CHAD LAYTON & EMILY ACOSTA

You've been hacked — Now what? Steps a company must take following a cyber attack

In the short time since our first cyber risk article published in the Spring edition of *The Illinois Manufacturer,* another major hack has occurred. And this time it was not the private sector, but, rather, the U.S. Office of Personnel Management that was breached.[1] On Thursday, June 4, the White House announced the breach of up to four million current and former federal employees' records dating as far back as the 1980s[2] and impacting an estimated 2.1 million current federal employees. While the U.S. Government was the victim this time, this recent attack is yet another example that no entity is immune from the risk of a cyber attack.[3]

Given that the chance of a cyber attack is more than a mere possibility, companies must be proactive by developing and implementing comprehensive strategies designed to minimize the impact of a data breach. In fact, data shows that companies that are proactive in this area save time and money, and minimize the impact of a data breach on its business, in the event one occurs. For example, companies that have a strong security posture as well as a business continuity management plan will experience lower costs and expenses in the event of a data breach.[4] The data speaks to developing an incident response plan before a breach ever occurs.

This article discusses the issues that a company should consider and steps it should take following a cyber security breach.

First Things First: Emergency Response

In the event of a breach, one of a company's first and primary concerns must be identifying and containing the breach. To the extent possible, a company will also want to recover any lost data. As is the case with any crisis, a company will be better equipped to address a breach if it forms an incident response team before a breach ever occurs.

The incident response team should include personnel from several relevant areas of the company, including management, IT and human resources. It is also critical to identify an IT forensics expert that is experienced in responding to data breaches, so that you can contact that company immediately upon learning of a breach. It may also be important to retain a media consultant, depending on the nature of your business as well as the breach itself. A breached company will also want to place its insurance carrier on notice of the incident.

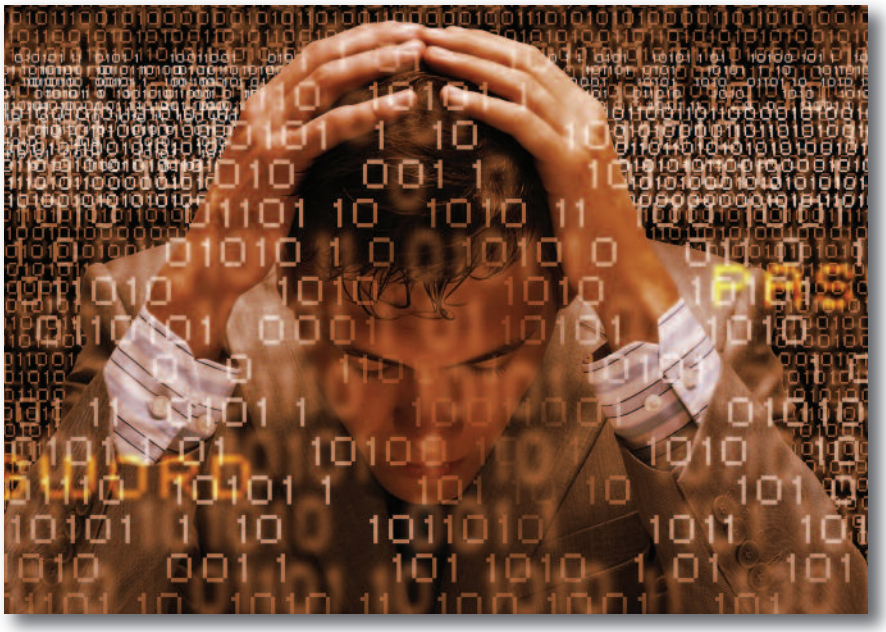
Finally, the participation of an attorney in the incident response process will allow for the protection of the attorney-client privilege, and will also provide assistance with responding to an investigation by the United States or other government entity, should one occur. Legal counsel will also be able to ensure your compliance with the notification laws of every state that is impacted by the breach.

Documenting Post-Breach Efforts

In the event of a breach, it is critical that your company document all post-breach remedial measures. This information will be important for determining the sufficiency of your remediation efforts, preventing similar incidents from occurring in the future, and — if necessary — responding to an investigation by the United States government or other entity.

