Hack to the Future: Ten Cyber Risk Developments to Watch in 2015

January 2015 • Lockton Companies

Cyber breaches, cyber attacks, and related developments frequently dominated the news in 2014. Looking back can help us anticipate and prepare for what may happen in 2015. Here are the most important developments of 2014 and the trends we are likely to see in 2015 related to cyber risk and insurance.

WILLIAM BOECK
Senior Vice President
Insurance & Claims Counsel
Global Technology & Privacy Practice
+1 816.960.9670
wboeck@lockton.com

1. BIG DATA BREACHES

Any look back at what happened in 2014 would have to begin with the large number of significant payment card data breaches that hit retailers including Target, Home Depot, and Staples. Apart from the effects these breaches have had on the companies involved (such as lost income, executives losing their jobs, and shareholder lawsuits) these large breaches may be most noteworthy for their effect of raising the level of attention given to cyber risks within companies, and for spurring changes to payment card systems in the US and beyond. These breaches have also had important ramifications in the cyber insurance market.

LOCKTON®

While payment card data breaches grabbed most of the headlines, it is important to note that other significant breaches took place involving other types of data.

- In May 2014, eBay announced that employee login credentials had been breached which could allow criminals to access personally identifiable information (PII) of eBay users.
- JPMorgan Chase disclosed that information for 83 million accounts had been breached.
- On the healthcare front, roughly 4.5 million patient records were breached at Community Health Systems. That could be the largest reported breach of protected health information (PHI) ever. The breach reportedly was the result of a cyber attack originating from a country more often associated with industrial espionage than the compromise of individuals' personal information.

2. AGGRESSIVE REGULATORS

2014 saw US regulators become even more aggressive with respect to data privacy and security issues. The FTC at least temporarily[1] weathered a challenge by Wyndham Hotels to its ability to regulate cyber security matters, and has continued to be very active in this space.

Notable FTC actions last year include:

- The first enforcement action[2] involving the Internet of Things.[3]
- Increasing focus on enforcing companies' compliance with their information privacy policies.
- Bringing an action[4] against a company and its former CEO in connection with the collection of health information (unusual because the claim is brought against a corporate officer and because the Office of Civil Rights (OCR) in the federal Department of Health and Human Services typically gets involved with PHI risks, not the FTC).
- Actions against Apple[5] and Google[6] in connection with in-app purchases by children without parental consent.

The fines stem from companies' failure to implement appropriate protections for consumer information, use of consumer information for marketing purposes, and do not call list violations. The Federal Communications Commission (FCC) showed up at the cyber security regulators party last year, and has issued millions of dollars in fines. The FCC could be a significant regulator going forward.

The Office of Civil Rights (OCR) in the Department of Health and Human Services has stated that they are bringing more data privacy and security enforcement actions than ever.[7] They aren't focused only on big breaches either. For example, the OCR reached a settlement[8] with QCA Health Plan, Inc., involving a stolen laptop with unencrypted PHI of only 148 people. This resulted in a $250,000 fine and a number of corrective measures.

The SEC has also joined the party. In 2011 the SEC issued guidance[9] on cyber security issues for companies. In 2014, they took action. In April, the SEC Office of Compliance Inspections and Examinations (OCIE) announced[10] that it would be auditing 50 broker-dealers and investment advisors to assess their cyber risks and preparedness. The SEC has made clear[11] what it expects companies to do to prepare for cyber risk; well-informed commentators say that this is a prelude to enforcement actions in 2015.

Regulators outside the US are also gearing up to become more aggressive. A few examples:

- The European Parliament has updated its laws to provide for fines of up to €100 million for violation of data protection laws.
- In Germany, the Commissioner for Data Protection and Freedom of Information for the state of Rheinland-Pfalz imposed a fine of €1.3 million[12] on Debeka Health Insurance AG (Debeka) to resolve issues regarding misuse of protected consumer data. Debeka also agreed to pay €600,000 to endow a university chair to study data protection.
- The Australian government has amended the Privacy Act of 1988[13] to include the Australian Privacy Principles.[14] The Office of the Australian Information Commissioner (OAIC) has published guidance[15] for data breach notifications that stress the ability of the OAIC to bring enforcement actions and assess fines where appropriate.
- In the UK, the Information Commissioner's Office has continued to be active[16] in enforcing data privacy rights and obligations.

3. THE RIGHT TO BE FORGOTTEN

2014 was a year when the "right to be forgotten"[18] took important steps forward. In May, the European Court of Justice ruled[19] that Google must remove information about an EU citizen that was no longer relevant and that could reflect badly on him. Since then, Google and others have received hundreds of thousands of requests to remove information that was once public. While the EU has issued guidelines[20] to assist companies in deciding what to remove, the difficulties the requests present for companies receiving them are nevertheless significant.

