FALL 2016 E-NEWSLETTER

At Digital Mountain we assist our clients with their cybersecurity, computer forensics and e-discovery needs. For this E-Newsletter, we focus on the topic of ransomware and the information security, legal and financial impact it has on organizations.

RANSOMWARE - LEGAL LIABILITY AND ENFORCEMENT

Judge-made law or "case law" is useful because it provides crucial insight to the public regarding how similar cases should be resolved. As time passes and similar cases are adjudicated, the public receives increased certainty regarding the outcome of similar cases. Unfortunately, case law inherently lags behind real-time events, so when individuals and organizations use new technologies or use old technologies in novel ways it's difficult to predict the legal repercussions. This is especially true for those seeking guidance on liability for ransomware, malicious software that locks critical files and systems and demands payment for the key. This article highlights concerns and obligations for organizations seeking to understand ransomware liability.

Although most case law about ransomware involves interagency litigation designed to disrupt the physical infrastructure of large ransomware operations, agency enforcement actions, such as those brought by the Federal Trade Commission ("FTC") and the Department of Health and Human Services' Office of Civil Rights, provide examples of when an organization, even as a ransomware victim, may be held accountable for security failings.

Shabby Security is "Unfair and Deceptive"

Since 2000, the FTC has brought roughly 60 enforcement proceedings against organizations alleging unreasonable data security practices in violation of Section 5 of the FTC Act as an unfair and/or deceptive trade practice. Recently, the FTC alleged that ASUS failed to patch pervasive bugs in its network routers, causing harm to consumers, and that ASUS did not timely disclose the vulnerabilities when it became aware of them. Most companies, including Google, Microsoft, Facebook, and ASUS, have succumbed to the pressure of the FTC, entering into consent agreements that provide the terms of the settlement agreement (often no admission of guilt and no monetary fines unless the organization violates the agreement, which usually provides for 20 years of FTC oversight related to an organization's security practices). Although these enforcement proceedings do not directly relate to ransomware, the enforcement proceedings focus on the overall security hygiene of an organization and not the particular malware variant affecting the

organization. Thus, it is safe to assume that ransomware attacks will trigger investigations into the overall security posture that led to the infection of ransomware – according to the FTC, relaxed security (depending on the type of data secured and facts of the incident) is an unfair act and practice.

The FTC's enforcement of reasonable data security is not going to slow down, especially in light of the 3rd Circuit's ruling in *FTC v. Wyndham Worldwide Corp* (a case challenging the FTC's jurisdiction related to data security), because the court held that the FTC is appropriately wielding its power despite not providing *specific* notice to organizations of what security protocols are required (i.e., the FTC has not and does not plan to publish specific rules and regulations related to data security).

Notably, the FTC has investigative and enforcement powers for many other laws that impact different sectors of the economy (e.g., healthcare and financial services). In fact, the court in *Wyndham* used the term "coexist" to characterize the relationship between Section 5 and other data regulations. Furthermore, when asked about FTC's Section 5 and HIPAA, Jay Mayfield of the FTC's Office of Public Affairs said, "Nothing in the regulations prohibits the FTC from pursuing actions against doctors and hospitals," despite other regulations, such as HIPAA's Security Rule and Breach Notification Rule.

The Healthy Protection of ePHI

The US Department of Health and Human Services (HHS), through their Office of Civil Rights, publishes annual guidelines for interpreting and complying with the Security Rule. The HHS Security Rule provides the obligations related to ensuring security of electronically protected health information (ePHI). The HHS' factsheet[1] on ransomware reports that in early 2016, nearly four thousand daily ransom-driven attacks were conducted, up from approximately one thousand per day a year earlier. Clearly, there's cause for concern.

Organizations that encounter ransomware experience a rush of negative emotions. Now let's say that your organization stores electronically protected information of patients or consumers. In this case, a second wave of frustration will come when government agencies deem the ransomware attack as a data breach. That's right, organizations that store protected information, health, personal, or financial, are responsible for proactively protecting that data against a ransomware attack – actual or anticipated. Resulting investigations will focus on the organization's efforts to prevent the attack, and the organization's response following the attack.

Let's dive a bit deeper into the rules and regulations that apply:

HIPAA Security Rule (45 C.F.R. §§ 164.302 – 318.)

This is the governing rule for organizations that collect, receive, transmit, and/or store ePHI. There are several key practice points that are essential for compliance.

1. The first step in the assessment is to determine if ePHI exists in an organization's stored data. The definition of ePHI is covered under Section 1171 of Part C of Subtitle F of Public Law 104-191, the HIPAA Administrative Simplification section. Again, in concise form, ePHI is any information on health (physical or mental), treatment, or payment for treatment which could reasonably identify an individual, and is collected, stored, transmitted, or received electronically. Because the definition makes no mention of any product or service provided in conjunction with the collection of ePHI, employers who collect ePHI as part of an application for group health insurance benefits are subject entities, as are schools and universities that collect physical exam forms or vaccination records.

2. Once a determination is made that ePHI is a part of stored data, the organization is *required* to conduct a risk analysis of protection efforts, strategies employed, vulnerabilities, and corrective actions. The risk assessment should then be documented with a remediation plan. A plan for periodic review should also be included.

3. In the event of a ransomware attack, it's important to note that an organization may be subject to the Breach Notification Rule (45 C.F.R. 164.400-414). This rule sets out the steps that must be taken following a security incident, whether or not the incident successfully exposed ePHI beyond the organization's network. HHS treats any security incident as a data breach unless the organization can prove a "…low probability that the PHI has been compromised." If the breach affects five hundred people or more, the breach must be reported to the media.

4. Once the required/recommended notifications have been made, the organization is required to pursue containment and remediation strategies. From that point, the organization may be subject to investigation by HHS, and potential fines. The HHS investigation process concludes with either a determination of non-violation, a voluntary compliance agreement of some kind, or a formal violation. If HHS determines there was criminal conduct involved, HHS notifies the Department of Justice, which conducts a separate investigation.

HHS' reporting indicates that the investigation and resolution process is responsible for the adjudication of the majority of cases.

Gramm-Leach-Bliley Act

Also known as the Financial Services Modernization Act of 1999, Gramm-Leach-Bliley Act (GLBA) recognized that when relaxing regulations on mergers of financial institutions such as banks, insurance companies, and brokerage houses, the risk of exposure for personal data would increase. Title V of the Act, (15 USC 94 §§6801 – 6827), specifically addresses the disclosure and fraudulent access to information covered by the Act. The Act covers financial institutions and requires notification of data privacy and protection policies, such as developing, implementing, and maintaining a comprehensive written information security plan, which must include particular attributes (e.g., designated manager; risk assessments; monitoring and testing; vendor/3P management controls).[2] GLBA's Safeguards Rule is often used in conjunction with the FTC's Section 5 authority to bring actions against financial institutions that fail to properly protect consumer financial information. In what may be a prescient move for increased enforcement, the FTC opened a public comment period on the security provisions of GBLA effective August 29, 2016.

Conclusion: Not so Cryptic

Despite the low volume of available case law, the trend with respect to government enforcement of organization liability after a ransomware attack is an easy read. The rules and regulations indicate that knowing the data exists constitutes a responsibility to protect it, irrespective of an actual attack or a perceived threat. The increase in ransom-driven attacks should make organizations sit up and take notice that if risk assessments haven't been conducted, they should be, and corrective action taken to prevent vulnerabilities. Case law may lag, but cybercriminals don't.

[1] http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf
[2] e.g., In the Matter of ACRAnet, Inc., No. C-45331 (F.T.C. Aug. 17, 2011).

UPCOMING INDUSTRY EVENTS

October 2016
Privacy + Security Forum,
Washington, DC: October 24-26

The Sedona Conference Working Group 1 on Electronic Document Retention,
Atlanta: October 27-28

November 2016
Georgetown Law's The Advanced EDiscovery Institute,
Washington, DC: November 10-11

December 2016
Association of Defense Counsel Annual Meeting,
San Francisco: December 8-9

Click here to see more upcoming events and links

Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: