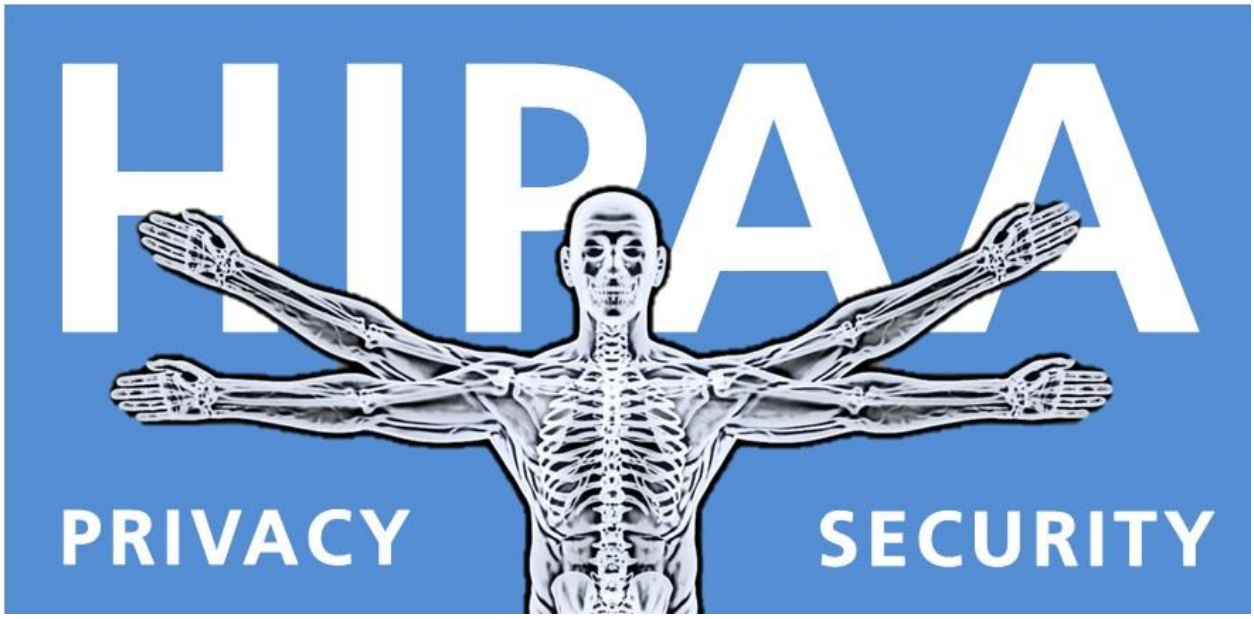


HEALTH PRIVACY + SECURITY UPDATE

Health Data Security in Crisis, Phase 2 Audits, and Other HIPAA Privacy + Security Updates

By Daniel J. Solove + Paul M. Schwartz

2015 Issue 1

This post is part of a post series where we round up some of the interesting news and resources we're finding. We have split the health/HIPAA material from our updates on other topics. To see our updates for other topics, click here. For a PDF version of this post, and for archived issues of previous posts, click here.

HEALTH PRIVACY

HHS HIPAA Enforcement Actions

HHS OCR announces $125,000 resolution agreement with Cornell Prescription Pharmacy for shortcomings in safeguard PHI, training (April 2015) [Link]
-- HHS charged the following violations of HIPAA: failure to reasonable safeguard PHI, failure to implement written policies and procedures to comply with the Privacy Rule, failure to provide and document training on HIPAA Privacy Rule policies and procedures
-- Resolution Agreement [Link] - $125,000 penalty, 2-year corrective action plan (CAP)

HHS critiqued for not issuing enough fines for health data breaches (April 2015) [Link]
-- Sisi Wei and Charles Ornstein write in ProPublica: "Since October 2009, health care organizations and their business partners have reported 1,199 large-scale data breaches, each affecting at least 500 people, to the U.S. Department of Health and Human Services. Of those, seven breaches have resulted in fines."
-- Cite: Sisi Wei and Charles Ornstein, *Over 1,100 Health Data Breaches, but Few Fines* (April 16, 2015)

Only 1 OCR resolution agreement in 2015 [Link]
-- Thus far, there has been only 1 OCR resolution agreement so far in 2015.
-- In 2014, there were 6 resolution agreements.
-- There were 5 resolution agreements in 2013 and 5 in 2012.