Lest anyone think the right to be forgotten is a non-US issue, it is worth noting that aspects of it are creeping into US laws. As of January 1, 2015, California law[21] requires websites to include an "eraser button" that allows children under the age of 18 to delete information they have created on web sites where they are registered users.

4. NIST CYBER SECURITY FRAMEWORK

In February 2014, the US National Institute of Standards and Technology (NIST) published its Framework for Improving Critical Infrastructure Cybersecurity.[22] The Framework is intended to provide companies with a description of what a comprehensive cyber security program should contain. Further development of the Framework by NIST is encouraged in the recently passed Cybersecurity Enhancement Act of 2014.[23] Given that the NIST Framework is quickly becoming a baseline for companies to follow, the Framework will be important to watch in 2015.

5. CYBER EXTORTION ON THE RISE

As Brian Krebs of KrebsOnSecurity.com[24] put it, 2014 was the year cyber extortion went mainstream. 2014 saw significant growth in extortion scams by criminals that infected a victim's computer system with ransomware[25] that will corrupt or delete data unless the ransom is paid.

A typical scam would be one where the victim's files are encrypted and cannot be restored without the encryption key. The criminals provide the key in return for the ransom payment. Unfortunately, the ransom demanded is often small enough that companies elect to pay it (often by Bitcoin[26]) rather than take on the expense and headache of recovering data by other means.

While there were notable successes in combatting cyber extortion scams in 2014, such as the takedown of the botnet[27] that made distribution of the Cryptolocker[28] ransomware possible, as long as extortion scams continue to succeed, their prevalence in 2015 seems assured.

The moral of the story is:

- Back up your data, and
- Carry cyber policies that will respond to an extortion event.

6. MOBILE PAYMENTS AND DIGITAL WALLETS

In 2014, Apple introduced Apple Pay.[29] For those unfamiliar with it, Apple Pay involves giving your credit card information to Apple which will then place a token[30] associated with that number in an encrypted chip on an iPhone 6. The phone can then be used to pay for purchases without the credit card or credit card number ever being disclosed to the merchant or to criminals that have compromised the merchant's systems. Apple Pay, and other existing or upcoming systems designed for the same purpose, appear likely to reduce or eliminate the risks inherent in using payment cards today. These systems seem certain to become more widely adopted in 2015, with the result being that payment card data breaches should eventually become smaller and less severe.

7. EMV PAYMENT CARD MIGRATION

One of the most important events that will take place in 2015 is the migration of payment cards in the US from magnetic stripes to chip-and-pin EMV cards. EMV cards are considered more secure because they require thieves to have more than the card number to make fraudulent charges. To make a charge with an EMV card the user must also input a PIN associated with the card.

One of the most important events that will take place in 2015 is the migration of payment cards in the US from magnetic stripes to chip-and-pin EMV cards.

The migration to EMV cards will take place this year because the card brands are imposing a liability shift on October 1, 2015. If a merchant has not installed equipment to handle EMV card payments, and a customer has an EMV card, the merchant will be liable for any resulting fraud on the customer's account. If the merchant has installed the necessary equipment to handle EMV card transactions,

but the customer's bank hasn't issued him or her an EMV card, the bank is liable. If the merchant is set up to handle EMV cards, if a customer uses an EMV card, and if fraud nevertheless takes place, the card brands will be liable.

The importance of the EMV card migration and the liability shift cannot be overstated. It is absolutely essential that every business that accepts payment cards understand and prepare for this now.

8. INTERNATIONAL CONFLICTS OVER PRIVACY RIGHTS

In 2014 the US and EU collided over the disclosure obligations of Microsoft concerning data pertaining to EU citizens that Microsoft stores in the EU.

A US Government agency (we don't know which one) served Microsoft with a search warrant[31] for the content of an individual's email account. The contents are stored on a server in Dublin, Ireland.

Microsoft has resisted the warrant on the grounds that US search warrants don't apply to locations outside the United States. As Microsoft's Deputy General Counsel[32] put it, the "US government doesn't have the power to search a home in another country, nor should it have the power to search the content of email stored overseas."

Predictably, the European Commission agrees. The EC takes the view that the information can only be obtained via established legal frameworks that provide access to it.

The US government has argued (successfully so far) that the warrant applies to any location under Microsoft's control.

Microsoft (with the active support of Ireland[33] and the EU[34]) is continuing to resist efforts to obtain the data because providing it would violate EU law. This battle will continue in 2015 and will be interesting to watch, given the ramifications the case is likely to have on the legal frameworks governing the cross-border transmission of information subject to privacy protections.

