Westlaw Journal
COMPUTER & INTERNET
Litigation News and Analysis • Legislation • Regulation • Expert Commentary
VOLUME 32, ISSUE 24 / MAY 7, 2015

EXPERT ANALYSIS

Data Breaches: Response and Risk-Mitigation Requirements

By Kenneth N. Rashbaum, Esq.,
Barton LLP

Each week brings new tales of woe to C-suite personnel and general counsel who are responsible for the safekeeping of the most valuable organizational asset: information. In addition to their acute-onset migraine headaches from cyberattacks and breaches, they face a maze of possible federal, state and international laws and regulations triggered by a data breach.

Many companies are in industries that confront a legal double-whammy. First, they may face mandated notification and/or remediation steps when data have been disclosed. They also may face investigations by regulatory agencies and/or litigation for allegedly allowing the breach to occur by falling below cybersecurity mitigation regulations. With planning and preparation, these organizations can react quickly and cost-effectively in a manner that complies with the myriad of regulations and statutes that govern the response to a breach.

This article will suggest a framework for analyzing the appropriate response to a cyberattack and/or breach as required by statutes and regulations and in light of business concerns. The best prevention of a cyberattack or breach, though, is to take steps to mitigate the risk of such an intrusion in the first place. This article will also suggest how to leverage existing mandates for breach mitigation into a plan for cyber-risk management. After all, the least expensive way to respond to a breach is to prevent it.

The terms "cyberattack" and "breach" are separated here because not all cyberattacks result in the unauthorized disclosure of protected data (though most do). Similarly, not all breaches are the result of attacks, because many unauthorized disclosures are caused by such negligent acts as leaving portable storage media, smartphones or tablets that contain unencrypted data in unsecured locations where they are lost or stolen.[1]

Rather than curse the darkness of the Dark Web,[2] corporate officers can light candles by leveraging breach-mitigation requirements to prepare workflows and a culture of security that can reduce the chances of a successful cyberintrusion. In the process, they can also provide defensibility against possible claims arising from a breach. It's important to keep in mind that there is no strict liability for data breaches. The legal standard for liability in the event of a cyberbreach is whether reasonable steps had been taken to avert a breach.

FRAMEWORK OF RESPONSE OBLIGATIONS AFTER A CYBERATTACK OR BREACH

The mosaic of laws and regulations regarding a response to a cyberattack tests the metaphorical skills of even the most literary minds. Descriptions of the dilemma such as "Byzantine," "Gordian knot," "three-dimensional chess" and a "cyber Tower of Babel" are all germane, but none of these appellations really do justice to the network of laws, regulations and industry practices. The following framework can assist in the analysis.

The best prevention of a cyberattack or breach is to take steps to mitigate the risk of such an intrusion in the first place.

What data were compromised?

What data were compromised in the breach, and from what service sector? Not all information is protected by laws or regulations.

- Was the information "personal data"? The definition of this term may vary among industries, but generally it comprises information that is traceable to an identifiable person. For example, the "privacy rule" of the Health Insurance Portability and Accountability Act of 1996, the law known as HIPAA, specifies 18 such identifiers.[3]

- Are the data otherwise protected by a statute or regulation? In the United States, privacy and breach response law is sector-specific. This contrasts with universal privacy laws in places such as the European Union. Also, some industries have mandated specific time periods for disclosures and notifications of breaches and, in some cases, the content of those notifications.[4]

Where are the affected persons located?

Where does the organization do business, and where are its customers located?

- In the United States, 47 states have statutes or regulations that specify obligations in the event of a breach of protected information.[5] Most of these provisions comprise the time periods for and the content of the data owners or data subjects. Some statutes and regulations include requirements for notification of law enforcement.

- Some countries within the European Union, as well as Asia and elsewhere, require that certain companies whose information has been breached must notify their national data-protection authorities and, if the data aren't encrypted, send notifications to potentially affected individuals.[6] If a U.S. organization stores or maintains personal or otherwise protected data from citizens of another country with data breach notification laws, it may be required to notify the relevant data-protection authority and the potentially affected individuals.

Investigation and remediation duties

What is required of the organization to investigate and/or remediate the vulnerability that led to the breach?

- If an organization has cyber-risk insurance, it should notify the insurance carrier as soon as practicable after it learns of an attack or other breach. Most insurance policies have a notification provision that specifies the conditions for notice and the time when it must be made. Failure to heed these notice periods can result in a reservation of rights by the carrier or, far worse, a disclaimer of coverage.[7]

- Consult third-party and in-house information technology resources to close down backdoors, trapdoors and other entrance points, and to isolate and remove the intrusion. Preserve audit trails and metadata. Also, interview IT personnel, end users and third-party vendors as to how the intrusion occurred. This will be needed for subsequent investigations or litigation and, of course, to harden the system and strengthen safeguards against another such attack or breach.

- If relevant, ascertain the safeguards used by third-parties that have access to the organization's network. The Target breach occurred, in part, as a result of a vulnerability of a heating, ventilation and air conditioning, or HVAC, contractor.[8]

Regulatory and litigation exposure

What is the regulatory and litigation exposure in the wake of a cyberattack or breach, and how should the organization prepare?

- Lawsuits in the event of a cyberattack or massive breach may be any of the following: class actions averring violations of state privacy laws; suits by individuals who allege actual

damages from identity theft or fear of identity theft that caused the aggrieved person or persons to spend time and expense to protect against identity theft; litigation brought by the Federal Trade Commission[9]; or, in the case of public corporations, shareholder derivative litigation alleging corporate waste and breach of fiduciary duty for failure to ensure that management had appropriate safeguards in place.[10]

- A plethora of federal and state agencies with often overlapping jurisdictions may take action in the event of a cyberattack or breach. They include the FTC (which may bring proceedings for deceptive or unfair trade practices with regard to privacy and security representations), the Securities and Exchange Commission, the Department of Health and Human Services, and state attorneys general.

- Consult counsel (outside, in-house or preferably both) and the "breach response team" as to notifications to regulatory agencies.

- Implement a data-preservation protocol designed by the breach response team so that information on the method and results of the attack or breach, which may be potentially relevant to an investigation or lawsuit, is not lost.

REDUCE THE RISK BY FOLLOWING REGULATORY MANDATES

The least costly cyberattack or data breach is one that never takes place because good information-governance hygiene prevented it. This is not just common sense, nor is it aspirational. Many cyberattacks and breaches are avoidable because they resulted from negligence and/or a failure to follow written protocols on information management (such as failing to encrypt data on a USB stick or mobile device and losing that device or clicking on an attachment of unknown provenance that turns out to be malware).

Regulations in health care,[11] financial services[12] and education[13] mandate written information-security plans that comprise technical, administrative and physical safeguards for certain data, training on those security policies and assessments of vulnerability or security risks on a periodic basis. By following these standards, an organization can significantly reduce the risks of cyberattacks and breaches.

However, the statutes and regulations cited here provide only broad standards and guidelines. To be effective, an information security plan must be tailored to the nature of the business and the culture of the organization. Steps to an effective information security plan include the following:

- Find a champion within the organization. Although the recent spate of data breaches has made information security a selling point, cybersecurity is still seen by senior management as a cost center. A champion in senior management is critical to getting resources for the initiatives and making the argument for a return on investment.

- Form a cybersecurity team. In 2015, security is not just an IT issue. In the age of "bring your own device" policies and with the increased use of cloud services, a company's data may be in several places around the world simultaneously. This makes security everyone's concern. The drop of 46 percent in Target's revenue after its massive data breach in 2013 is testimony to the business imperative of information security.[14] In addition to the cybersecurity champion mentioned above, the team should include someone from the IT, legal and risk and compliance departments as well as representatives of the business owners who use company data on a day-to-day basis. In some organizations, it may be culturally beneficial to have outside counsel facilitate the initiative. The team should prepare information security policies with practical business operations in mind. The only thing worse than having no policies is having policies that no one follows but create a standard by which the organizations will be measured.

- Form a "breach response" team. The breach response team should be on call for attacks and breaches, and it should include persons who know the technical and legal responses and

Not all cyberattacks result in the unauthorized disclosure of protected data (though most do) and not all breaches are the result of attacks.

requirements. The team should hold periodic breach response drills and adjust response protocols as indicated by the performance of the workforce during these cyberattack drills (which, of course, should be documented).

- Prepare a data map. The map should include details about the organization's data, such as what type of data the organization stores and where and how this information is used. This will make data management and breach response much more efficient.

- Conduct training. Train the workforce on organizational cybersecurity policies and document the training. Include cybersecurity awareness and information management training in new-employee orientation, and provide "pop-up" security reminders on a regular basis.

- Maintain automated or regular security updates. If possible, automate security patches so that safeguards are always current. Update malware detection and eradication and conduct vulnerability scans and penetration analyses regularly.