OCR HIPAA Audits

OCR HIPAA Audits – Phase 2 is beginning [Link]
-- Phase 2 audits will cover both covered entities and business associates
-- OCR sent pre-audit screening surveys for the Phase 2 Audits.
-- 350 covered entities to be selected. BAs of these CEs will then be selected
-- Phase 2 will take place over the next 3 years.
-- Most will be "desk audits" but there will be some onsite ones too.
-- Entities will have 2 weeks to respond to an audit request.

McDermott, Will, & Emery, *Useful Advice for Preparing for a HIPAA Audit* (July 2014) [Link]
Some tips include:
-- confirm that a Risk Assessment has been completed or will be completed soon
-- confirm that "the organization has a complete inventory of business associates for purposes of the Phase 2 Audit data requests"
-- confirm that appropriate documentation is in place for addressable implementation specifications that were replaced by an alternative
-- "[e]nsure that the organization has implemented a breach notification policy"
-- "Confirm that workforce members have received training on the HIPAA Standards that are necessary or appropriate for a workforce member to perform his/her job duties"

FTC Enforcement

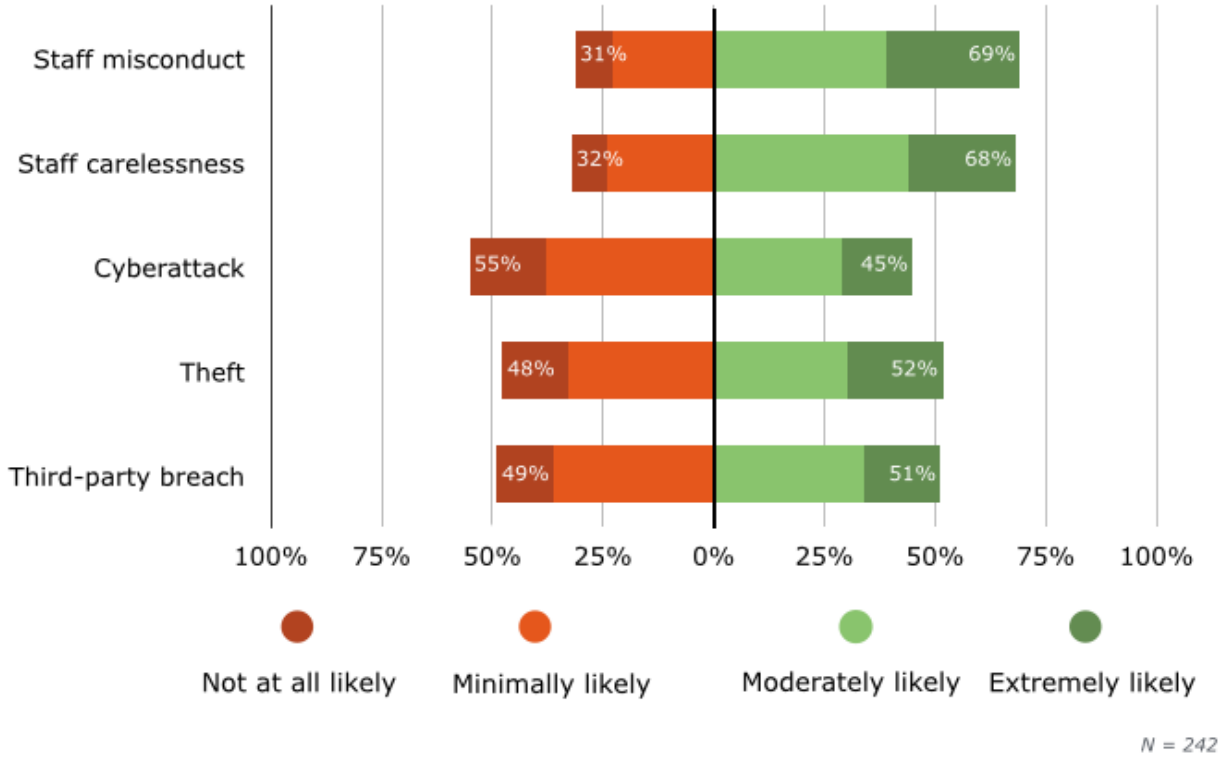
Cora Han, *Using Consumer Health Data? FTC Business Blog* (Apr. 27, 2015) [Link]
-- Discusses how it's not just HHS that protects people's health data – the FTC has resolved a number of cases involving health data.
-- "The FDA plays a role, too, focusing, for example, on apps that are medical devices and could pose a risk to patients' safety if they don't function as intended."
-- The posts lists a few FTC cases involving healthcare data. From the post:

