Bloomberg BNA

Privacy and Security Law Report®

Corporate Security

The authors review major developments in cybersecurity in 2015, many of which will reverberate into the new year and beyond. They propose a strategy for organization-wide compliance in this dynamic and challenging environment.

The Most Important Cybersecurity Developments of 2015: What You Need to Know for the New Year

BY JENNIFER O. MITCHELL AND KURT R. HUNT

Jennifer O. Mitchell is a partner in Dinsmore & Shohl LLP's Health Care Practice Group and leads the firm's HIPAA Privacy and Security practice and initiatives. In her cybersecurity practice, she works with clients in all industries to minimize the risk of privacy and data security breaches and assists with all aspects of privacy and security compliance, governance, audits/investigations, enforcement actions, breach analyses, training and strategic planning.

Kurt R. Hunt is a member of Dinsmore & Shohl LLP's corporate department. He focuses his practice on privacy, cybersecurity, and public utility issues, particularly in the telecommunications industry.

More than ever, organizations need to stay up-to-date on the ever-changing landscape of cybersecurity. Some of the most important cybersecurity developments of 2015, including data breaches and governmental enforcement, judicial and regulatory decisions, changing cybersecurity standards, and a major international legal decision are instructive for companies across all industries as they head into 2016.

There are developments with which every organization should be familiar as it updates and implements changes in its cybersecurity policies and practices.

Data Breaches, Cybersecurity Incidents

Not surprisingly, 2015 continued the trend of major data breaches making headlines. Privacy Rights Clearinghouse, a non-profit privacy group, tracked more than 160 data breaches in the United States that affected organizations ranging from the usual targets—health care providers and insurers, financial institutions, and Fortune 50 companies—to dry cleaners and other smaller entities that previously did not consider themselves to be at risk of a major cybersecurity incident.

State and federal government agencies are also targets as evidenced by a number of highly-publicized breaches this year. No organization is free from cybersecurity risk, and no organization is immune to data compromises.

Recent data breaches have shown the potential for misuse of data and the risks posed to both consumers and businesses. Cybersecurity is an issue that involves

Cybersecurity Resolutions for 2016

- Evaluate and identify all cybersecurity risks.
- Fully understand state and federal legal obligations, as well as any applicable self-regulatory programs.
- Audit current technical cybersecurity measures; consider hiring outside experts to help detect and prevent attacks.
- Review and update internal information security policies, data breach plans, document retention policies, password policies, and privacy policies.
- Review agreements with outside vendors and audit vendors' security practices.
- Evaluate the costs and benefits of acquiring cybersecurity insurance.

everyone, and companies in all industries need to devote adequate attention and resources to addressing cybersecurity issues. Between January and August 2015, over 500 breaches are estimated to have occurred, and those breaches involved more than 140 million individuals' records.

The Federal Bureau of Investigation now ranks cybersecurity near terrorism at the top of its list of priorities.

In addition, there are significant financial, reputational, operational and legal risks associated with a cybersecurity intrusion or data breach. How data is collected, utilized, and, most importantly, protected can no longer be ignored. Businesses must proactively plan to avoid potential breaches and the costs associated with them.

In the 2015 Ponemon Data Breach Study, it was estimated that the average cost of a data breach in the U.S. was $6.5 million. These costs were associated with breach notification, organizing the incident response team, conducting investigations and forensics, identifying individuals affected by the breach, lost business, legal services, investigations, and enforcement fines and penalties.

The following are just a few of the many examples of high profile breaches and cybersecurity attacks that occurred in 2015.

Anthem

Anthem, one of the largest health insurers in the United States, experienced a breach of unprecedented magnitude. The breach involved the protected health information — including Social Security numbers and other highly sensitive medical information — of approximately 80 million customers. Months later, Anthem remains mired in numerous class action lawsuits from customers and regulatory inquiries.

Major League Baseball

Major League Baseball provides a less financially catastrophic example, but one that sheds light on the wide variety of motives and vulnerabilities that lead to cybersecurity incidents.

