Nassau Lawyer

April 2017 www.nassaubar.org Vol. 66, No. 8

Data Breaches and the Cost of Delay and Disorganization

Of the many risks facing organizations today, the most prominent may be the risk of a data breach. In New York, a data breach is an unauthorized acquisition of computerized data, which compromises the security, confidentiality or integrity of private information.1 Whether the data breach is the result of a cyberattack or an inadvertent disclosure of confidential information, an organization faces a myriad of costs and liabilities, including, but not limited to, liabilities from civil litigation, governmental investigations and enforcement actions, as well as legal, investigative, remediation and expert consulting fees, and reputational harm and loss of business.

To mitigate the potential impact, it is essential that an organization manages and deals with a data breach in a prompt and organized manner. As provided in this article, delay and disorganization can have severe consequences and exponentially increase the liabilities of an organization.

Federal and State Regulatory Agencies Impose Costs and Liabilities for Delay

Recently, the first Health Information Portability and Accountability Act (HIPAA) enforcement action based upon the lack of a timely breach notification was announced by the U.S. Department of Health and Human Services, Office for Civil Rights (OCR).2 Presence Health, one of the largest healthcare networks in Illinois, agreed to pay $475,000 to settle potential violations of the HIPAA Breach Notification Rule. Presence Health filed a breach notification report with OCR concerning the protected health information (PHI) of 836 individuals that went missing, including individuals' names, dates of birth, medical record numbers, dates and types of procedures.3

After discovering the missing PHI, however, OCR's investigation revealed that Presence Health failed to notify such individuals without unreasonable delay and within sixty days of discovering the breach.4 Additionally, Presence Health failed to notify prominent media outlets as required by law.5 While the delay appeared to be due to an internal miscommunication and not a deliberate violation of the rule, the lesson learned is that disorganization and delay is costly and violations will be strictly enforced.6

Costly penalties and impact from delay and disorganization are not limited to the health care arena. On September 13, 2016, Governor Cuomo and the New York State Department of Financial Services (NYDFS) proposed a sweeping new cybersecurity regulation that imposes rigorous cybersecurity requirements on banks, consumer lenders, insurance companies and other financial institutions regulated by the NYDFS. The regulation is effective as of March 1, 2017.7 Along with requiring cybersecurity policies and risk assessments to be put into place, NYDFS requires a breach notification to the Superintendent within seventy-two hours of a cybersecurity event that either (1) requires notification to any other government body; or (2) has a reasonable likelihood of materially harming any material part of the normal operations of the business.8

As part of the regulation, the chair of the board or another senior officer must certify in writing to the superintendent that the organization is in full compliance. This annual compliance requirement opens the door to significant liability for board members and senior officers if the purported compliance is false or inadequate. In other words, besides financial penalties and costs related to timely reporting, the individuals who certify compliance may be exposed to personal liability - civil and even criminal penalties for false disclosures made with an intent to deceive a regulator - if the organization is found to be noncompliant.

Besides regulatory agencies, many states have significant liabilities for untimely notification. As an initial matter, almost all of the regulations enacted by states apply to any business that collects personal information nationwide. In other words, if a business in New York has a data breach that involves New Jersey, Florida, and Texas residents, then the organization must provide notification and comply with each of the individual state's requirements.

Of particular note is Florida's breach notification statute. Florida enacted one of the most stringent and robust data protection statutes and imposes a thirty-day deadline to provide notice to individuals affected by a data breach. This thirty-day deadline is the shortest deadline among all states with similar state breach notification statutes and it imposes a penalty of one thousand dollars a day for each day the notification is late and a fifty thousand dollar penalty for each subsequent thirty-day period up to one hundred and eighty days.9 In short, similar to the above-referenced federal and state agencies, untimely reporting with regard to state breach notification statutes can result in very significant costs and harm.

Although delays in timely reporting and disclosures are often the result of disorganization, even if an organization is timely, it can still face severe penalties for disorganization. For instance, OCR recently announced a $2.2 million settlement with MAPFRE Life Insurance Company of Puerto Rico (MAPFRE) based on the impermissible disclosure of unsecured electronic protected health information (ePHI) as well as Social Security numbers.10 MAPFRE filed a timely breach report with OCR indicating that a USB storage device containing ePHI was stolen.11 However, after MAPFRE filed the report an OCR investigation revealed that MAPFRE did not conduct a risk analysis and failed to implement corrective measures.12 The size of the settlement is due to the fact that OCR uncovered that MAPFRE made misrepresentations to OCR, including that it had conducted a risk analysis and implemented risk management plans and MAPFRE failed to execute a security awareness and training program, failed to implement encryption and failed to execute reasonable and suitable policies and procedures. 13 In sum, whether an organization is untimely with regard to its cybersecurity breach notification obligations or fails to take corrective actions, the costs and liabilities are extensive.