> -- PaymentsMD. The FTC settled allegations that a medical billing company collected consumers' personal medical information without their consent.
> -- GMR Transcription Services. That settlement involved allegations that a medical transcription company outsourced services to a third party without adequately checking to make sure it could implement reasonable security measures.
> -- Accretive Health. According to that settlement, a company providing medical billing and revenue management services to hospitals put consumers' personal information at risk by (among other things) transporting laptops with sensitive data in a way that made them vulnerable to theft. The FTC also said the company gave access to personal information to employees who didn't need it do their jobs.

Reports and Surveys

54% of patients likely to change providers based on privacy violations (March 2015) [Link]
"A combined 54 percent of respondents say they would be "very" or "moderately likely" to change providers as a result of their personal health information being accessed without their permission."

CHART: By Breach Type: Likelihood to Switch Providers After Security Breach

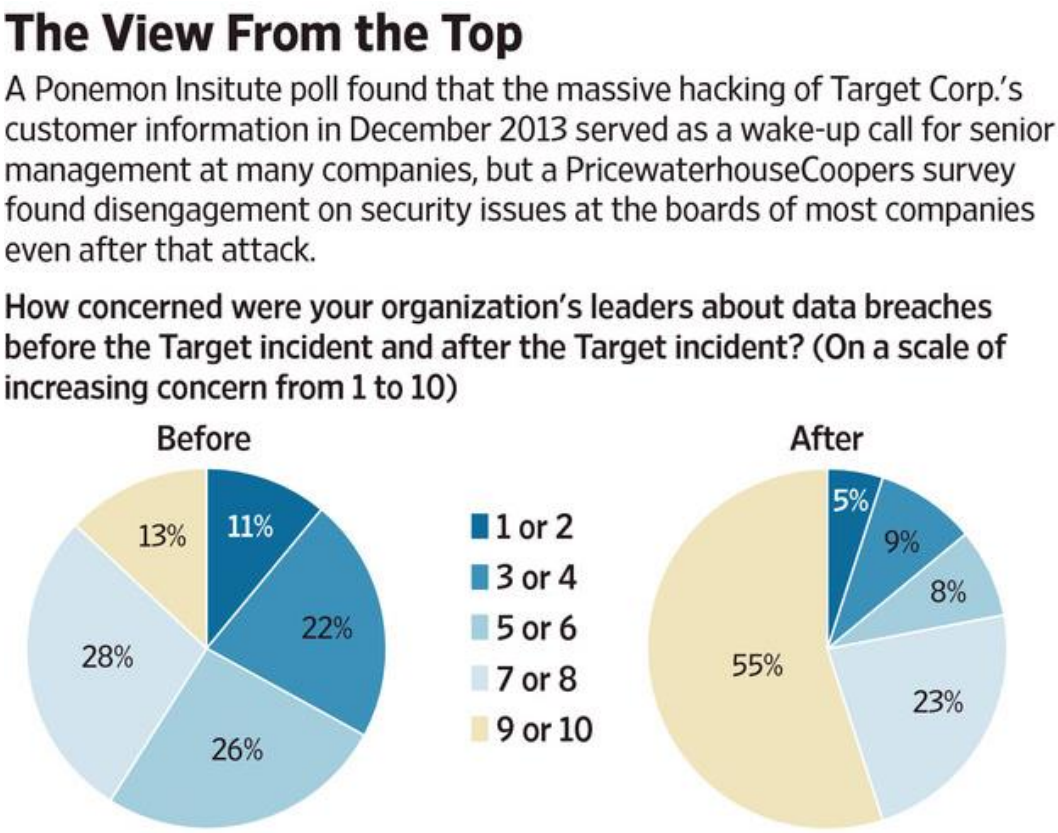


85% of HIPAA breaches are not due to hacking – the leading cause is lost or stolen devices (April 2015) [Link]

Vendors are a major cause of data breaches (April 2015) [Link]
-- "Anywhere from one-fifth to two-thirds of data breaches have been linked to hackers getting into a vendor or third party, according to various surveys."
-- "20% of IT professionals say insufficient vetting of vendors was a leading cause of a breach at their company in 2014"

Only 51% of companies conduct security awareness training (April 2015) [Link]

Upper management a lot more concerned about data breaches April 2015) [Link]
-- Before the Target breach, on a 1-10 magnitude-of-risk scale, 13% of upper management rated data breaches a 9 or a 10; after the Target breach, 55% rated data breaches a 9 or a 10.
-- Before the Target breach, those rating a breach as a 7 or above rose from 41% to 78%.



FBI emphasizes cybercriminals' interest in healthcare information [Link]
Online, a single hacked medical record goes for $70 while the prevailing rate for a stolen credit card number ranges between $0.50 and $1.

Ponemon Institute, *Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data* (May 2015) [Link]
-- 65% of healthcare organizations had more than one data security incident during the past 2 years.
-- 58% of healthcare organizations had "between 11 and 30 electronic information-based security incidents."
-- Greatest risk by far is employee negligence (70%); next highest risk is cyber attacks (40%).
-- 96% of organizations had a security incident involving lost or stolen devices.
-- 88% had a security incident due to spear phishing.

-- 56% say that "more funding and resources are needed to make [an incident response process] effective."
-- 59% of business associates had at least 1 "data breach involving the loss or theft of patient data"; 29% had 2+ breaches.
-- At BAs, 60% of the breaches were discovered by employees – this was the most common way that breaches were detected.

Figure 7. What security threats healthcare organizations worry about most
Three responses permitted