The Federal Bureau of Investigation found evidence employees of the St. Louis Cardinals hacked into the baseball operations database of the Houston Astros, which is believed to have contained proprietary scouting information and analytics.

Despite the competitive advantage provided by unauthorized access to this information, the alleged motive in this hack was apparently personal. The FBI's initial investigation indicated Cardinals front-office employees conducted the hack to sabotage the new general manager of the Astros, who had recently left the Cardinals organization.

This incident reinforces the importance of strong employee and data security policies—such as policies requiring regular password changes—to address the possibility of poor employee security practices or, in extreme circumstances, possible internal attempts at retaliation and/or sabotage.

Office of Personnel Management

This year also included what may prove to be the most damaging data breach yet experienced by any organization. In June, the Office of Personnel Management—an independent agency of the United States federal government—announced its systems had been compromised, and unknown attackers had gained access to the confidential information of approximately 21 million federal employees (14 PVLR 1275, 7/13/15).

The compromised information, according to the OPM's letter to affected individuals, may have included each employee's ''name, Social Security number, address, date and place of birth, residency, educational, and employment history, personal foreign travel history, information about immediate family as well as business and personal acquaintances, and other information used to conduct and adjudicate [their] background investigation.''

Experts have decried the impact of the breach on national security, and it has been reported the Central Intelligence Agency pulled agents from China as a direct result of the breach.

Experian

In October, Experian, which stored and processed significant amounts of information related to credit assessments for T-Mobile U.S. Inc., experienced a breach that affected 15 million consumers (14 PVLR 1802, 10/5/15). Initial investigations indicated that the breach had occurred over the course of two full years and resulted in the compromise of social security numbers, addresses, identification numbers, and more.

Excellus Blue Cross Blue Shield

In another long-lasting breach, Excellus Blue Cross Blue Shield discovered that its systems had been compromised from approximately December 2013 through August 2015, when the breach was discovered during a cybersecurity risk analysis (14 PVLR 1673, 9/14/15). More than 10 million individuals' information was compromised.

Although much of the information was encrypted, it is believed that the attackers may have also gained access to administrative controls enabling them to decrypt critical information.

  PVLR ISSN 1538-3423

Ashley Madison

Ashley Madison, a Web-based dating service targeted to individuals already in a relationship, experienced a breach affecting more than 32 million customer accounts (14 PVLR 1564, 8/24/15). In addition to the typical user name and password information, the breach exposed e-mail addresses and user profiles which include highly detailed and private information.

These examples, and the sheer volume of data breaches experienced in 2015, reinforce cybersecurity risks are still on the rise, and organizations must be vigilant and prepared.

Judicial and Regulatory Decisions and Government Enforcement

No doubt related to the increase in cybersecurity incidents over the past few years, 2015 has been a banner year for judicial and regulatory activity in the areas of cybersecurity and privacy.

Federal Trade Commission

LabMD

One of the most important regulatory developments this year is, unexpectedly, good news for businesses.

LabMD, Inc., a clinical testing laboratory, was accused by the Federal Trade Commission (FTC) of failing to provide ''reasonable and appropriate'' security for personal information stored on its network. Instead of settling during the investigation stage and entering into an onerous consent order, like nearly all other FTC targets, LabMD challenged the agency's evidence and authority. In response, the FTC issued an administrative complaint against LabMD in August, 2013 (12 PVLR 1533, 9/9/13).

After years of litigation before the FTC's Chief Administrative Law Judge, collateral actions in the U.S. Court of Appeals for the 11th Circuit (14 PVLR 156, 1/26/15), an unprecedented U.S. House Oversight and Government Reform Committee investigation of the action against LabMD (13 PVLR 1318, 7/28/14), and blockbuster testimony from a whistleblower who, after receiving immunity from the Department of Justice, testified that the FTC's evidence against LabMD had been fabricated, the result was a hard-fought victory for LabMD, which one legal commentator called ''stunning.''

