New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 254—NO. 29
WEDNESDAY, AUGUST 12, 2015

Outside Counsel

Expert Analysis

Counsel's Capacity To Control Cybersecurity Costs

By **A. Jonathan Trafimow**

And **Steven S. Rubin**

As the average cost of a data breach in the United States approaches $7 million,[1] companies must prepare to mitigate such an incident or close their doors. Appropriate legal and technical preparation can help to reduce the adverse consequences of an attack. Currently, based on the nature of a company's business and the information it collects, a myriad of laws and regulations may apply. Failure to take appropriate steps to adequately come into compliance subjects a business to enforcement actions by agencies, lawsuits from affected consumers and fines under various state regulations.

Compliance with the number and complexity of federal and state cybersecurity laws and regulations is no simple task. An essential part of a cybersecurity program is a written information security plan (WISP),[2] which sets forth the company's methodologies in identifying, protecting, detecting and responding to incidents and creates a network of relationships with experts to contact in the event of a suspected breach. WISPs, which have been used by various government agencies over the past several years in developing security procedures, are now being used by many companies.

A WISP not only allows a company to identify and address potential compliance issues, but also incorporates legal principles to mitigate damages in the event of an incident. A WISP also provides guidance and procedures to each department on how it should handle information. A WISP provides a structure to manage a company's compliance and respond to incidents.

A WISP not only allows a company to identify and address potential compliance issues, but also incorporates legal principles to mitigate damages in the event of an incident.

Authority to Regulate

It is not clear what authority various administrative agencies have to regulate cybersecurity under existing laws. We do know, however, that where an agency has statutory authority to regulate, courts usually will accept the agency's reasonable interpretation of the extent of that authority.

For example, under section 5(a) of the Federal Trade Commission Act (FTCA), the Federal Trade Commission (FTC) may sue any business subject to its jurisdiction for engaging in "acts or practices in or affecting commerce" that are "unfair" or "deceptive." 15 U.S.C. §45(a)(1) (2006). In *FTC v. Wyndham Worldwide Corp.*, 10 F.Supp.3d 602 (D.N.J. 2014), the FTC alleged that a private company that manages hotels and time shares violated the FTCA by failing to take appropriate security measures to protect the sensitive personal data it collected and maintained of consumers.

The FTC is not the only federal agency to assert the jurisdiction to regulate cybersecurity practices. The SEC, Office of Comptroller of the Currency (OCC) and Federal Communications Commission have all implemented regulations requiring companies to adopt policies and procedures that address administrative, technical, and physical safeguards. Several agencies have gone even farther, implementing industry-specific regulations.

The SEC announced that companies should disclose in their registration statements (pursuant to the Securities Act of 1933) and in their periodic reports (pursuant to the Securities Exchange Act of 1934) cyber risks and incidents which may affect the value of a security.[3] The OCC requires the implementation of a comprehensive written information security program for any national banks and federal savings associations. For these and other regulations, the agency responsible for enforcement has provided little guidance as to what would constitute legally compliant security standards.

As the law develops, WISPs may become an industry best practice. Some states have already implemented statutes that require companies to develop and maintain an information security program. Massachusetts law requires any person who owns or licenses information about a resident to develop, implement and maintain a writ-

A. JONATHAN TRAFIMOW *and* STEVEN S. RUBIN *are partners at Moritt Hock & Hamroff.* STEPHEN E. BREIDENBACH, *a law student, assisted in the preparation of this article.*

ten information security program. The program must include administrative, technical and physical safeguards appropriate to the business' size, information exposure, storage and type. In Oregon, any business in possession of personal information must implement a similar information security program. However, the Oregon regulation specifically requires that the business set in place methods to identify reasonably foreseeable internal and external risks, address the risks that come up and regularly test to make sure such methods are functioning appropriately.

Cybersecurity Framework

On Feb. 12, 2013, President Barack Obama signed Executive Order 13636 which, among other things, identified 16 industries deemed essential to the nation's Cybersecurity Infrastructure (the "Critical Infrastructure"), and directed The National Institute of Standards and Technology to develop a Cybersecurity Framework (NIST Framework). Following the release of the draft standards, on Feb. 12, 2014 the final NIST Framework took effect. This standard, having its origins from a Presidential Executive Order, has quickly become the authority for companies seeking to assess their cybersecurity compliance.

For companies that are and are not in the Critical Infrastructure, promulgation of the NIST Framework along with cases like *FTC v. Wyndham* raise challenging questions of regulatory compliance. The FTC has already stated that the NIST Framework "is fully consistent with the FTC's enforcement framework"[4] as to matters of risk assessment and mitigation. In fact, several FTC enforcement actions arose from failure to implement measures consistent with the NIST Framework's subcategories.

In *CBR Systems*, the FTC brought an action against the defendant for failing to implement measures to protect data in transit (NIST Framework PR.DS-2) and further failing to implement sufficient measures to prevent, detect, and respond to unauthorized access to their computer networks.[5] In *BJ's Wholesale Club*, the FTC brought an enforcement action alleging that the defendant failed to: transmit data in an encrypted format (NIST Framework PR.DS-2), disable default usernames/passwords (NIST Framework PR.AC-1) and implement intrusion detection systems (NIST Framework DE.CM-1).[6] As a result, both companies were subjected to fines, were required to implement a comprehensive information security plan and obligated to obtain audits by an independent third-party security professional every other year for 20 years. These remedial measures could have been avoided if these companies had a properly implemented WISP.

Role of WISP

The FTC has made it clear that reasonable cybersecurity does not mean perfect security, but it does mean a business must continuously assess and address current risks.[7] A WISP structures a company's review and organization of its cybersecurity infrastructure and facilitates improvements. For example, a WISP can develop a record of how a company: identifies sensitive information, addresses threats, manages risk and continuously improves its security infrastructure by learning from previous incidents. Without such a structure, a business may fail to recognize a critical component of its cybersecurity framework and will be less prepared to respond to a security breach quickly and effectively.

The FTC has made it clear that reasonable cybersecurity does not mean perfect security, but it does mean a business must continuously assess and address current risks.

A WISP can also potentially limit legal liability by showing that the company took reasonable steps to protect its data. Victims of a data breach may assert a variety of statutory, contractual, quasi-contractual and tort causes of action, such as: negligence, breach of contract, conversion, unjust enrichment, violation of state consumer protection statutes and misrepresentation. Many of these actions originate from a company having failed to implement security mechanisms that were deemed reasonable industry practices. However, if a company can prove its data was protected by cybersecurity practices consistent with industry best practices a court may be inclined to consider an early dismissal of the action.

Thus, a properly drafted WISP will require that a company's breach response be documented and will be consistent with evidentiary rules. In responding to an incident, a company should know not only the appropriate information to preserve but also, how to maintain that information in an admissible format. As shown below, a company's awareness and ability to demonstrate its compliance is imperative to avoiding legal liability.

Privilege and Work Product

Legal counsel is an integral part of the WISP creation process, among other reasons, because the utilization of legal advice in connection with the WISP creates an argument that at least some aspects of the process are shielded from disclosure in litigation because of the attorney-client privilege or attorney work product doctrine. If legal counsel played no role, information provided to a company from a computer security professional would most likely be discoverable in litigation. For example, if a security professional advised a company of the need to install a virus scan, the company failed to implement that suggestion, and later, was breached because an employee downloaded malware onto the unprotected computer, plaintiff's attorney most likely could obtain the professional's report and offer evidence that the company received and ignored the precaution.

While a court may or may not accept assertions of privilege in this context, courts have repeatedly recognized that "full and frank communication between attorneys and their clients…promote

broader public interests in the observance of law and administration of justice." *Upjohn Co. v. United States*, 449 U. S. 383, 389 (1981), quoted in *Swidler & Berlin v. United States*, 524 U.S. 399, 403 (1998).

In the corporate context, the U.S. Supreme Court identified a number of factors that bear on whether a communication is privileged, including: Were the communications made by company employees to company lawyers, each acting in that capacity; whether the communications concerned matters within the employees' scope of corporate duties; whether the employees' communications were made to counsel at the direction of corporate security; whether the communications were made to secure the corporation legal advice from counsel and the employees understood that they were being questioned so that the corporation could obtain legal advice; whether the communications were confidential and employees understood them to be confidential; whether the information needed from the investigation could be obtained from senior management; and whether the communications were kept confidential by limiting their dissemination. *Upjohn*, 449 U.S. at 394-95.

The New York Court of Appeals has endorsed the Upjohn standard as an "intermediate standard" which extends to "communications with low- and mid-level employees." See *Niesig v. Team I*, 76 N.Y.2d 363, 371 (N.Y. 1990);.

Privileged information shared with a consultant who has been retained by a law firm for the purpose of assisting with legal advice also may be protected under the attorney-client privilege. Where a lawyer needs outside help to provide effective consultation to the lawyer's client, the attorney-client privilege may attach. *United States v. Kovel*, 296 F.2d 918, 922 (2d Cir. 1961) ("What is vital to the privilege is that the communication be made in confidence for the purpose of obtaining legal advice from the lawyer.") "Nevertheless, the extension has always been a cabined one, and '[t]o that end, the privilege protects communications between a client and an attorney, not communications that prove important to an attorney's legal advice to a client.'" *United States v. Mejia*, 655 F.3d 126, 132 (2d Cir. 2011) (quoting *United States v. Ackert*, 169 F.3d 136, 139 (2d Cir. 1999).

The work product doctrine, partially codified by Rule 26(b)(3) of the Federal Rules of Civil Procedure, "is intended to preserve a zone of privacy in which a lawyer can prepare and develop legal theories and strategy 'with an eye toward litigation,' free from unnecessary intrusion by his adversaries." *United States v. Ghavami*, 882 F.Supp.2d 532, 539 (S.D.N.Y. 2012) (internal citations omitted); see also *Doe v. Poe*, 244 A.D.2d 450, 451-52 (App. Div. 1997) aff'd, 92 N.Y.2d 864 (App. Div. 1998).

To be covered by the doctrine, a document must have "been prepared in anticipation of litigation by or for a party, or by the party's representative." *Ghavami*, 882 F.Supp.2d at 539 (internal citations omitted). The doctrine encompasses an attorney's mental impressions, which is entitled to virtually unlimited protection, as well as fact work product, which may be ordered disclosed upon a showing of substantial need. Id. at 540 (internal citations omitted). Both the attorney-client privilege and attorney work product can be waived. Id. (internal citations omitted).

The generation of a WISP may require the hiring of outside vendors as well as communication with different levels of staff hierarchy. All communications should include provisions explaining that the information is confidential and being gathered for the purpose of rendering legal advice. The communications should be limited and the attorney should assess: (1) what information is being communicated, (2) whether the employee being communicated with is in the best position to know the information being sought, (3) how the information relates to the law the business is attempting to comply with and (4) that the employee being communicated with understands the company intends to keep the information confidential.[8]

While questions an attorney asks are protected, the subject matter obtained by those questions is not. For example, even if a court held that company's WISP was privileged in a particular case, the court could also decide that other information about the company's cybersecurity practices was discoverable. Alternatively, if the underlying information was unavailable, our hypothetical plaintiffs' counsel might renew the argument for access to at least certain sections of the WISP. Information that is attorney work product may nevertheless be discoverable if: (1) the facts are essential to the case and (2) cannot be obtained without undue hardship. Fed. R. Civ. P. 26. Suffice it to say that litigation involving WISPs drafted with the assistance of legal counsel may involve disputes regarding assertions of both the attorney-client privilege and the attorney work product doctrine.

Most businesses face complex and growing cybersecurity concerns. Business lawyers can bring real value to their clients by addressing these concerns and reducing their clients' liability risks. WISPs are an important option to consider.

1. Ponemon Institute, 2015 Cost of Data Breach Study: Global Analysis 2 (2015), http://www-03.ibm.com/security/data-breach/.

2. See, e.g., 12 C.F.R. Part 364, app. B; 16 C.F.R. §314.3.

3. Division of Corporation Finance, SEC, CF Disclosure Guidance: Topic No. 2 (October 13, 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

4. Julie Brill, FTC, On the Front Lines: The FTC's Role in Data Security (Sept. 17, 2004), http://www.ftc.gov/system/files/documents/public_statements/582841/140917csisspeech.pdf.

5. FTC, Cord Blood Bank Settles FTC Charges that it Failed to Protect Consumers Sensitive Personal Information (Jan. 28, 2013), http://www.ftc.gov/news-events/press-releases/2013/01/cord-blood-bank-settles-ftc-charges-it-failed-protect-consumers.

6. FTC, BJ's Wholesale Club Settles FTC Charges (June 16, 2005), http://www.ftc.gov/news-events/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges.

7. FTC, Discussion Draft of H.R.__, Data Security and Breach Notification Act of 2015 (March 18, 2014), https://www.ftc.gov/system/files/documents/public_statements/630961/150318datasecurity.pdf.

8. *Upjohn Co.*, 449 U.S. at 395-96.