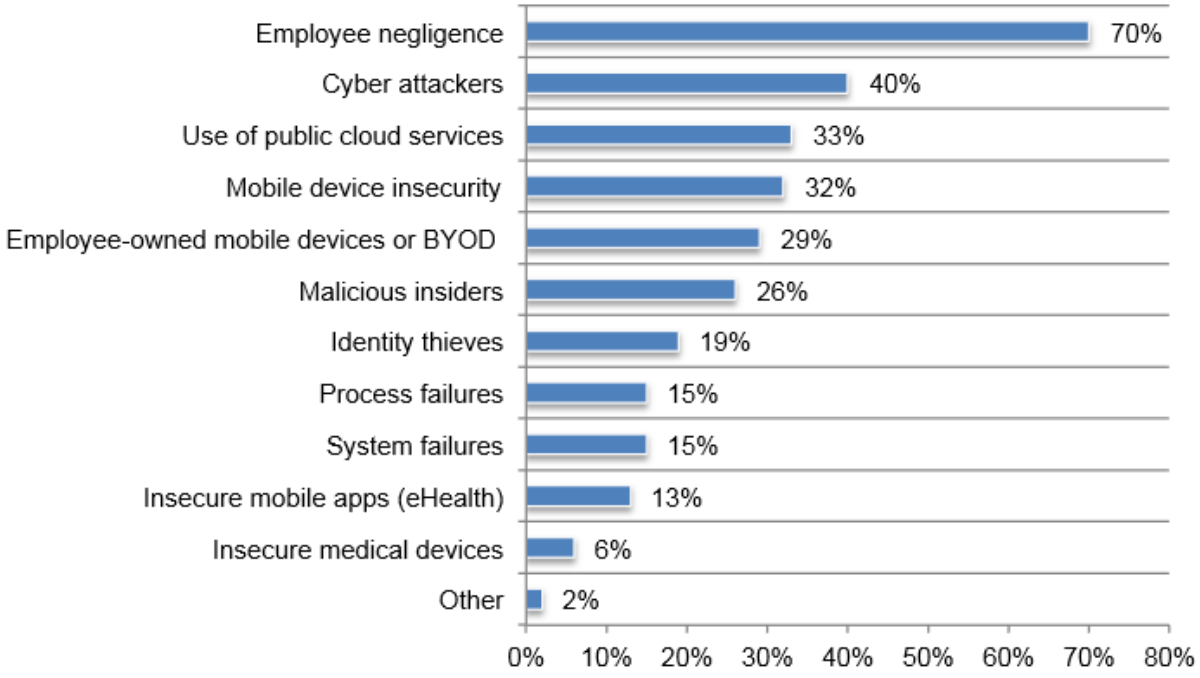