In November, the Administrative Law Judge (ALJ) dismissed the FTC's complaint against LabMD, holding that ''[b]ecause [the FTC] failed to meet its burden of proving the first prong of the three-part test in Section 5(n)—that [LabMD]'s conduct caused, or is likely to cause, substantial consumer injury—[LabMD]'s alleged failure to employ 'reasonable and appropriate data security' for information maintained on its computer networks cannot be declared an 'unfair' act or practice in violation of Section 5(a) of the FTC Act'' (14 PVLR 2109, 11/23/15). The long-term consequences of the ALJ's decision are uncertain.

Complaint counsel has appealed that decision to the Commission (14 PVLR 2185, 12/7/15)and, as research by former Commissioner Joshua Wright has confirmed, the Commission has reversed every ALJ decision in the past 20-plus years favoring a respondent. If, as is statistically nearly certain, the Commission reverses the ALJ and rules against LabMD, LabMD will appeal to U.S. Circuit Court.

Regardless, the FTC's landmark loss may very well slow the agency's efforts to use Section 5 of the FTC Act as a ''blank check'' to enforce poorly-defined cybersecurity standards.

The trial team in this litigation was led by Dinsmore & Shohl's William Sherman and Reed Rubinstein. Dinsmore was counsel to Cause Of Action, a government watchdog organization that defended LabMD in the administrative case as part of its educational mission.

Wyndham Worldwide

In August, the U.S. Court of Appeals for the Third Circuit affirmed in *FTC v. Wyndham Worldwide Corp.*, 2015 BL 271793, 799 F.3d 236 (3d Cir. 2015) the FTC's authority to enforce cybersecurity standards in court under Section 5 of the FTC Act prohibiting ''unfair'' or ''deceptive'' trade practices (14 PVLR 1592, 9/7/15).

Because the FTC had not promulgated cybersecurity regulations, and because the Section 5 action against Wyndham was filed in an Article III court and not under the Commission's administrative procedures, the Third Circuit rejected Wyndham's argument that it had not been given fair notice of the FTC's authority to regulate cybersecurity or what standards should be applied.

The Third Circuit reasoned the relevant issue ''is whether Wyndham had fair notice that its conduct could fall within the meaning of the statute'' as construed by a judge.

''[I]f the federal courts are to decide whether Wyndham's conduct was unfair in the first instance under the statute without deferring to any FTC interpretation, then this case involves ordinary judicial interpretation of a civil statute, and the ascertainable certainty standard does not apply,'' the court said.

The court went on to note that ''If later proceedings in this case develop such that the proper resolution is to defer to an agency interpretation that gives rise to Wyndham's liability, we leave to that time a fuller exploration of the level of notice required [from the agency].''

The *Wyndham* opinion limits FTC's authority by applying Section 5(a)-(n) as written. Taken together, these opinions suggest that the FTC's authority is much less expansive than it has claimed.

Morgan Stanley Smith Barney

The FTC's position on cybersecurity as demonstrated in the *Wyndham* matter were further reinforced by a closing letter issued in August to Morgan Stanley Smith Barney LLC in connection with an inquiry into whether Morgan Stanley's data security practices violated Section 5 of the FTC Act (14 PVLR 1518, 8/17/15).

The FTC closed that investigation without issuing any penalties and, in doing so, provided insight into its stance on ''reasonable'' cybersecurity practices by listing several of Morgan Stanley security practices as ''factors'' in declining to take action, including the implementation of ''comprehensive policies'' prior to the alleged breach and Morgan Stanley's quick response to the alleged breach.

There are lessons to be learned from *Morgan Stanley*—in which no fines were issued because of the company's policies and responses—and *Wyndham*—in which the hotel chain was hammered by the FTC for repeated and egregious security failures. In the eyes of

the FTC, prevention is not everything. Rather, preparedness (having appropriate policies in place and properly implemented) and responsiveness (reacting appropriately to cybersecurity incidents) are key to helping avoid potential regulatory penalties.

The FTC, however, is not the only regulatory agency actively enforcing against alleged cybersecurity failures. Organizations in heavily regulated areas—such as the health care, financial, and telecommunications sectors—should also be careful to heed the actions of their primary regulators.

