BakerHostetler

Brief

The BakerHostetler Data Security Incident Response Report 2015

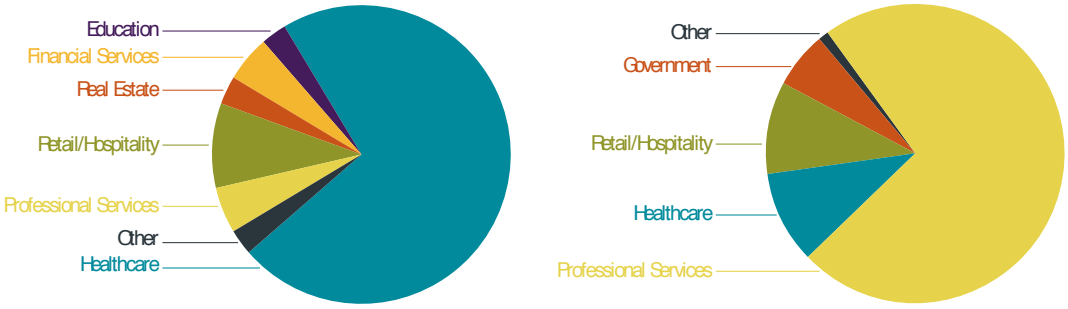
The rate of disclosures of security incidents in 2015 continues at a pace that caused many to call 2013 and then 2014 “the year of the breach.” Most incidents are described publicly with attention-grabbing terms such as “hack” or “breach,” but those terms are inadequate to describe the diversity of incidents companies are facing. Though there is some speculation that “breach fatigue” is setting in, high-profile incidents continue to grab headlines. Privacy and data security issues are firmly entrenched as a significant public and regulatory concern and a risk/opportunity that executive leadership and boards of directors must confront.

In this climate of heightened awareness, the forensic investigation firms we work with release annual reports identifying trends from their prior year investigations. Because of the value we have found in these annual reports when working to help companies become better prepared to detect and respond to incidents, we decided to begin issuing our own annual reports to enhance the discussion of the nature of the threats faced by companies, as well as detection and response trends, and the consequences that follow. This inaugural 2015 BakerHostetler Security Incident Response report provides insights generated from our review of the more than 200 incidents on which BakerHostetler’s award-winning Privacy and Data Protection Team advised clients in 2014.

Our report is based on data for incidents affecting more than 160 clients and includes dates of incident, discovery and notification, the number of individuals notified, data at risk, mitigation solutions, regulatory and law enforcement involvement, vulnerability types, the use of support services, and post-notification consequences.

We hope that this report will assist companies in becoming “compromise ready.”

No Industry is Immune but Frequency and Severity Differ



Frequency Severity

Incidents do not discriminate – they affect all industries. Why? Because they do not occur only to companies that have payment card data or protected health information (PHI). All companies have employee data and disruptive malware is prevalent. Websites are defaced by politically motivated hacktivists and attacks are initiated by cybercriminals looking for profit or intellectual property. Our 2014 data set confirms this, with all industries represented. The sectors affected the most were education, financial services, real estate, retail/hospitality, professional services, and healthcare. Tens of thousands of incidents involving PHI have been reported since HITECH's breach notification requirement went into effect in 2009, so it is no surprise that by frequency, healthcare tops our list. While PHI incidents are disclosed more frequently, driven in part by HIPAA presumption that a breach occurred, the severity when measured by number of affected individuals is often less (many incidents affect less than 10 people). It is also not surprising that professional services and retail/hospitality services providers top the list when it comes to severity. And because incidents affecting these sectors often require forensic investigation and draw more media coverage, the cost and potential financial consequences are dramatically higher on a per-incident basis.

Human Error is Most Often to Blame

If you read the annual reports of forensic firms you will see that phishing and spear-phishing is the predominant method used to attack companies. Because not all incidents involve an external attack (we engaged a forensic firm in 30 percent of the incidents on which we worked), our list of the top five causes of an incident is a little different. These causes are:

1 employee negligence;

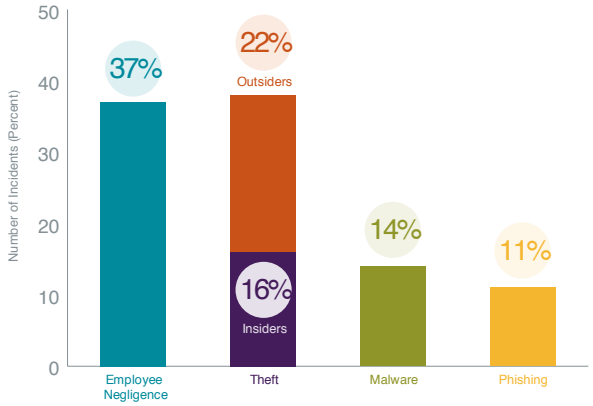
2 external theft of a device;

3 employee theft;

4 phishing; and

5 malware.

The large number of the incidents we saw in 2014 that included employee negligence as part of the primary underlying cause is proof that companies cannot eradicate security risk solely through the use of better technology. Sure, encrypting portable devices can help in cases where employees leave devices in unlocked cars, but technical security solutions do not stop employees from being phished, failing to review logs, or improperly configuring servers. Companies must match security solutions that provide defense-in-depth with detection capabilities as well as employee training and awareness driven by the right "tone from the top" and appropriate information security policies and procedures.



A definitive cause was determined for 139 of the incidents. In those cases, 51 (37 percent) could be attributed to employee negligence. Theft was the cause of 53 incidents (38 percent), 31 (22 percent) by outsiders and 22 (16 percent) by insiders. Malware was responsible for 20 incidents (14 percent) and phishing for only 15 (11 percent).

Why Rapid Detection is Critical

Forensics firms continue to report that as many as two-thirds of the incidents they investigate are not self-detected by the company. Our data showed the opposite. Incidents were discovered by our clients—as opposed to a third party—64 percent of the time. Of the 36 percent discovered by third parties, 27 percent were due to theft. We cannot stress enough the need for companies to spend sufficient time and resources developing their detection capabilities.

Timing is crucial at all stages of an incident response. An incident needs to be detected and the cause identified as quickly as possible. If a company is slow to detect, or worse, does not self-detect, it will face at least four major issues:

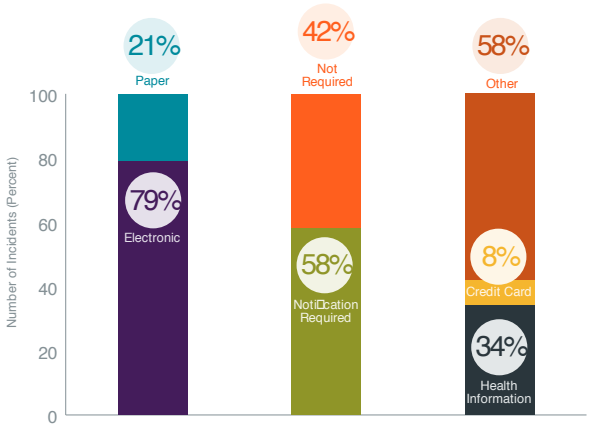
1. The company misses an opportunity to block the attack before it gets to critical data and is slower to mitigate potential harm to the company and affected individuals;
2. Forensic data that could be used to precisely determine what occurred, and thereby limit the scope of at-risk data and offer some reassurance to affected individuals, may be lost (e.g., logs are overwritten);
3. If the data is actually used for fraud or identity theft, signs of the misuse may be detected by third parties, which can lead to the story breaking publicly before the company is aware of the incident; and
4. When third parties break the story, the company often is forced to discuss the incident before it can investigate and contain the incident and then explain what occurred, who is affected, what mitigation services it is offering, and what it is doing to prevent the issue from occurring again. As a result, the company is more likely to be viewed as not handling the incident well. Companies that face this scenario often say too much too soon in an effort to reassure or deflect, which often then leads to more intense scrutiny and an increased likelihood of adverse consequences.

Detection Times Must be Shortened

Of the incidents in which we identified the dates of detection and notification, the average amount of time that elapsed from incident occurrence to detection was 134 days. Many of the incidents we worked on involved PHI, for which notification is required within 60 days of discovery. On average, notification was made to affected individuals within 50 days of the time the company became aware of the incident.

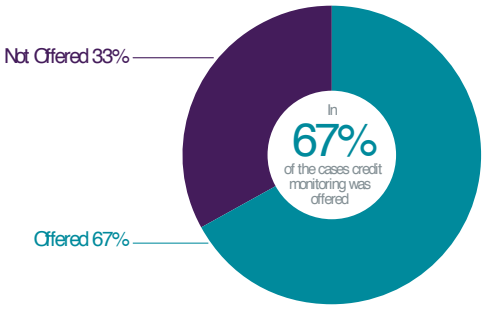
It's Not Just Electronic Records at Risk

Often it is assumed that data security incidents are unique to electronic data, but this is not always the case. Of the incidents we handled in 2014, 21 percent involved paper records. Whether paper or electronic, the data at risk that led to the decision to notify in 58 percent of our incidents was data subject to state breach notification laws, such as Social Security or driver's license numbers and financial account information. Health information was affected in 34 percent of the incidents and eight percent involved payment card data.



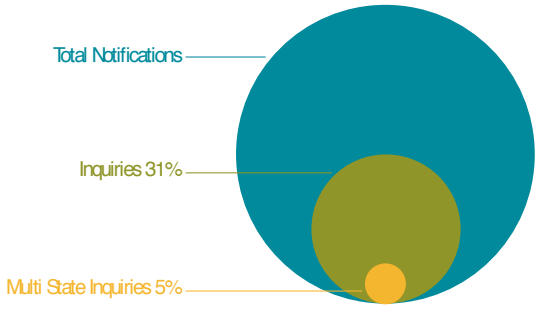
What Happens After the Incident?

