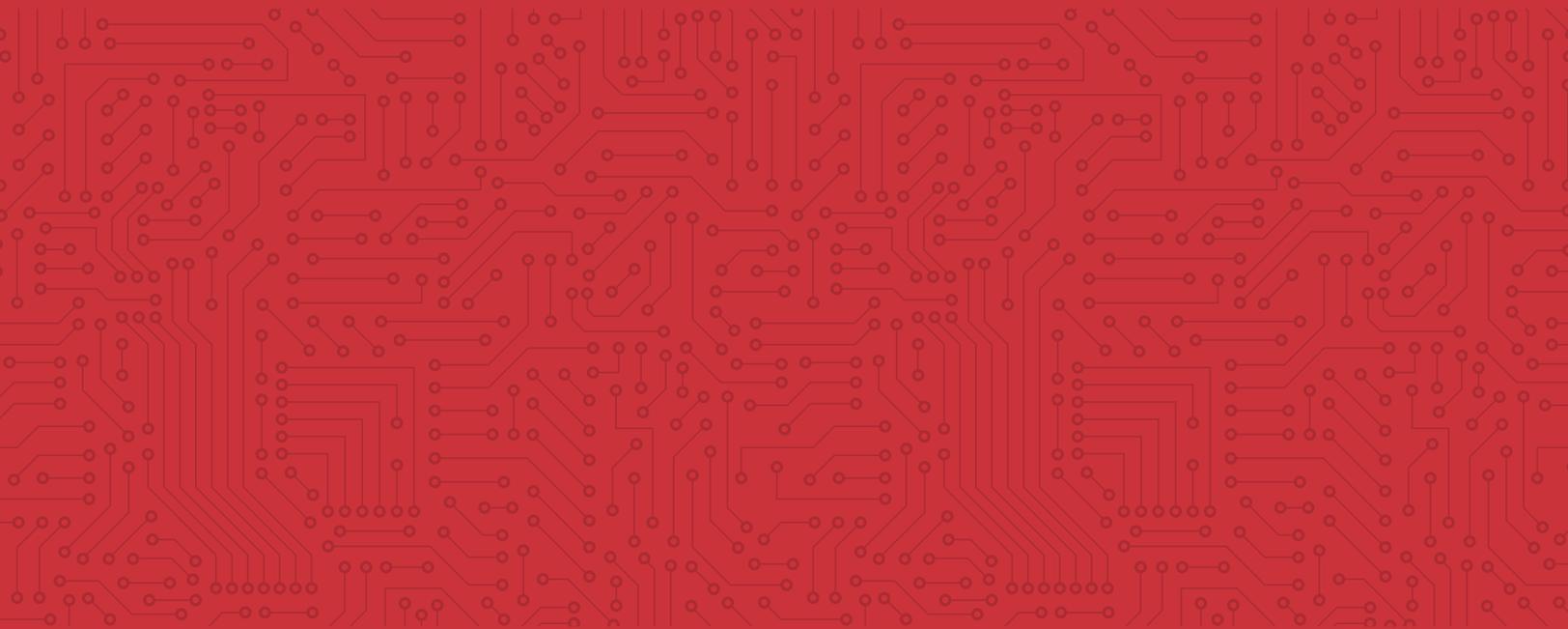


BakerHostetler

Is Your Organization Compromise Ready?

2016 Data Security
Incident Response Report



SUMMARY

Incident Response Trends

The trends from last year's inaugural BakerHostetler Data Security Incident Response Report and this year's edition drive one primary recommendation—the continued need for companies to be “Compromise Ready.”

Every company should be constantly focused on preventing, detecting, and having the right capabilities in place to respond to data security incidents. Accepting that incidents are inevitable does not mean that you stop trying to prevent them. Rather, in addition to reducing risk profiles through information governance and implementing preventative security measures, companies must focus on adapting measures to changing risks, faster detection, containment, and effective response. Central to this is improving preparedness based on internal and external “lessons learned.”

The findings in this Report, developed from analyzing over 300 incidents we helped manage in 2015, are an important component of preparedness efforts. We have identified the issues and consequences companies actually experience. Budgets are tight, and employees are continuously being asked to take on more duties. Having insight into how these issues arise and the resulting financial impact can help companies prioritize and focus data

security incident preparedness decision-making. This Report can also be used to win support for additional personnel and budget increases, and to help management and boards exercise appropriate oversight.

Not convinced that being compromise ready is important? Historically, the primary concern companies had about security incidents was the reputational impact caused by a public disclosure. Our experience shows reputational impact does not necessarily occur just by disclosing an incident. The hardest hits to a company's reputation are more likely to occur when the notification shows that the underlying cause should have been prevented or that the company is viewed as not handling the response well. And contrary to what many believe, a company that is quicker to notify is not always viewed more favorably.

We hope you find a way to use these findings to incrementally improve your company's level of preparedness.

300+
incidents in 2015

This Report shares “lessons learned” from more than 300 incidents in 2015.