How to Mitigate Costs and Liabilities

The best and most succinct guidance concerning how to organize and respond to a data breach is provided by the Federal Trade Commission (FTC).14 The first step for any organization to deal with a data breach is to secure operations and assemble a team of experts. There is no doubt that cybersecurity overall is both a legal and a technical issue and, thus, the team must include outside cybersecurity counsel (counsel with specific experience in this particular field), which will retain technical resources to do a forensics investigation and remediate systems. Notwithstanding the need for experienced cybersecurity counsel to determine the legal requirement to notify and avoid the severe penalties associated with a delay as outlined above, cybersecurity counsel can also mitigate an organization's litigation liabilities to the extent possible by shielding findings and communications between the technical experts, team members and the organization under attorney-client privilege.15

John J. Cooney

Nicole Della Ragione

After retaining a team of experts, the experts must begin securing the system and fixing vulnerabilities. Securing the system includes preventing additional data loss and further attacks.16 Once secure, an organization should begin to examine relationships with service providers, conduct risk assessments and develop a communication plan.17 As demonstrated above in the MAPFRE matter, it is essential that an organization can accurately represent that it has remediated its systems, implemented corrective actions and is in compliance with applicable regulations.

As indicated, cybersecurity counsel will analyze the applicable state and federal laws and regulations based upon the circumstances and determine the notification trigger date as well as the appropriate individuals, businesses, authorities and entities to notify. This requires a detailed analysis given that obligations are dependent upon the residency of the affected individual, the specific elements of data, the number of affected individuals and the respective organization's industry. For instance, obligations vary widely depending on whether the data at issue involves Social Security numbers or credit card numbers and security code or PHI, or combinations thereof. Given the aforementioned severe penalties and increased scrutiny with timely reporting and notifications, it is critical that state and federal obligations are analyzed thoroughly and a plan to communicate and comply is initiated.

Organization and Promptness is Key

The rapid increase in frequency of cyberattacks and the associated surge in regulatory enforcements, private party class actions, as well as state and federal government investigations, means that cybersecurity and data protection should be a top priority for organizations across all industries. Implementing an organized approach and avoiding unnecessary delays will ensure that an organization can concentrate on the data breach and the respective business ramifications and not worry about the aforementioned severe penalties and liabilities associated with delays and disorganization.

John J. Cooney, Esq. is a partner at Ruskin Moscou Faltischek and chair of the Firm's Cybersecurity and Data Privacy practice group. His e-mail is jcooney@rmfpc.com. Nicole Della Ragione, Esq. is an associate at the firm and a member of its Cybersecurity and Data Privacy practice group. Her e-mail is ndellaragione@rmfpc.com.

1. Information Security Breach and Notification Act, N.Y. Gen. Bus. L. §899-aa(1)(c) (2005).
2. First HIPAA enforcement action for lack of timely breach notification settles for $475,000, U.S. Dep't Health and Hum. Serv. (Jan. 09, 2017), http://wayback.archive- it.org/3926/20170127111957/https://www.hhs.gov/about/news/2017/01/09/first-hipaa-enforcement-action-lack-timely-breach-notification-settles-475000.html.
3. First HIPAA enforcement action for lack of timely breach notification settles for $475,000, supra note 2.
4. Id.
5. Id.
6. James Swann, Delayed Breach Notice Costs Illinois Health Systems, 16 Privacy & Security L. Rep. (BNA) No. 126 (Jan. 16, 2017).
7. Cybersecurity Requirements for Financial Services Companies, 23 N.Y.C.R.R. Pt. 500.21 (2016).
8. 23 N.Y.C.R.R. § 500.17.
9. Fla. Stat. § 501.171(9)(a) (2016).
10. HIPAA settlement demonstrates importance of implementing safeguards for ePHI, U.S. Dep't Health and Hum. Serv. (Jan. 18, 2017), http://wayback.archive-it.org/3926/20170127111936/https://www.hhs.gov/about/news/2017/01/18/hipaa-settlement-demonstrates-importance-implementing-safeguards-ephi.html.
11. HIPAA settlement demonstrates importance of implementing safeguards for ePHI, supra note 10.
12. Id.
13. James Swann, Stolen Storage Device Leads to $2.2M Settlement for Insurer, 16 Privacy & Security L. Rep. (BNA) No. 195 (Jan. 30, 2017).
14. Data Breach Response: A Guide for Business, Fed. Trade Comm'n (Sept. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business.
15. In re: Target Corporation Customer Data Security Breach Litigation, MDL No. 14-2522 (Oct. 23, 2015).
16. Data Breach Response: A Guide for Business, supra note 14 at 1-2.
17. Id. at 3.