It is also important that your company preserve all relevant information including hardware. A company that fails to preserve all relevant data exposes itself to potential liability for spoliation of evidence claims — a separate and independent cause of action that is based on a party's failure to preserve information relevant to a lawsuit.[5] Moreover, documenting remediation efforts will prove helpful in defending against subsequent lawsuits, in the event of litigation. Such an audit and evalua-

see **HACKED** *page 23*



Chad Layton is a shareholder and **Emily Acosta** is an associate with the law firm of Segal McCambridge Singer & Mahoney in Chicago. Chad can be reached at 312-633-3533, clayton@smsm.com. Emily can be reached at 312-645-5634, eacosta@smsm.com. The firm is an IMA member company.

HACKED

Cont. from page 13

tion should include identifying what data was compromised and how, what systems were affected by the breach, how the breach was detected and when, and the post-breach efforts. Of course, a natural — and critical — part of this process will involve addressing whatever issues are attributable to the identified vulnerabilities in the system.[6]

In addition to allowing an emergency response team to perform its various duties, companies should also evaluate any ongoing cyber risks on a higher level, including device management, information management and employee training. Once a breach occurs, your company is "on notice" of such an incident. While the law does not require a company to be perfect, the standard of reasonableness requires that a company make reasonable post-breach efforts to prevent future incidents, in light of the lessons learned from the breach itself. The failure to do so could prove extremely detrimental in the event of litigation.

Compliance Issues and Notiication Requirements

A third, but crucial step is to identify and comply with the relevant notification requirements. There may be state, federal as well as industry-specific requirements that must be satisfied. Notably, a company is required to comply with the notification laws of every state in which a breach occurs. This means that your company could, potentially, be responsible for complying with the laws of 47 different states.

Depending upon the nature of the breach, a company will also need to consider whether it is necessary to provide identity monitoring and protection to the victims of the breach. It also may be appropriate to assist victims by providing identity recovery services.

Dollars and Sense

The costs associated with a data breach are significant. As reported in The Ponemon Institute's Cost of Data Breach Study: Global Analysis, in the United States, the average cost of a non-malicious data breach was $195 per record, and the average cost of a malicious or criminal attack was $246 per record.[7] Additionally, in the United States, where companies are (for the most part) legally required to notify victims of a data breach, the average notification cost exceeds $500,000 in the event of a single breaching event. Perhaps more troubling is the fact that the average cost of business lost by a U.S. company following a breach exceeded a staggering $3.3 million, and businesses also suffer from the loss of reputation, diminished goodwill, as well as abnormal customer turnover.

The failure to comply with post-breach legal requirements could prove even more costly. For example, Illinois law requires that a company inform victims of a data breach, and the failure to do so could expose your company to liability for consumer fraud violations and hefty fines.[8] Further, a company that violates other, relevant laws, following a data breach[9] potentially subjects itself to civil penalties.[10] Not surprisingly, legal violations are also aggressively prosecuted.[11] For example, in the first quarter of 2014 alone, the Consumer Financial Collection Bureau collected almost $40 million in fines and penalties.[12] For these reasons, it is critical that any company that experiences a breach ensures timely compliance with any relevant laws, statutes and regulations.

Post-Breach Employee Training

IBM estimates that over 95 percent of all breach incidents investigated can be attributable to "human error" in some respect.[13] The most commonly recorded form of human errors include system misconfiguration, poor patch management, use of default user names and passwords or easy-to-guess passwords, lost laptops or mobile devices, and disclosure of regulated information via use of an incorrect email address. Perhaps unsurprisingly, the most prevalent contributing human error is "double clicking" on an infected attachment or unsafe URL. Incorporating employee training helps to reduce the pre-breach risks that result from human error. However, it is equally important to reinforce cyber risk training after a breach, to ensure that your company is maintaining a culture of cyber awareness.

Interestingly, following the OPM hack discussed above, the federal government (as it must) continues to send vital information to its thousands of employee. Multiple reports have surfaced that many employees are mistaking these emails for malicious phishing campaigns and deleting and reporting them. This is one area that should be addressed in post-breach employee training.[14]

The last thing that any company wants is for history to repeat itself, and to fall victim to the same type of data breach a second time. Post-breach employee training and awareness can help your company to manage this risk. Moreover, attorney involvement in post-breach training will allow for the protection of the attorney-client privilege.

Is litigation on the horizon following a breach?

A company should expect litigation following a breach. Data shows that the rising prevalence of cyber breaches also means an increase in consumer protection class action lawsuits. Some courts are dismissing these class action suits because plaintiffs have not suffered an actual harm or injury and thus lack standing or the ability to bring a lawsuit.[15] Some other high profile suits, however, have been allowed to proceed. For instance, *In re Target Corp. Customer Data Security Breach Litigation,* Target brought a motion seeking to dismiss the suit, however, the motion was denied. After this decision,[16] Target agreed to pay $10 million to settle the lawsuit.[17]

Conclusion

According to former F.B.I director Robert Mueller, "there are only two types of companies: those that have been hacked and those that will be."[18] Cyber and data security breaches effect companies of all sizes and are only becoming more ubiquitous in an increasingly connected business environment. Given how common these kinds of threats are becoming, companies must take actions before, during, and after attacks to minimize costs, reduce exposure and to manage this important risk. ■

References

1. *"Data hacked from U.S. government dates back to 1985: U.S. official,"* Reuters Tech, http://www.reuters.com/article/2015/06/06/us-cybersecurity-usa-idUSKBN0OL1V320150606 (June 5, 2015).

see **HACKED** *page 24*

HACKED

Cont. from page 23

2. *Id.*
3. Despite this recent attack on the U.S. Government, the Senate failed to pass new cyber security legislation that would encourage the sharing of information concerning cyber threats between the private sector and the federal government, and enhance law enforcement's ability to investigate and prosecute cyber crimes. *"Senate Fails to Include Cybersecurity Legislation as Part of the National Defense Authorization Act,"* The National Law Review, Legislative Activity, http://www.natlawreview.com/article/senate-fails-to-include-cybersecurity-legislation-part-national-defense-authorizatio (June 15, 2015).
4. Ponemon Institute Research Report, 2014 *Cost of Data Breach Study: Global Analysis,* Ponemon Institute (May 2014).
5. *Compare Kilburg v. Mohiuddin,* 2013 IL App (1st) 113408, 990 N.E.2d 292 *appeal denied,* 996 N.E.2d 14 (Ill. 2013) *and appeal denied,* 996 N.E.2d 14 (Ill. 2013) (complaint alleged facts sufficient to support finding that cab company had duty to preserve event data recordings), *with Trask-Morton v. Motel 6 Operating L.P.,* 534 F.3d 672 (7th Cir. 2008) (pre-suit destruction of electronic data and documents was not spoliation absent evidence that motel acted in bad faith and had reason to anticipate litigation).
6. Notably, subsequent remedial measures may not be admissible as evidence of negligence in the event of litigation.
7. Ponemon Institute Research Report, *2014 Cost of Data Breach Study: Global Analysis,* Ponemon Institute (May 2014).
8. Failure to properly notify a consumer of a data breach amounts to a violation of the Illinois Consumer Fraud and Deceptive Business Practices Act ("CFDBPA"). See 815 Ill. Comp. Stat. Ann. 530/20. When prosecuting a CFDBPA violation, in addition to common civil remedies, the Attorney General or State's Attorney may request and the Court may impose a civil penalty of up to $50,000 per violation. See 815 Ill. Comp. Stat. Ann. 505/7. Additionally, in cases involving senior citizens, the court may impose an additional civil penalty of up to $10,000 for each violation. *Id.* Finally, the Attorney General or the State's Attorney may also recover costs associated with prosecuting the case. 815 Ill. Comp. Stat. Ann. 505/10.
9. A majority of states define a breach as the unauthorized access and acquisition of data that compromises the security, confidentiality and/or integrity of personal information, but notably, often excludes the good faith acquisition of the information. *See, e.g.* Cal. Civ. Code § 1280.15; 815 ILCS § 530/1 *et seq.;* Mich. Comp. Laws §§ 445.63, 445.72; Tex. Bus. & Com. Code §§ 521.002 et seq.
10. For instance, the Dodd-Frank Act, which applies to many financial institutions, provides that "[a]ny person that violates, through any act or omission, any provision of Federal consumer financial law shall forfeit and pay a civil penalty." The statute provides for three tiers of penalties. The first tier applies to "any violation of a law, rule, or final order or condition imposed in writing by the Bureau" and sets a penalty of not more than $5,000 per day that the violation occurred or the party continues to fail to pay the penalty. The second tier provides that "for any person that recklessly engages in a violation of a Federal consumer financial law, a civil penalty may not exceed $25,000 for each day during which such violation continues." Finally, the third tier provides that "for any person that knowingly violates a Federal consumer financial law, a civil penalty may not exceed $1,000,000 for each day during which such violation continues." 12 U.S.C. § 1055(c)(1)-(3).
11. In California, for example, a company can face administrative penalties up to $25,000 per patient when medical information is compromised. Cal. Civ. Code § 1280.15. Additionally, delays in notification can result in a $100/day fine up to $250,000. Id. In Michigan, a company could pay up to $250.00 for each failure to provide notice, up to $750,000.00. See Mich. Comp. Laws §§ 445.63, 445.72. And in Texas, a company could be forced to pay at least $2,000, but not more than $50,000, per violation. *See* Tex. Bus. & Com. Code §§ 521.002 *et seq.* The State also assesses a penalty of $100 per day for a failure to timely notify consumers, up to $250,000. *Id.* Finally, Texas provides for the full recovery of attorneys' fees, court costs, and investigatory costs, incurred in obtaining injunctive relief or civil penalties. *Id.*
12. Semi-Annual Report of the Consumer Financial Protection Bureau, October 1, 2013-March 31, 2014, available at http://www.consumerfinance.gov/reports/semi-annual-report-spring-2014/.
13. IBM Global Technology Services, Managed Security Services, *IBM Security Services 2014 Cyber Security Intelligence Index,* IBM Security Services (June 2014).
14. http://www.businessinsider.com/federal-employees-are-mistaking-official-government-emails-for-phishing-scams-2015-6
15. *Maglio v. Advocate Health & Hospitals Corp.,* 2015 IL App (2d) 140782-U (trial court's dismissal of plaintiffs' claims where plaintiffs did not allege that any of their personal information was used in any unauthorized manner, but rather, only asserted an increased risk of such, was appropriate).
16. Of note, the U.S. Supreme Court recently granted granted certiorari in *Spokeo, Inc. v. Robins,* to consider a question critical to the viability of data breach class actions: standing. Since the Supreme Court's most recent standing decision in *Clapper v. Amnesty Int'l USA,* a majority of lower courts have dismissed data breach claims for failing to satisfy Article III's injury-in-fact requirement; however, a growing chorus of lower courts have sanctioned such actions.