Securities Exchange Commission

In 2015, the Securities Exchange Commission (SEC) launched its Cybersecurity Examination Initiative and provided guidance to regulated entities about the types of written policies it would require (14 PVLR 580, 4/6/15).

In September, the SEC issued its first cybersecurity-related enforcement. An investment management company, R.T. Jones Capital Equities Management, Inc., was fined $75,000 and forced to adhere to a cybersecurity compliance plan as the result of a hack of a third-party-hosted web server that allegedly made thousands of clients ''vulnerable to theft'' (14 PVLR 1749, 9/28/15).

Federal Communications Commission

The Federal Communications Commission (FCC) has also become active in identifying and enforcing its expectations regarding cybersecurity.

Most recently—in November—the FCC entered into a consent decree with Cox Communications to settle a 2014 breach of personal information for $595,000 (14 PVLR 2031, 11/9/15).

Department of Health and Human Services Office of Civil Rights

Lahey Hospital and Medical Center

On the health care front, on Nov. 25 the Department of Health and Human Services Office of Civil Rights (OCR) entered into a settlement agreement with Lahey Hospital and Medical Center (Lahey) related to alleged violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule and Security Rule in connection with a 2011 laptop theft (14 PVLR 2185, 12/7/15).

OCR's investigation revealed widespread non-compliance with the HIPAA rules, including failure to conduct a thorough risk analysis, failure to implement adequate physical and technical safeguards, and failure to implement and maintain appropriate policies and procedures so as to safeguard electronic protected health information, resulting in the disclosure of 599 individuals' protected health information.

Lahey agreed to pay $850,000 and will adopt a robust corrective action plan to correct HIPAA compliance deficiencies. Lahey is also required to provide OCR with an enterprise risk analysis and ongoing evidence of compliance and is also required to report certain incidents.

Triple-S Management Corporation

On the heels of that report, on November 30, 2015, OCR reported a $3.5 million settlement with Triple-S Management Corporation (TRIPLE-S), on behalf of its wholly owned subsidiaries, Triple-S Salud Inc., Triple-C Inc. and Triple-S Advantage Inc., formerly known as American Health Medicare Inc. (14 PVLR 2202, 12/7/15). According to OCR, TRIPLE-S will pay $3.5 million and will adopt a corrective action plan and comprehensive compliance program.

TRIPLE-S is an insurance holding company based in San Juan, Puerto Rico. After receiving multiple breach notifications from TRIPLE-S involving unsecured protected health information (PHI), OCR initiated investigations and found widespread non-compliance, including failure to implement appropriate administrative, physical, and technical safeguards to protect the privacy of its beneficiaries' PHI; impermissible disclosure of its beneficiaries' PHI to an outside vendor with which it did not have an appropriate business associate agreement; use or disclosure of more PHI than was necessary; and failure to perform a thorough risk analysis and implement security measures to ameliorate security risks.

Companies can expect to see more of these types of judicial and regulatory decisions and governmental investigations and enforcement actions in 2016 and beyond.

Changing Standards

Two of the chief frustrations businesses have about cybersecurity and privacy are that key standards are still developing and there is still no uniform federal data breach law governing businesses that operate in more than one state. Because of this, it is important to remember other sources of authority – including state data breach laws, informal regulatory guidance, and industry standards – when developing compliance plans and undertaking breach notification and remediation efforts.

When companies experience breaches, they will need to look at the laws that apply in every state in which they do business to ensure they have taken all appropriate steps to address their legal obligations.

The FTC has formed a new Office of Technology Researchand Investigation (OTRI), which will research and provide guidance on a variety of matters, including ''privacy, data security, connected cars, smart homes, algorithmic transparency, emerging payment methods, big data, and the Internet of Things'' (14 PVLR 551, 3/30/15) . Hopefully, OTRI will help develop more bright-line guidance for organizations that are trying in good faith to comply with the laws applicable to their business and FTC's cybersecurity goals.

The FTC has also released informal guidance, titled ''If the FTC comes to call,'' on what a company should expect from FTC investigations into data security. This document is not definitive or binding, but it provides insight into the FTC's current thoughts on data security and could help guide a company's creation of a data security policy.