This battle will continue in 2015 and will be interesting to watch, given the ramifications the case is likely to have on the legal frameworks governing the cross-border transmission of information subject to privacy protections.

9. PHYSICAL DAMAGE FROM CYBER EVENTS

Many people will recall the Stuxnet[35] worm that infected computers in Iran that controlled nuclear centrifuges and physically destroyed a large number of them. In 2014 it was reported[36] that an attack on a steel mill[37] in Germany resulted in serious damage to blast furnaces there. The possibility of similar future attacks on industrial control systems is real and must be taken seriously. This will be an issue to watch in 2015.

10. CHANGES IN THE CYBER INSURANCE MARKET

As a consequence of the large and expensive retail breaches over the past year, the cyber insurance marketplace changed dramatically in late 2014.

Cyber coverage for companies with payment card data is becoming more expensive and harder to get. Underwriters are asking deeper questions and are asking for more information than they have in the past. Some insurers are no longer willing to cover such companies; others are reducing the policy limits they are willing to provide. In addition to underwriting becoming more stringent, pricing is going up (even on, and sometimes especially on excess layers). All of this comes at a time when there is unprecedented demand for cyber insurance.

Companies that don't have payment card data exposures are not facing the same problems. For them the availability and cost of cyber insurance has changed little in the past year.

Cyber underwriters continue to innovate. In 2014, AIG introduced its CyberEdge PC[38] policy that, for the first time in a form for general use, can cover property damage and bodily injury resulting from a cyber event. It does this by providing excess DIC coverage over a company's existing insurance programs. We also continue to see a willingness on the part of some underwriters to push the envelope on cyber policy terms and conditions in order to provide solutions, not just policies, to clients. That is essential at a time when the cyber risks companies face are so dynamic.

Sources

1 http://www.bna.com/3rd-circuit-wade-n17179893179/

2 http://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles

3 http://en.wikipedia.org/wiki/Internet_of_Things

4 http://www.ftc.gov/news-events/press-releases/2014/12/medical-billing-provider-its-former-ceo-settle-ftc-charges-they

5 http://www.ftc.gov/news-events/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million

6 http://www.ftc.gov/news-events/press-releases/2014/09/google-refund-consumers-least-19-million-settle-ftc-complaint-it

7 http://www.dataprivacymonitor.com/enforcement/hhs-attorney-major-hipaa-fines-and-enforcement-coming/

8 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/qca_agreement.pdf

9 http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

10 http://goo.gl/WCS39M

11 http://www.sec.gov/News/Speech/Detail/Speech/1370542057946

12 http://goo.gl/iIkiRQ

13 http://www.comlaw.gov.au/Details/C2014C00757

14 http://www.oaic.gov.au/privacy/privacy-act/australian-privacy-principles

15 http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-guides/data-breach-notification-guide-august-2014.pdf

16 https://ico.org.uk/action-weve-taken/enforcement/

18 http://en.wikipedia.org/wiki/Right_to_be_forgotten

19 http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf

20 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf

21 http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568

22 http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

23 https://www.congress.gov/bill/113th-congress/senate-bill/1353/text

24 http://krebsonsecurity.com/2014/06/2014-the-year-extortion-went-mainstream/

25 http://en.wikipedia.org/wiki/Ransomware

26 http://en.wikipedia.org/wiki/Bitcoin

27 http://en.wikipedia.org/wiki/Botnet

28 http://en.wikipedia.org/wiki/CryptoLocker

29 http://www.apple.com/apple-pay/

30 http://en.wikipedia.org/wiki/Tokenization_%28data_security%29

31 https://www.eff.org/document/search-warrant-email-stored-microsoft

32 http://blogs.microsoft.com/on-the-issues/2014/04/25/one-step-on-the-path-to-challenging-search-warrant-jurisdiction/

33 http://digitalconstitution.com/wp-content/uploads/2014/12/Ireland-Amicus-Brief.pdf

34 http://digitalconstitution.com/wp-content/uploads/2014/12/albrecht-microsoft-ireland-amicus-brief1.pdf

35 http://en.wikipedia.org/wiki/Stuxnet

36 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile

37 http://www.securityweek.com/cyberattack-german-steel-plant-causes-significant-damage-report

38 http://www.aig.com/cyberedge-pc_1247_593419.html

LOCKTON

Our Mission

To be the worldwide value and service leader in
insurance brokerage, employee benefits, and risk management

Our Goal

To be the best place to do business and to work

www.lockton.com

g\white paper\boeck\2015\boeck-hack to the future-jan15.indd\#3547