The incident response trends indicate:



The range of incident causes is broad



All industries are affected



Detection capabilities need to improve



It is difficult to provide meaningful notification quickly



Identifying a forensic service provider before an incident occurs should be a priority



Mitigation services are not always offered

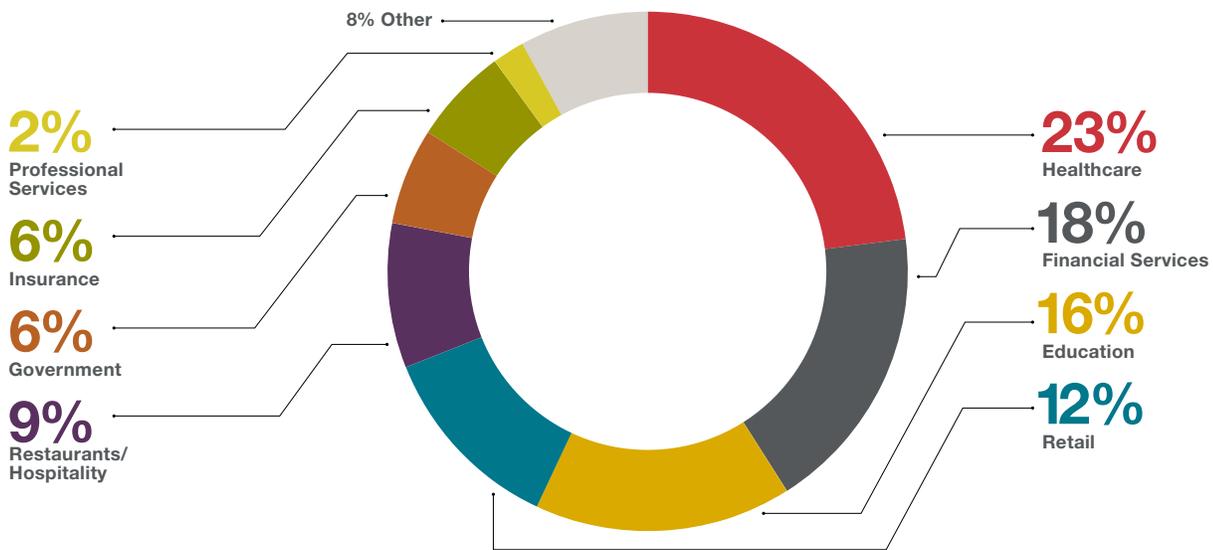


Regulatory investigations are more common than lawsuits after notification occurs

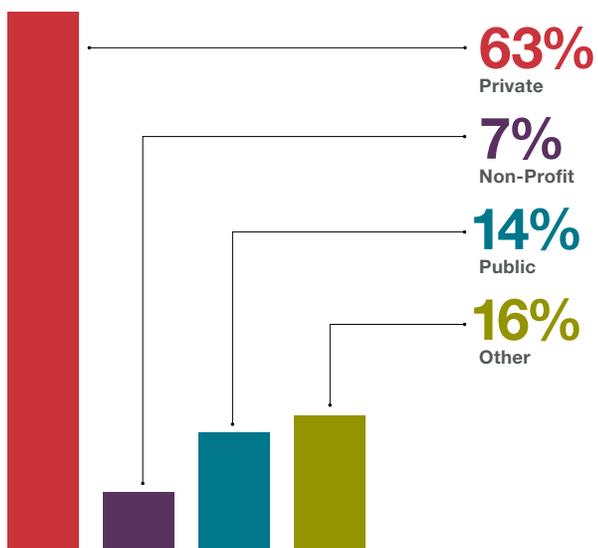
AT A GLANCE

Incident Response Trends

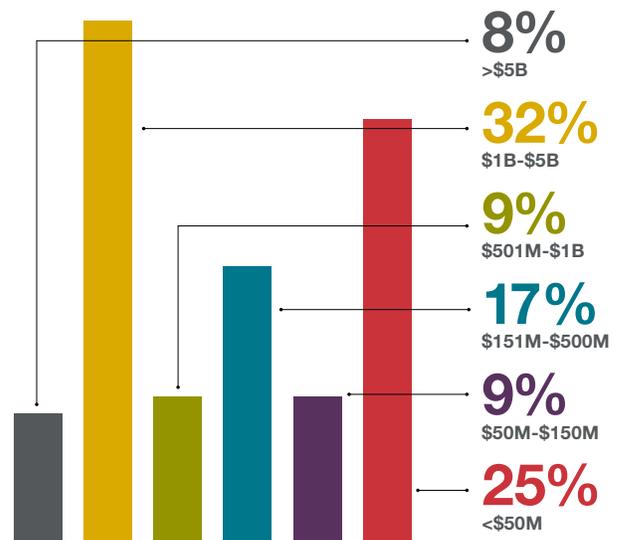
Industries Affected



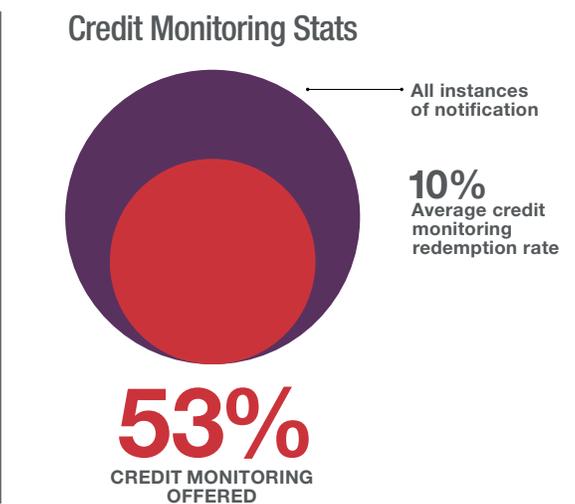
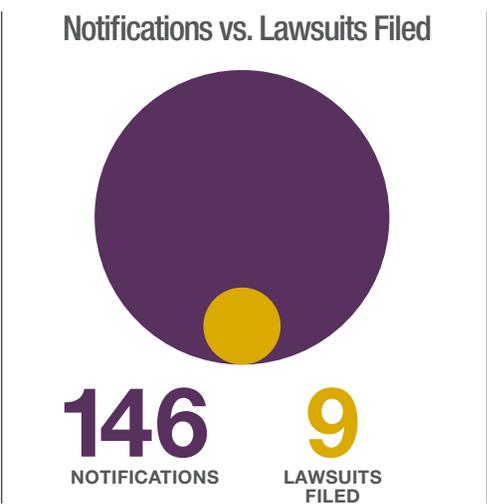
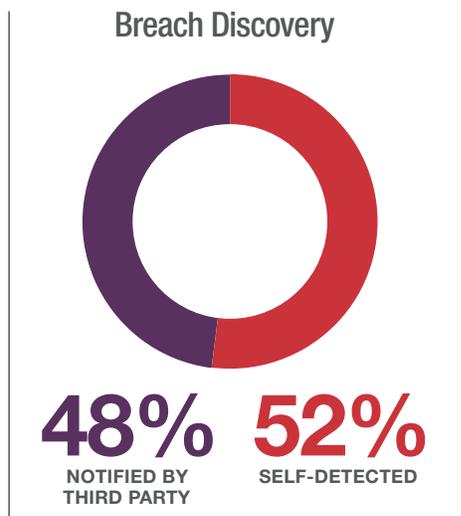
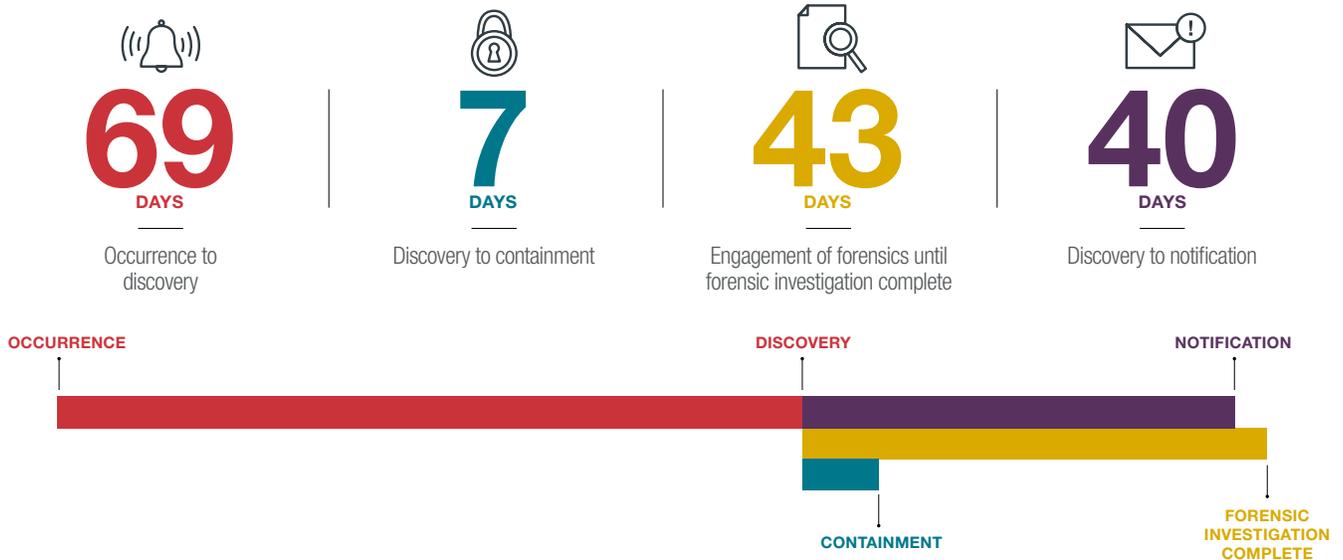
Company Breakdown



Company Size by Revenue



Incident Response Timeline



All Industries Affected— But Not in the Same Way

We reported two findings last year that remain true: (1) incidents do not discriminate—they affect all industries, and (2) there is a difference between frequency and severity of incidents across industries. The volume of data, the value of different data and intellectual property, the number of endpoints to guard, third-party and unknown fourth-party vendors, inadvertent disclosures, commodity malware, ransomware, and threat actors are examples of the types of risks that make incidents inevitable across all industries. Companies that possess data that is easily monetized, as well as companies subject to laws that presume a breach occurred, continue to see a higher percentage of incidents. The sectors most frequently affected in 2015 were healthcare, financial services, retail, and education.