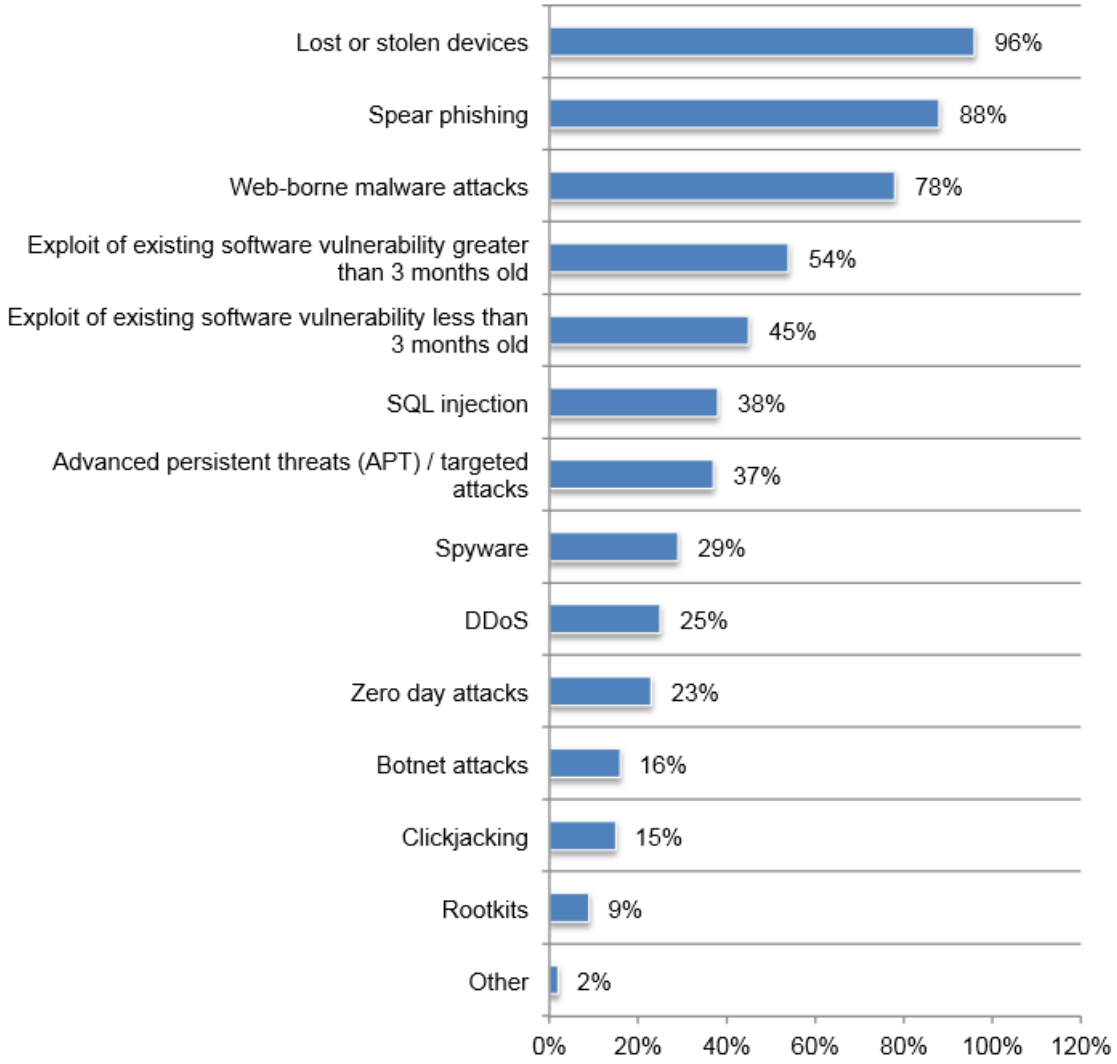


Figure 8. Security incidents healthcare organizations experienced
More than one response permitted



Data Breach

OCR Updates Online Breach Reporting Portal [Link]
The agency made three substantial changes to the information reporting requirements online. First, "Breach End Date" and "Discovery Date" are now required fields. Second, "Safeguards in Place Prior to the Breach" no longer asks for specific technical measures such as "firewalls" or "biometrics" and instead asks for generic measures such as training or policies. Third, "Actions Taken in Response to the Breach" requests specific solutions such as "adopted encryption technologies" or "strengthened password requirements" which may indicate what the department is hoping to see companies do in response to breaches in the future.

Anthem Healthcare (Blue Cross / Blue Shield) loses 80 million names, SSNs to hackers [Link]
Anthem Healthcare, the parent company of Blue Cross / Blue Shield lost 80 million names and social security numbers in a hack. The company is notifying victims by mail, and if possible, email.

Anthem customers targeted by opportunistic phishing attacks [Link]
Many Anthem customers are now receiving emails purporting to offer credit monitoring services. The emails include a link that collects personal information from the user, and there are reports that scammers are also targeting victims by telephone.

CareFirst data breach -- 1.1 million members in DC Area accessed in cyber attack (May 2015) [Link]

ABOUT THE AUTHORS

Daniel J. Solove *is the John Marshall Harlan Research Professor of Law at George Washington University Law School and the founder of* ***TeachPrivacy,*** *a privacy/data security training company. Along with Paul Schwartz, Solove is a Reporter on the American Law Institute's Principles of Data Privacy. He is the author of 10 books including Understanding Privacy and more than 50 articles.*

Professor Solove is the organizer, along with Paul Schwartz of the ***Privacy + Security Forum*** *– Oct. 21-23 in Washington, DC, an event aims to bridge the silos between privacy and security.*

100+ Speakers at the Privacy + Security Forum

Paul Schwartz *is the Jefferson E. Peyser Professor of Law at UC Berkeley School of Law and a Director of the Berkeley Center for Law and Technology. Schwartz is also a Special Advisor at Paul Hastings, where he works in the Privacy and Data Security Practice. He is the author of numerous books and articles on information privacy and information law. With Daniel Solove,*

he is the co-author of Privacy Law Fundamentals (a short reference book) and Information Privacy Law (a casebook).

Professor Solove's HIPAA Privacy + Security Training

The views here are the personal views of Professors Solove and Schwartz and not those of any organization with which they are affiliated.

The authors would like to thank Ariel Glickman, Bryan Lee, Grant Nelson, Amy Roller, Sonia Shaikh, and Adam Shaw for their assistance with this post.

Please join one or more of Professor Solove's LinkedIn groups:

Privacy and Data Security

HIPAA Privacy & Security

Education Privacy and Data Security

Image Credits: Fotolia + DJS Mashup

Click below to sign up for Professor Solove's newsletter. It is free and is only sent out occasionally, so it will not clog your inbox.