CONCLUSION

Cyberattack and breach protocols and scans and breach response drills can't prevent every disclosure, but the legal, regulatory and business-relations standards do not require perfection. The standard in virtually every regulation governing information security and in litigation consists of "reasonable steps" that are consistent with industry practices.

The legal standard for liability in the event of a cyberbreach is whether reasonable steps had been taken to avert a breach.

Reasonable steps, though, can only be demonstrated by documented protocols that show that technical and administrative plans are taken seriously.

NOTES

[1] *See, e.g., In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, MDL No. 2360, 2014 WL 1858458 (D.D.C. May 9, 2014).

[2] The BBC has defined the "Dark Web" as "anonymous, virtually untraceable global networks used by political activists, criminals and the like." *See* Adrian Goldberg, *The dark web: Guns and drugs for sale on the internet's secret black market*, BBC, Feb. 3, 2012, http://bbc.in/1FrupND.

[3] 45 C.F.R. § 164.514.

[4] In January 2015, President Barack Obama proposed national legislation called the Personal Data Notification and Protection Act that would create a uniform national standard for data breach notification. *See* White House, The Personal Data Notification & Protection Act, *available at* http://1.usa.gov/1EdJd04 (last visited Apr. 28, 2015). *See also* White House Press Sec'y, Fact Sheet: Safeguarding American Consumers & Families (Jan. 12, 2015), *available at* http://1.usa.gov/1zfdM6W.

[5] Security Breach Notification Laws, BEAZLEY, https://www.beazley.com/our_business/professional_liability/tmb/data_breach_map.html. The information on the website was last updated in October 2014. The website was last visited April 20.

[6] United Kingdom, etc. As of this writing, the EU Data Protection Directive 95/46/EC does not require member states to implement breach-notification legislation. The directive is the subject of a revision proposal that has been approved by the European Parliament that would comprise requirements for notification to the new pan-European Data Protection Authority and the affected individuals, subject to certain limitations and exceptions.

[7] *Travelers Indem. Co. of Conn. v. P.F. Chang's China Bistro Inc.*, No. 3:14-cv-01458, 2014 WL 5280480, *complaint filed* (D. Conn. Oct. 2, 2014).

[8] Brian Krebs, *Target Hackers Broke in Via HVAC Company*, KREBS ON SECURITY (Feb. 5, 2014), http://bit.ly/1DtKBIg.

[9] *See, FTC v. Wyndham Worldwide Corp. et al.*, No. Civ. 2:13-cv-01887, 2014 WL 1349019 (D.N.J. Apr. 7, 2014), *motion to certify appeal granted* 10 F. Supp. 3d 602 (D.N.J. 2014). The case is currently on appeal before the 3rd U.S. Circuit Court of Appeals about whether the federal agency has authority to regulate data-security practices. Oral argument was heard March 3 before a three-judge panel with Circuit Judges Thomas L. Ambro, Anthony J. Scirica and Jane R. Roth. The parties filed supplemental briefs with the appellate panel at the end of March, and a decision is likely in the near future. *See generally FTC v. Wyndham Worldwide Corp. et al.*, No. 14-3514 (3d Cir.).

[10] *See Palkon v. Holmes*, No. 2:14-CV-01234, 2014 WL 5341880 (D.N.J. Oct. 20, 2014), dismissing the Wyndham derivative lawsuit. Although U.S. District Judge Stanley R. Chesler of the District of New Jersey found that the business-judgment rule protected Wyndham's directors, he set out criteria for appropriate exercise of that judgment after reports of data breaches.

[11] 45 C.F.R. § 164.312.

[12] 17 C.F.R. § 248.30; 16 C.F.R. §§ 314.3-14.4.

[13] 34 C.F.R. §§ 99.7 & 99.32.

[14] *See* Maggie McGrath, *Target Profit Falls 46% On Credit Card Breach And The Hits Could Keep On Coming*, FORBES, Feb. 26, 2014, http://onforb.es/1HUMMMO.

Kenneth N. Rashbaum is a partner at **Barton LLP** in New York, where he heads the privacy and cybersecurity practice. He counsels clients on federal and state laws, industry regulations, and international standards for information governance, and he represents multinational organizations and health care providers in government proceedings and litigation regarding privacy and security. He is also an adjunct professor at the Maurice A. Deane School of Law at Hofstra University. He can be reached at krashbaum@bartonesq.com. Caroline Gange, a student at the Maurice A. Deane School of Law, assisted with the research for this article.