entity type and size.

One year later the NIST published the Cybersecurity Framework, which lays out this process. *See* Framework for Improving Critical Infrastructure Cybersecurity, NIST, Feb. 12, 2014, ver. 1.0, located at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf. ("The Framework"). The Framework is a "risk-based" approach to cybersecurity and is divided into three parts: Core, Tiers and Profile.

The "Core" of the Framework is a series of activities and outcomes and includes references to various standards to guide the conduct. There are five Functions (and multiple sub-Functions called categories and sub-categories) in the Core, which are Identify, Protect, Detect, Respond, Recover. The sub-categories under these functions describe the various areas and then set forth specific steps to be taken. For example, under the Function of Protect there are 6 categories (Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology). Each one of the categories has multiple subcategories with specific steps to be taken, such as "Audit/log records are determined, documented, implemented and reviewed in accordance with policy."

The "Tier" part of the Framework assesses where the particular entity stands with its cybersecurity efforts to date. There are 4 Tiers: Partial, Risk Informed, Repeatable, and Adaptive. The NIST encourages users of the Framework who are still at Tier 1 (Partial) to attempt to move up to the next level and so on. Contained within the Tier section is a framework for assessing at which Tier an entity stands at a given time and also which Tier they seek to reach.

Lastly, the Profile section of the Framework is where the first two parts are aligned with the particular entity's business requirements, risk tolerance and resources. Businesses are instructed to develop both a "current" Profile and a "target" Profile to help identify achievements and gaps.

The Framework also contains a very helpful table (Table 2) that illustrates the application of the Framework. The NIST indicates that the Framework document will be continually updated as needed. While the Framework by definition is "voluntary," it is expected that utilizing the processes within the Framework may be necessary in order for a business' conduct to be viewed as "reasonable" in both enforcement and civil actions.

Resources

National Conference of State Legislatures Compilation of State Data Breach Laws, *see* http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

The FTC has also published a number of guides for businesses which outline the basic legal obligations for companies that handle personal information about consumers or employees. *See* http://business.ftc.gov/privacy-and-security/data-security

The Council on Cybersecurity: The Critical Security Controls for Effective Cyber Defense, 5.0. *See* http://www.counciloncybersecurity.org/ and https://ccsfiles.blob.core.windows.net/web-site/file/c9665df3a5f54d2b8e6edab493c3b076/CSC-MASTER-VER50-2-27-2014.pdf?sv=2012-02-12&st=2014-09-11T18%3A34%3A36Z&se=2014-09-11T18%3A36%3A36Z&sr=b&sp=r&sig=C3MmgpL2aCys%2B3%2BEV3P8jYvr7Z8yUaYMC2OOaBUNc2Q%3D.

EU Cybersecurity initiatives and guidelines. *See* http://ec.europa.eu/digital-agenda/en/cybersecurity

Federal Laws Relating to Cybersecurity, Eric A. Fischer, Congressional Research Service, June 20, 2013, Table 2

The "Framework," http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf