Meeting Your Cybersecurity Obligations

By Steve Rubin and A. Jonathan Trafimow

The Federal Trade Commission ("FTC"), currently the predominate enforcer of cybersecurity regulations, has commented that "security is an ongoing process of using reasonable and appropriate measures in light of the circumstances"[1] which is not covered by any checklist.[2] Failure to take appropriate steps to adequately come into compliance subjects a business to possible enforcement actions by agencies, lawsuits from affected consumers and fines from various state regulations. Compliance with the number and complexity of federal and state cybersecurity laws and regulations is no simple task. In this evolving legal environment, a Written Information Security Plan ("WISP") provides the necessary structure companies need to identify and implement conforming practices. A WISP not only allows a company to adapt to industry and regulatory changes, but also incorporates legal principles to mitigate damages in the event of an incident.

Cybersecurity Regulations—Specific and General

Nearly every business is subject to some form of cyber security regulation. The U.S. Securities and Exchange Commission (the "SEC"), Office of the Comptroller of the Currency (the "OCC"), and Centers for Medicare & Medicaid Services (the "CMS"), along with several other state and federal agencies, have all begun to incorporate cybersecurity principles into their regulations. This has led to a myriad of rules, each having its own jurisdictional scope and requirements. These rules generally require a number of technical safeguards, such as the implementation of firewalls, anti-virus software, system audits and that the company's security standards be documented. But, depending on the type of information a business collects, agencies may also impose additional constraints. Where information has traditionally been highly regulated, agencies have begun to require specific safeguards. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") requires that covered entities restrict and document access to protected health information;[3] determine which applications are important to patient care;[4] and record the movement of hardware and electronic media.[5] For registered investment companies and advisors, the SEC has provided that failure to prepare for a cyber incident could result in a breach of their fiduciary obligations,[6] and make the company liable for fraudulent activity.[7] The SEC has also suggested that a covered entity's cybersecurity obligations may extend to commercial or market-sensitive information.[8] Finally, the Sarbanes-Oxley Act of 2002 ("SOX") imposes severe penalties on corporate officials who fail to implement internal controls, including technical safeguards,[9] to ensure the truth and accuracy of each annual or quarterly report.[10]

Even when a company's practices are not regulated by the above agencies, they may still be subject to the regulations of the FTC. Under section 5(a) of the Federal Trade Commission Act ("FTCA"), the FTC may sue any business subject to its jurisdiction for engaging in "acts or practices in or affecting commerce" that are "unfair" or "deceptive."[11] The FTC has brought several actions against defendants where those defendants claimed to have reasonable security, but failed to implement sufficient measures to prevent, detect, and respond to unauthorized access to their computer networks.[12] As a result, companies have been subjected to fines, required to implement a comprehensive information security plan and obligated to obtain audits by independent third party security professionals for 20 years.

A company's compliance obligations do not stop with its internal practices, but also extend to their relations with company affiliates. In *GMR Transcription Services, Inc.*, the FTC found that the defendant failed to implement reasonable and appropriate security by not contractually requiring appropriate safeguards and not monitoring its vendor to ensure its compliance.[13] While a company may not be able to directly control its affiliates' practices, a business can nonetheless take precautions to show that it assessed its affiliates' cybersecurity and required them to implement appropriate safeguards.

As a part of any information security program, counsel should review any vendor agreements along with its vendor's WISPs and security audits. Attorneys should make sure that these agreements include, among other things, a provision mandating notification if the vendor updates its security practices or significantly changes its operating procedures. While it is unclear what constitutes appropriate monitoring, counsel should review its vendors' WISPs to assess their cybersecurity practices. Depending on the nature of the information being shared, it may be necessary to require the vendor to undergo a security audit immediately or at random intervals throughout the business relationship.

A company's cybersecurity practices need not be perfect. Where a company has taken every reasonable precaution, the FTC has provided that a breach "will not violate the laws that [it] enforces."[14] Companies seeking to implement appropriate cybersecurity safeguards should ensure their WISP is in compliance with the National Institute of Standards and Technology's Cybersecurity Framework ("NIST Framework"). In response to growing cybersecurity concerns, President Obama signed Executive Order 13636 which directed the National Institute of Standards and Technology to develop a Cybersecurity Framework. Following the release of the draft standards, on February 12, 2014, the final NIST Framework took effect. The FTC

has already stated that the NIST Framework "is fully consistent with the FTC's enforcement framework"[15] as to matters of risk assessment and mitigation.

WISP Comes to the Rescue

As an essential part of a cybersecurity program and before a potential breach occurs, companies need to develop a WISP, an internal company document that enumerates a company's regulatory requirements, risks and responses to determine its conformity. A WISP identifies and ranks the critical components of a business according to its business objectives and legal obligations. The company can then concentrate its available resources in areas requiring heightened security and elimitate those where such protection is not incumbent. As a company's obligations fluctuate, a WISP offers an effective means of continuing to provide appropriate safeguards.

As a result of technological developments and changes in business practices, companies must continuously adapt their security structure to meet the demands of new regulations and industry best practices. Events such as acquiring business from other countries, outsourcing company functions and utilizing new software can all have profound effects on a business's compliance needs. A WISP pinpoints how data traverses a company's network and helps identify gaps in its security practices. A company can then assess potential risks and implement reasonable cost-effective responses to meet its regulatory requirements.

While the law continues to struggle to keep up with technology, old regulations may be interpreted broadly in an attempt to address the technologically changing landscape. 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 adapt to the evolving law.

A WISP Can Limit Customer Actions

The benefits of a WISP are not limited to proving a company's regulatory compliance; it also has the potential to limit customer lawsuits by showing a company took reasonable steps to protect its data. As discussed below, companies that can demonstrate that their stolen data was effectively protected or that they employed reasonable practices but could not prevent an incident (both of which are required in a WISP), may persuade a court to dismiss an action. In one case, several tapes containing protected information, including medical records and social security numbers, were stolen.[16] Yet, the court determined that the plaintiffs had not suffered an injury-in-fact because defendant's practice of storing encrypted data on tapes made it unlikely the attacker would be able to "open and decipher" the stolen information.[17] In another case, the court found that even though unencrypted customer data was stolen, the company had not violated its duty of reasonable care.[18] The court reasoned the event was unforeseeable, and that defendant acted reasonably by "transmitt[ing] and us[ing] data in accordance" with its WISP.[19]

Lawyers Provide Even More Protection by Protecting Your WISP

Legal counsel is an integral part of the WISP creation process 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. Where a lawyer needs outside help to provide effective consultation to the lawyer's client, the attorney-client privilege may attach.[20] 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."[21] The doctrine protects an attorney's mental impressions, which receive virtually unlimited protection, and work product.[22] Both the attorney-client privilege and attorney work product can be waived.[23] As constructing a WISP requires a thorough review of a company's procedures and technical practices, counsel should take every precaution to preserve a company's potential claims of privilege and work product.

Conclusion

While technology continues to evolve, so will the complexities of a company's cybersecurity obligations. It will not be long before all companies are subjected to at least some form of cybersecurity compliance. Having a properly drafted WISP can help your business comply with this ever-changing legal environment.

Endnotes

1. Orson Swindle, *Prepared Statement of the Federal Trade Commission On Protecting Our Nation's Cyberspace*, FED. TRADE COMM'N (Apr. 21, 2004) (statement of Orson Swindle, Former Commissioner, FTC), https://www.ftc.gov/public-statements/2004/04/prepared-statement-federal-trade-commission-protecting-our-nations.
2. Joseph J. Lazzarotti, *Checklists Not Enough When Developing a WISP, FTC Director Comments at IAPP Global Privacy Summit*, NAT'L L. REV. (Mar. 9, 2015), http://www.natlawreview.com/article/checklists-not-enough-when-developing-wisp-ftc-director-comments-iapp-global-privacy.
3. 45 C.F.R. § 164.308(a)(4)(ii)(A) (2013); 45 C.F.R. § 164.308(a)(4)(ii)(C).
4. *Id.* § 164.308(a)(7)(ii)(E).
5. *Id.* § 164.310(d)(2)(iii).

6. *See, e.g.*, 17 C.F.R. § 270.17j-1 (2012); 17 C.F.R. § 275.204A-1.
7. *See, e.g.*, 17 C.F.R. § 270.17j-1 (2012); 17 C.F.R. § 275.204A-1.
8. SEC, IM GUIDANCE UPDATE No. 2015-02 2 (2015), http://www.sec.gov/investment/im-guidance-2015-02.pdf.
9. Auditing Standard No. 5, PUB. CO. ACCOUNTING OVERSIGHT BD. (2007), http://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_5.aspx (Under section 36 audits include a review of the "effect of information technology on internal controls over financial reporting.").
10. 15 U.S.C. § 7241 (2002).
11. *Id.* § 45(a)(1).
12. *Cord Blood Bank Settles FTC Charges That It Failed to Protect Consumers Sensitive Personal Information*, FED. TRADE COMM'N (Jan. 28, 2013), http://www.ftc.gov/news-events/press-releases/2013/01/cord-blood-bank-settles-ftc-charges-it-failed-protect-consumers; *BJ's Wholesale Club Settles FTC Charges*, FED. TRADE COMM'N (June 16, 2005), http://www.ftc.gov/news-events/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges.
13. *Provider of Medical Transcript Services Settles FTC Charges That It Failed to Adequately Protect Consumers' Personal Information*, FED. TRADE COMM'N (Jan. 31, 2014), https://www.ftc.gov/news-events/press-releases/2014/01/provider-medical-transcript-services-settles-ftc-charges-it.
14. Orson Swindle, *Prepared Statement of the Federal Trade Commission On Protecting Our Nation's Cyberspace*, FED. TRADE COMM'N (Apr. 21, 2004), https://www.ftc.gov/public-statements/2004/04/prepared-statement-federal-trade-commission-protecting-our-nations ("Although a breach may indicate a problem with a company's security, breaches can happen...even when a company has taken every reasonable precaution. In such instances, the breach will not violate the laws that the FTC enforces.").
15. FED. TRADE COMM'N, ON THE FRONT LINES: THE FTC'S ROLE IN DATA SECURITY (2004), http://www.ftc.gov/system/files/documents/public_statements/582841/140917csisspeech.pdf.
16. *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14 (D.D.C. 2014).
17. *Id.* at 29.
18. *Guin v. Brazos Higher Educ. Serv. Corp.*, No. Civ. 05-668 RHK/JSM, 2006 WL 288483 , (D. Minn. Feb. 7, 2006).
19. *Id.*
20. *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.").
21. *United States v. Ghavami*, 882 F. Supp. 2d 532, 539 (S.D.N.Y. 2012) (internal citations omitted) (The work product doctrine, partially codified by Rule 26(b)(3) of the Federal Rules of Civil Procedure, is designed to allow "a lawyer [to privately] prepare and develop legal theories and strategy 'with an eye toward litigation.'"); *see also* Doe v. Poe, 244 A.D.2d 450, 451-52 (N.Y. App. Div. 1997), *aff'd*, 92 N.Y.2d 864 (N.Y. App. Div. 1998); *Bras v. Atlas Constr. Corp.*, 153 A.D.2d 914, 915-16 (N.Y. App. Div. 1989).
22. *Ghavami*, 882 F. Supp. 2d at 540.
23. *Id.* (internal citations omitted).

Steven S. Rubin is a partner at Moritt Hock & Hamroff LLP where he chairs the firm's patent practice and co-chairs the firm's cybersecurity practice. With an electrical engineering background, Mr. Rubin concentrates his practice on all phases of patent-related matters, both domestically and internationally.

A. Jonathan Trafimow is a partner at Moritt Hock & Hamroff LLP where he chairs the firm's employment practice and co-chairs the firm's cybersecurity practice. Mr. Trafimow represents employers in all areas of workplace discrimination, retaliation, harassment and civil rights claims, and class actions. He also routinely advises employers on compliance with local and federal employment laws and regulations.

The authors thank Stephen E. Breidenbach, student of the Maurice A. Deane School of Law at Hofstra University, for his assistance in the research and drafting of this article.