Also related to post-breach guidance, the Cybersecurity Unit of the U.S. Department of Justice released a document entitled ''Best Practices for Victim Response and Reporting of Cyber Incidents'' (14 PVLR 802, 5/4/15)(14 PVLR 802, 5/4/15). This 15-page guide provides a preparedness checklist and guidance on creating and executing an incident response policy.

For organizations looking instead for guidance on what security policies the FTC expects to be adopted, FTC Chairwoman Edith Ramirez gave a speech in Janu-

   ISSN 1538-3423

ary in which she identified ''three key steps that companies should take to enhance consumer privacy and security:'' (1) adopt security-by-design protocols; (2) minimize collected and retained data; and (3) increase transparency and provide consumers with notice and choice where appropriate (14 PVLR 68, 1/12/15).

Although the Chairwoman was speaking in the context of privacy concerns implicated by the ''Internet of Things'', her three key steps likely identify data security practices the FTC views or is starting to view as standard and appropriate.

Industry groups also have their own cybersecurity standards, which develop on an almost continual basis. One of the biggest—the Payment Card Industry Security Standards Council—recently published additional regulations to its Data Security Standard (PCI DSS) (14 PVLR 1086, 6/15/15). The new Designated Entities Supplemental Validation (DESV) procedures will require certain entities to fulfill additional compliance validation requirements.

Although the entities subject to the enhanced rules have not yet been determined, the PCI SSC's activity serves as a reminder for all companies accepting credit card payments to be aware of their data security obligations under PCI DSS and to review their policies and practices to ensure compliance.

Finally, states remain extremely active in the cybersecurity arena, passing and amending laws related to protecting personal information and addressing data breaches. California, Montana, New York, Washington and Wyoming, among others, all saw legislative activity and new laws related to cybersecurity in 2015.

International Shake-Up

Of all the developments in cybersecurity in 2015, however, the biggest came on the international front.

Since 2000, thousands of companies have relied on the U.S.-EU Safe Harbor program to comply with the European Union's strict data protection laws when transferring personal data from EU member states to the U.S.

On Oct. 6, the Court of Justice of the European Union (CJEU) invalidated the European Commission decision that established the Safe Harbor (14 PVLR 1825, 10/12/15). This decision was in part due to concerns about the United States' domestic surveillance practices, as well as the conclusion numerous U.S.-based companies were not complying with the restrictions of the safe harbor.

As a result of this decision, EU data privacy regulators are no longer required to recognize the Safe Harbor as a means for organizations to comply with EU data protection laws. With this one decision, the CJEU disrupted more than a decade of privacy and cybersecurity practices.

Organizations that previously relied on Safe Harbor certification must now seek another method of legal compliance. Failure to find an alternative means of compliance — or stop transferring data—could expose an organization to fines or orders to suspend data flows. To assist companies with this major legal transition, the European Commission issued a formal Communication in November providing guidance on how to lawfully transfer personal data from the EU into the U.S. now that the U.S.-EU Safe Harbor framework has been invalidated.

One of the options is making operational changes, such as requiring revocable consent from each data subject or shifting data processing servers to the EU to avoid trans-Atlantic data transfers altogether. Of course, such operational changes may be cost-prohibitive or logistically impossible for certain companies.

For those companies, the Commission highlighted other options more similar to the invalidated safe harbor. The main option is ''model contracts'', which contain provisions pre-approved by EU regulators, to govern transactions involving trans-Atlantic data transfers.

Another option for establishing lawful trans-Atlantic data transfers is to adopt Binding Corporate Rules (BCRs). Similar to the Safe Harbor, successful utilization of BCRs requires an organization to demonstrate implementation of adequate safeguards for protecting personal data throughout its organization; however, BCRs are limited in scope and cannot apply to transfers of data outside a corporate group.