For the second year in a row, healthcare represented the highest percentage of incidents we worked on. And again, while frequency was high, the severity measured by number of potentially affected individuals was relatively low (fewer than 500 individuals per incident on average). And the data that yielded the low average number of affected individuals for healthcare incidents included a couple of healthcare incidents that involved notification to millions of individuals. Topping the severity list by number of affected individuals was restaurants/hospitality, mostly due to financially motivated attacker groups having moved their focus from grocers and big-box retailers to restaurants, hotels, and casinos.

Consistent Findings

- ▶ *Incidents do not discriminate—they affect all industries.*
- ▶ *There is a difference between frequency and severity of incidents across industries.*

Frequency

Percentage of Incidents by Industry

Severity

Average Size of Notification

Industry	Frequency (Percentage of Incidents)	Severity (Average Size of Notification)
HEALTHCARE	23% <i>Healthcare was more frequent but not as severe</i>	340K
FINANCIAL SERVICES	18%	2K
EDUCATION	16%	1K
RETAIL	12%	33K
RESTAURANTS/HOSPITALITY	9%	2.2M <i>Restaurants/Hospitality topped the severity list of number of affected individuals</i>
INSURANCE	6%	1.1M

Why Do Incidents Occur?

Not every incident is attributable to a sophisticated, never-before-seen, unpreventable external attack. The causes are manifold, from a lost unencrypted device, to an employee replying to a phishing message asking for copies of W-2 forms, to unauthorized remote access to a network or a sophisticated threat actor determined to find a point of entry. And not every external attack is attributable to a sophisticated threat actor. There are opportunistic threat actors aware of one exploit, or others who bought a toolkit or rented a botnet online and have limited capabilities. And then there is the people problem. Networks are built, operated, and maintained by people (your own or your vendor's), and people are fallible—which is one of the reasons why regulators focus on education and awareness programs. Mistakes and accidents happen, along with the occasional intentional bad actor (although not as often as people expect).

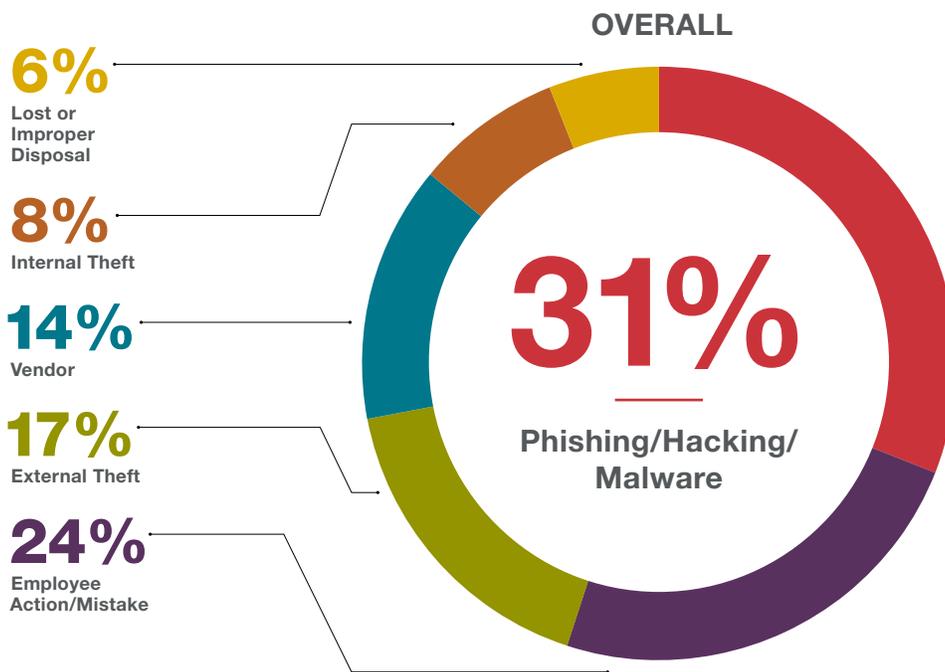
This year phishing/hacking/malware took the number one spot, accounting for about 31% of incidents.

Top causes for healthcare, retail and restaurants/hospitality, and financial services

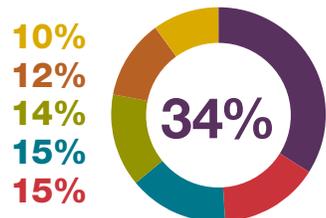
Last year, we identified human error as the leading cause of incidents. While human error continues to be a significant source, this year phishing/hacking/malware took the number one spot, accounting for about 31% of incidents. However, when we looked at the underlying issues that enabled many of the phishing/hacking/malware incidents to succeed, they could often be attributed to human error in some way, so in a way our numbers show that human error is a factor over half of the time.

Causes

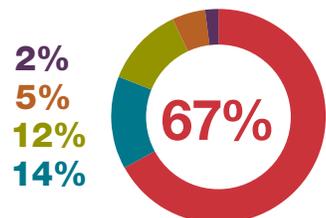
- Phishing/Hacking/Malware
- Employee Action/Mistake
- External Theft
- Vendor
- Internal Theft
- Lost or Improper Disposal



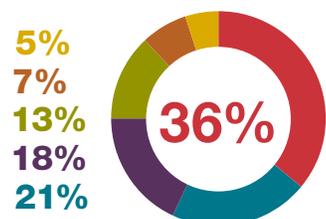
HEALTHCARE



RETAIL AND RESTAURANTS/HOSPITALITY



FINANCIAL SERVICES



Data at Risk

The data at risk that led to the decision to notify in 61% of our incidents was data subject to state breach notification laws—generally a person’s name associated with a Social Security number, driver’s license number, or financial account information. Health information was affected in 27% of the incidents, and 13% involved payment card data.



27%

involved health information



13%

involved payment card data

Number of Individuals Notified

State breach notification laws do not require that notification letters identify how many individuals were affected. Aside from some very large or very small incidents where the company decides for some reason to disclose the number, the number of affected individuals usually is unknown to the public. This presents a challenge for companies trying to project costs of an incident when they are making decisions on insurance. For incidents in 2015 where notification was made to individuals, the average number of individuals notified was 269,609, and the median was 190,000.



AVERAGE:

269,609

MEDIAN:

190,000

The Value of Forensics

After detecting a potential compromise, it is important to work quickly to stop the attack and determine the extent of the incident and scope of information affected. Doing so positions a company to effectively mitigate the issue and tailor any necessary response. A forensic investigation is often the first step in that effort. If a company has good available forensic data, a forensic investigation often enables the company to either confirm that an incident did not occur or identify the specific data that is at risk. More specific and reliable findings often enable better communications about the incident and help to mitigate the consequences that sometimes result from disclosing incidents. Without good forensic data, the findings often leave companies deciding to err on the side of caution and assume that the worst-case scenario occurred because they cannot determine what actually occurred.

A forensic investigation occurred in 31% of the incidents we were involved in. For incidents involving healthcare entities, forensic investigations were used less often (in 13% of incidents). Reasons for this lower usage include incidents caused by oral disclosures, paper records, and other inadvertent disclosures for which forensic investigations were not needed. The average total cost of a forensic investigation was \$102,806.

When a forensic firm is engaged to investigate a potential compromise, there are different tools available to determine the scope of information affected and the extent of the attack. For incidents in 2015 in which a forensic firm was used, the most common types of investigation were (1) imaging devices and conducting manual review and (2) review of available logs. We did see a growth in the use of endpoint tools to look for indicators of compromise across large and multiple physical location environments as the primary investigative method.

Self-Detection on the Rise

A key first step to an effective response is detection. Historically, most companies did not self-detect—they were notified by a third party. Mandiant’s 2015 M-Trends Report showed that 31% of the matters Mandiant worked on in 2014 were self-detected. However, the firm’s 2016 M-Trends Report showed a meaningful improvement in self-detection to 52%. Our findings are consistent. In 2015, 52% of the incidents we worked on were self-detected. Self-detection was even higher for healthcare entities, at 59%.

Self-Detection Improving



52%

Self-Detected

48%

Notified by Third Party

Detection Through Notification

The core of the incident response lifecycle is detection, containment, analysis, and notification. One of the first issues a company must consider is how fast notification should occur. Before a company is positioned to provide a meaningful notification, it needs time to stop the attack, determine who is affected, identify any appropriate measures to prevent a reoccurrence, and mitigate potential harm to affected individuals. Very rarely is this possible within days or even a few weeks. To help identify realistic expectations on timing of notification, we looked at four timing metrics:



Detection

The time from when an incident first began until it was detected ranged from 0 to over 400 days. The overall average time to detect was 69 days and the median was 15 days. For the subset of matters involving an unauthorized person who gained access to a network, the average time to detect was 106 days and the median was 55 days.

Average amount of time from incident occurrence until discovery



HEALTHCARE

114
days

NON-HEALTHCARE

46
days



Containment

The average time from detection until containment was 7 days. A prerequisite to building an effective containment plan is learning enough about the attacker's capabilities and method(s) of access to the environment. This is where we see one factor making a big difference—a company's ability to get a forensic firm engaged and provide the firm with forensic data and visibility into the environment. Companies that have already identified the firm they will work with, that already have an MSA in place, and that conducted scenario planning together usually reach containment faster and with less impact to business operations. Other companies that fared better were ones that had detailed, lengthy, and centralized logging. And companies that used forensic firms with tools that enabled the firm to look quickly for indicators of compromise across many endpoints also often reached containment faster. Those companies for which the findings came from only imaging devices had slower containment.