We work with clients to find ways to prevent or mitigate the misuse of data at risk. Not only does this help the company mitigate potential liability, it can be part of the company's effort to restore its relationship with customers or patients. In the incidents we handled, credit monitoring was offered 67 percent of the time. Still, credit monitoring may not always be the right solution (e.g., it will not prevent unauthorized charges from being made on a payment card).



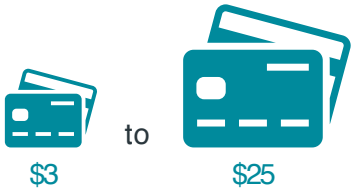
Many assume litigation always occurs after an incident is disclosed. But of 75 incidents where notification letters were mailed or substitute notification was posted, only five of the companies were sued by potentially affected individuals.

Another consequence that follows notification is regulatory action. Of the matters we handled, attorneys general were notified in 59 cases and inquiries were made 31 percent of the time. A multi-state inquiry was initiated less than 5 percent of the time, with the number of investigations involving healthcare and merchants being evenly split.



Merchants who have payment card data stolen from them or from one of their vendors may face non-compliance fines, case management fees, and assessments to reimburse issuing banks for the cost of issuing new cards as well as the incremental fraud that occurred on the stolen cards. We saw fines and assessments from all four card brands in 2014. The PCI DSS non-compliance fines ranged from $5,000 to $50,000. The initial demand for operating expense and fraud assessments ranged from $3 to $25 per card involved.

The PCI DSS non-compliance fines ranged from $5,000 to $50,000.



The initial demand for operating expense and fraud assessments ranged from $3 to $25 per card involved.

In healthcare, when a breach involving more than 500 individuals is reported, our experience is that the Department of Health and Human Services Office for Civil Rights (HHS OCR) initiates an investigation 100 percent of the time. In breaches involving fewer than 500 individuals, an investigation is commenced in just a very small percentage of those breaches. Of the more than 80 HHS OCR investigations we have helped clients defend, just one has resulted in a resolution agreement. In 2014, we helped clients defend against more than 28 investigations initiated by HHS OCR.

After the report of a breach, regulators most often ask to review:

- Copies of policies and procedures governing privacy and security;
- Evidence of education and awareness programs, including attendance logs;
- Risk assessments conducted by the organization over a several-year period preceding the incident;
- Risk mitigation plans developed as a result of the risk assessments;
- Vendor/Business Associate agreements in place, regardless of whether a vendor caused the breach; and
- Copies of disaster recovery and business continuity plans.

What Proactive Steps Should Companies Take?

Because it is not if but when an incident will occur, companies can become "compromise ready" by taking the following steps:

- Developing an incident response plan and practicing execution of the plan with tabletop exercises;
- Working with an experienced security consultant to conduct security assessments (to understand where assets and sensitive data are located);
- Implementing "reasonable" security and detection capabilities based on the recommendations of the consultant;
- Gathering threat intelligence to understand the nature of current risks;
- Conducting personnel training and awareness-raising activities to reduce the chance that an incident will result from employee negligence and those incidents that do occur will be quickly identified;
- Undertaking vendor due diligence and contract analysis, to reduce the chance that an incident will be caused by a company's business contacts; and
- Maintaining ongoing diligence, updating and adapting to changing risks, to proactively guard against evolving and emerging threats.

A board of directors addressing cybersecurity should consider the following oversight actions:

- Forming a risk committee;
- Engaging a "cyber adviser";
- Reviewing risk assessments;
- Evaluating whether the company has the right roles in its structure, including Chief Privacy Officer, Chief Information Security Officer and Chief Risk Officer, to oversee and carry out its privacy and security policies and plans;
- Evaluating privacy and security budgets to make sure that sufficient resources are in place to protect against and respond to data security incidents; and
- Addressing the opportunity for risk shifting through effective cyberinsurance coverage.

Theodore J. Kobus
New York
tkobus@bakerlaw.com
212.271.1504

Gerald J. Ferguson
New York
gferguson@bakerlaw.com
212.589.4238

Craig A. Hoffman
Cincinnati
cahoffman@bakerlaw.com
513.929.3491

Lynn Sessions
Houston
lsessions@bakerlaw.com
713.646.1352

Tanya Forsheit
Los Angeles
tforsheit@bakerlaw.com
310.442.8831

Randal L. Gainer
Seattle
rgainer@bakerlaw.com
206.332.1381

bakerlaw.com

BakerHostetler is one of the nation's leading law firms with more than 900 attorneys coast to coast, delivering the highest-quality legal counsel on the most complex and critical issues facing clients today. The firm has offices in Atlanta, Chicago, Cincinnati, Cleveland, Columbus, Costa Mesa, Denver, Houston, Los Angeles, New York, Orlando, Philadelphia, Seattle, and Washington, D.C.