Although the EU is working with the U.S. government to negotiate a way to address the invalidation of the Safe Harbor, companies should not rely on the success of those negotiations. If ''no appropriate solution'' is found by the end of January 2016, the Commission has expressly stated EU Data Protection Authorities ''will take all necessary and appropriate action, including coordinated enforcement action.''

Companies that have historically relied on the Safe Harbor, therefore, are strongly advised to immediately evaluate their alternative compliance options for transfers of personal data from the EU to the U.S.

Taking Action in 2016

In 2016, we will witness the full effects of the *LabMD* decision and the invalidation of the EU Safe Harbor and the further development of nascent state and federal cybersecurity requirements. Just as importantly, we will likely continue to witness an increase in enforcement efforts at the state and federal level.

Cybersecurity is now on the radar of almost every regulatory agency, and many—including the FTC, SEC, OCR, and FCC—are actively enforcing cybersecurity standards. There are also enough decisions and published guideposts that pleading ignorance of the standards is not likely to garner much sympathy. All organizations are expected to have basic cybersecurity policies in place and properly implemented, and all organizations are expected to be able to respond appropriately to data breaches.

All organizations—particularly those that have not yet addressed cybersecurity at a senior management and board level—should take action in the coming year to ensure that they are keeping up with developments in this area. For those looking for a place to start, we provide an overview of key steps below.

First, identify and understand your cybersecurity risks. This includes understanding the details of how your company collects, uses, and discloses information, and how your internal IT environment and vendor relationships operate.

A critical part of this process is conducting a thorough security risk analysis—often the first thing regulators ask to see when they open an investigation. Once the security risk analysis is complete (or updated, if the

previous analysis was more than a year old), an organization can begin working toward reducing risk.

Second, identify and understand your legal obligations. All companies will be subject to state or federal laws or regulations, or self-regulatory programs that establish minimum standards for information security practices. Before a company can take action, it must understand its obligations.

Third, once the key risks and obligations have been identified, take technical measures to help reduce the risk and potential severity of a cyber incident. Beginning with an audit of the technical measures currently in place, an organization should update the security of its day-to-day practices, including restricting data collection to only what is needed, controlling access to information, and segregating and encrypting especially sensitive information. Companies may also want to consider hiring cybersecurity vendors to help detect and prevent attacks.

Fourth, review and update your internal policies and procedures. These must ensure compliance with your legal obligations and provide at least reasonable protection for the data you control. Written information security policies, detailed data breach plans, document retention policies, password policies, privacy policies, and other information-centered policies should be reviewed on at least an annual basis. Companies across the country are being fined, penalized, and even subjected to corporate compliance programs and government monitoring or oversight simply because their internal policies are out-of-date or inadequate to address the true security requirements of their operations.

As part of this review, every organization should ensure that these policies are properly implemented—an inaccurate policy that isn't followed is often worse than having no policy at all. Google, for example, entered into a $22.5 million settlement with the FTC due to allegations that its customer-facing privacy policy misrepresented its actual practices.

Fifth, review the agreements you have in place with vendors that help store or process your organization's information. Do these agreements impose proper security obligations on those vendors? You may be able to shift cybersecurity liability through your service contracts, and you should certainly seek to review and audit your vendors' security practices to ensure that they value protecting your information as much as you do.

Sixth, companies should evaluate the costs and benefits of acquiring cybersecurity insurance. These policies can vary significantly in coverage, but they can offer key protections against uncertain and ever-developing cyber risks and can even be an impetus to help you evaluate and harden your organization's procedures. We continue to see an increase in contracts that require a company—especially one handling a third party's data—to obtain cybersecurity insurance.

Throughout all of these steps, be sure that all of the proper stakeholders are involved: boards, senior management, legal counsel, information technology experts, public relations experts, and others integral to ensuring that cybersecurity is taken seriously. Done right, cybersecurity is an organization-wide effort.

There is no way to eliminate cybersecurity risk entirely. At the same time, the recent regulatory and legal developments have made clear that inaction is unacceptable. By following the steps above and focusing on your organization's preparedness and responsiveness, you can transform cybersecurity from a ticking time bomb into a manageable risk.

  PVLR ISSN 1538-3423