Average amount of time from discovery until containment



Analysis

All companies are eager to complete the forensic investigation to determine the scope of an incident. On average, it took 43 days to complete forensic investigations.

Average amount of time from engagement of forensics until forensic investigation complete





Notification

The average time from discovery until notification was 40 days.

Average amount of time from discovery until notification



HEALTHCARE
39 days
NON-HEALTHCARE
40 days

Average number of individuals notified when notification was provided

ALL MATTERS
269,710
HEALTHCARE
163,000
NON-HEALTHCARE
355,341

Notifications provided (by mail or substitute notice) and lawsuits filed

NOTIFICATIONS
146
LAWSUITS FILED
9

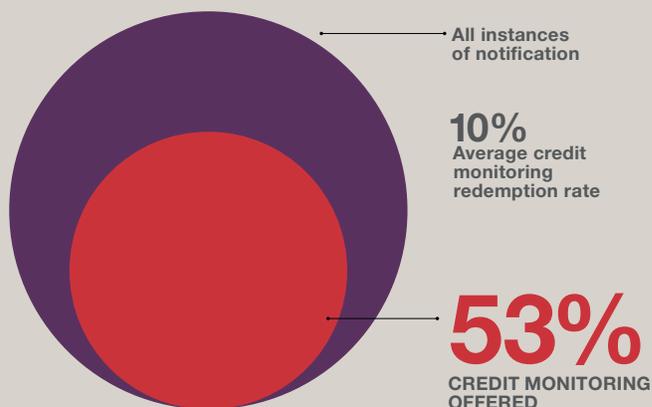
Beware of Paper Records

Although most security breach notification laws focus on incidents affecting electronic data, a number of state and federal laws impose notification requirements when an incident concerns hard-copy records that contain personal information. Paper records were involved in 13% of our 2015 incidents (an additional 2% were both paper and electronic). Paper records incidents were more common among our healthcare incidents, at 25%, due in large part to HIPAA requirements. Our advice from last year remains true—don't forget about paper when addressing information governance and incident response preparation.

Tailoring Offerings to Data at Risk

Many assume that notification and an offer of credit monitoring go hand-in-hand. However, only one state law requires an offer of credit monitoring, and that law only applies when Social Security numbers are at risk. Companies should tailor an offering, if one is made, to prevent the potential harm that could arise from the misuse of the data at risk. For example, credit monitoring products monitor credit profiles for signs of newly created accounts, but they do not monitor open payment card accounts for fraudulent charges, so credit monitoring is not designed to mitigate the theft of payment card data. There are, however, fraud resolution services, as well as services that will monitor the "dark web" for signs that stolen data is being sold. Last year, credit monitoring was offered 53% of the time that our clients provided notification. When offered, the average redemption rate was 10%.

Credit Monitoring Stats



The Incident Is Public— Now What

Not every incident results in notification to individuals or public awareness. Approximately 40% of the incidents we investigated last year did not require notification. Two of the most common reasons notification was not required were (1) because the information at risk did not meet the definition of “personal information” and (2) a forensic investigation determined that there was no unauthorized access or acquisition of personal information. This highlights the importance of engaging experienced incident response attorneys (often referred to as “privacy counsel” or a “breach coach”) and skilled forensic investigators.

Entities that publicly disclose an incident, by notifying either affected individuals or the media, are always concerned that litigation or regulatory action is inevitable. However, neither of those outcomes is certain. Regulatory investigations or inquiries occurred just 24% of the time, down from 31% last year. Litigation is even less likely—lawsuits were filed only 6% of the time.



Healthcare Investigations

The Department of Health and Human Services Office for Civil Rights (OCR) initiated an investigation of our clients 57% of the time *within the year* that the incident was report to HHS where the incident involved more than 500 individuals. Our experience demonstrates that OCR eventually investigates 100% of all incidents involving more than 500 individuals (there may be a lag time of months or even years following the initial report). Additionally, in some instances, if a business associate caused the incident, the covered entity may or may not be investigated.

For incidents involving fewer than 500 individuals, an investigation is commenced infrequently and is usually driven by a patient/member complaint.

Of the more than 100 OCR investigations we have helped clients defend, only two have resulted in finalized resolution agreements,

to date. We have negotiated the amounts and terms of the resolution agreements to tailor the corrective action plan to the client’s circumstances and reflect the continuous improvements the clients have made since the incident. We have even convinced OCR to withdraw a settlement demand.

Healthcare organizations should not underestimate the importance of their response during an investigation, and work with experienced outside counsel just as the organization does when litigation arises. Too many organizations focus solely on notification requirements during the incident response. It is critical to embark on a parallel track of preparing to respond to an OCR investigation by undertaking corrective action that may justify closing an investigation quickly. This approach may also help mitigate the amount of a fine or penalty that can be assessed.

After an incident is reported, regulators most often ask to review:

- Documentation of the incident response, investigation, mitigation, notification of individuals, substitute notice, and media notice provided
- Copies of policies and procedures governing privacy and security
- Evidence of education and awareness training programs, including attendance logs
- Sanctions policy and evidence of disciplinary action taken
- Security risk analysis conducted by the organization over a several-year period preceding the incident
- Risk mitigation plans developed as a result of the risk analyses
- Vendor/business associate agreements in place, regardless of whether a vendor caused the incident, and including internal business associate agreements with corporate entities
- Evidence of corrective action taken

Regulatory Investigations

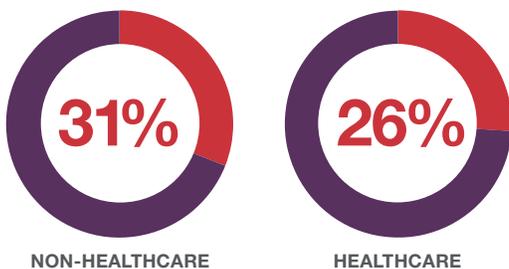
Regulatory scrutiny of data security practices continues. Of the matters we helped to manage, attorneys general were notified in 61 cases and they made inquiries 16% of the time. A multistate inquiry was initiated about 6% of the time, marginally up from 5% in 2014.

How Often Do AGs Inquire?

When notification was provided to state attorneys general pursuant to state breach notification laws, state attorneys general inquired about 31% of non-healthcare incidents reported. For incidents that involved PHI, state attorneys general made further inquiries about 26% of the incidents reported.

Some state attorneys general are more active than others. For example, one state's attorney general almost always requests that the reporting party provide a timeline of the specific steps taken in response to an incident when the notification is made more than 30 days after it was discovered. In anticipation of these types of regulatory inquiries, companies should maintain a detailed timeline of their investigation and response activities. Often it is not enough to just know what the text of the law states; you must also understand enforcement priorities.

How often an AG inquired after notifications were made



A Merchant's Largest Financial Exposure?

Merchants that have "card present" 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 amount of incremental fraud that occurred on the stolen cards. Because they are rule-based, the PCI DSS non-compliance fines range from \$5,000 to \$50,000. The range of the initial demand for operating expense and fraud assessments broadened this year to \$7-\$65 per at-risk card (compared with \$3-\$25 per card in 2014). The median assessment was \$30 per card, and the median number of total at-risk cards was 125,000. The primary variable in the assessments is the amount of fraud. For smaller incidents, a greater percentage of at-risk cards are vulnerable to fraudulent purchases. Thus, incidents with fewer than 500,000 at-risk cards generally have a wider range and tend to result in the highest per-card amounts. Incidents from 500,000 to 2 million at-risk accounts are often in the \$5-\$10 per-card range, and larger incidents usually approach the \$3-\$5 per-card range.

The per-card range of the initial demand for operating expense and fraud



The Post-Incident Consequence We Did Not Measure

One of the most underestimated and least discussed post-incident impacts comes from disruption and loss of productivity. For significant incidents, key personnel may spend some or all of the business day (or more) on incident response tasks for several months. Their day jobs either get done at night, are delegated, or are delayed. After the continuous intensity of the initial response dwindles, members of the incident response team still face completion of remedial measures, regulatory investigations, defense of lawsuits, insurance recoveries, and financial reporting. The impact on productivity caused by an incident can easily last a year or longer.

How to Be a Compromise Ready Company

8 Components of being compromise ready

- 1 Preventative and detective security capabilities
- 2 Threat information gathering
- 3 Personnel awareness and training
- 4 Proactive security assessments focusing on identifying the location of critical assets and data and implementing reasonable safeguards and detection capabilities around them
- 5 Assessing and overseeing vendors
- 6 Developing, updating, and practicing incident response plans
- 7 Understanding current and emerging regulatory hot buttons
- 8 Evaluating cyber liability insurance

3 Areas where companies can most improve

- 1 Detect incidents sooner
- 2 Contain them faster after detection
- 3 Keep good logs to facilitate a more precise determination of what occurred before the attack was stopped

In general, after an attacker gains an initial foothold in a network, there is a period of internal reconnaissance when the attacker works to learn about the network so the attacker can escalate privileges, move laterally, and complete the attack mission.

Preventative Measures

Obviously, accepting that incidents are inevitable does not mean it is not worth trying to stop them. Companies still need to use preventative technologies to build the proverbial moat around their castle. It is imperative that companies protect their systems and comply with any applicable security requirements—statutory, contractual, or formal/informal precedent—from enforcement actions by their regulators.

Stop the Attack Earlier

The goal of implementing detective capabilities as part of a defense-in-depth strategy is to find and stop the attack at the earlier phases of the “cyber kill chain,” before the attacker reaches sensitive data. This approach goes beyond trying to prevent attacks with firewalls and antivirus software to incorporate endpoint monitoring and a SIEM to aggregate logs. Companies are signing retainer agreements with security firms that will conduct investigations when incidents are detected. A good use of the annual retainer hours is onboarding activities—helping the security firm understand the company’s environment, looking at logging practices, ensuring logs contain what a forensic firm will need to conduct an investigation, and understanding the deployment process of endpoint monitoring.