    Similar to data breach class action members who allege that compromised personal information puts them at risk of future identity theft, Thomas Robins, a private plaintiff purporting to sue on behalf of a class of millions of others, alleged only that Spokeo's publication of inaccurate information would adversely affect his *future* employment prospects, not that it caused him an actual or concrete present harm. The district court dismissed the claims, and the Ninth Circuit reversed, holding that Robins' contention that his individual FCRA rights were violated was itself a sufficient basis to confer standing, even though the risk of any tangible harm lay in the future. Unlike in failed data breach class actions, the Ninth Circuit held that the violation of statutory rights constituted a concrete *de facto* injury.

    Ultimately, the Court's decision will have a significant impact on data breach litigation and the viability of plaintiffs' claims in these kinds of suits. See *Spokeo, Inc. v. Robins,* The Oyez Project at IIT Chicago-Kent College of Law, http://www.oyez.org/cases/2010-2019/2015/2015_13_1339 (last visited June 25, 2015).
17. *Target agrees to pay $10 million to settle lawsuit from data breach,"* Reuters Tech, http://www.reuters.com/article/2015/03/19/us-target-settlement-idUSKBN0MF04K20150319 (March 19, 2015).
18. Mueller, Robert S., III, former Director of the Federal Bureau of Investigation, "Combatting Threats in the Cyber World: Outsmarting Terrorists, Hackers, and Spies." RSA Cyber Security Conference. California, San Francisco. 1 Mar. 2012 speech.

Reprinted with permission from the summer 2015 issue of . . .

The Illinois Manufacturer

The Illinois Manufacturer is the official publication of the Illinois Manufacturers' Association (IMA)
220 East Adams Street • Springfield, Illinois 62701 • 217-522-1240 • Fax: 217-522-2367
1211 West 22nd Street • Suite 620 • Oak Brook, Illinois 60523 • 630-368-5300 • Fax: 630-218-7467
Visit http://www.ima-net.org/library/tim.cfm for editorial and advertising information