Recognize the Limits of Technology

The right technological safeguards may prove sufficient to prevent many attacks. But when companies find a way to stop one attack vector, attackers do not give up and look for a new line of work. Rather, they are repeatedly observed finding ways around technological barriers. Most security firms will tell you that a capable attacker will eventually find a way in. Why? Most networks are built, maintained, and used by people, and those people are both fallible (e.g., able to be phished) and subject to a range of constraints (e.g., budgets, production priorities). Companies should assume that even if they install the most advanced technology solutions and receive certain security certifications, their security measures may fail and an unauthorized person may gain access to their environment.

The Critical Nature of Your Incident Response Plan

That reality drives the next two areas of preparedness: (1) implementing detective capabilities (e.g., logging and endpoint monitoring tools and procedures) so that unauthorized access is detected quickly, and (2) developing and practicing a flexible incident response plan. Two key parts of incident response planning are identifying the companies you will work with to respond and then building those relationships before an incident arises.

Companies do not always get the luxury of having 30 days to investigate, determine who may be affected, and then mail letters. Spending a few days just negotiating and executing a master services agreement and a statement of work with a forensic firm so that the forensic firm can begin to investigate can make the difference between meeting or missing a 30-day disclosure deadline.

Conduct a Tabletop Exercise That Reflects Reality

Companies can use the Law & Order approach to building a tabletop exercise—read disclosures from other companies and the security firm reports that detail the incidents they investigate. It is often beneficial to have the law firm, forensic firm, and crisis communications firm that will work with you during the incident participate in developing and leading the exercises. An experienced incident responder leading the exercise will be able to provide helpful context during the exercise.

Many poor decisions are made during incident response, and an experienced incident responder can help avoid making mistakes. For example, the CISO may state that he or she will identify, contain, and fully investigate a significant incident in a few days when experience shows it will likely take much longer. Or the communications team may want to make notification no later than seven days after discovery or include a statement that the company is implementing “state-of-the-art security measures” to make sure an incident never happens again. Again, experience and our data show that this approach to communications is not prudent. Without experience at the company’s side, the company may fall into the same traps that have hurt other companies.

What Next If Forensic Findings Are Inconclusive?

One of the most difficult decisions a company faces during an incident response occurs when the forensic findings are inconclusive. Typically, this happens because there is not sufficient forensic data available to determine what occurred. Unfortunately, this is common. Companies often find themselves confronted with findings that show an attacker gained access to the network and had the capability to access and acquire sensitive data, but the investigation screeches to a halt at that point.

For example, a forensic firm may discover that an attacker gained access to a company’s network six months ago, installed tools, and then used the tools to connect to a database server. But beyond stating that the attacker had the capability to query and exfiltrate the results, the firm cannot determine whether the attacker’s queries failed, returned one row of data, or accessed the contents of the entire database. The company then has to turn to secondary indicators to attempt to infer the likelihood of unauthorized acquisition—are customers reporting fraud or misuse, or did law enforcement provide the initial notice because of intelligence they obtained? Lack of forensic data can occur for many reasons—

Being able to show precisely what was accessed during the attack usually results in notification to a smaller group of individuals about fewer at-risk data elements.

because the attack began long enough ago that logs have been overwritten, because logging was not configured to capture the necessary details or was not enabled at all, or because the attacker used anti-forensic techniques to destroy forensic artifacts, some of the most common being s-delete and time stomping.

Beware of Over-Notification

Because state breach notification laws are consumer protection laws, a company may choose to notify out of an abundance of caution. This usually results in over-notification. In many investigations for which there is adequate forensic data, the findings usually show that the amount of data at risk is less than it would be in the worst-case scenario. If you read breach notification press releases, it is not uncommon for companies to state that the attack affected only a percentage of their locations or involved only certain data elements. Surprisingly, being able to show precisely what was accessed during the attack usually results in notification to a smaller group of individuals about fewer at-risk data elements. Knowing with greater certainty what was at risk and having the ability to show that certain data elements were not affected often play key parts in a company’s dialogue with regulators and customers, and provide defenses in enforcement actions and lawsuits.

Theodore J. Kobus
*Leader, Privacy & Data
Protection Team*
New York
tkobus@bakerlaw.com
212.271.1504

William R. Daugherty
Houston
wdaugherty@bakerlaw.com
713.646.1321

Randal L. Gainer
Seattle
rgainer@bakerlaw.com
206.332.1381

Melinda L. McLellan
New York
mmclellan@bakerlaw.com
212.589.4679

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

Patrick H. Haggerty
Cincinnati
phaggerty@bakerlaw.com
513.929.3412

Eric A. Packel
Philadelphia
epackel@bakerlaw.com
215.564.3031

Tanya Forsheit
Los Angeles
tforsheit@bakerlaw.com
310.442.8831

Craig Hoffman
Cincinnati
cahoffman@bakerlaw.com
513.929.3491

Lynn Sessions
Houston
lsessions@bakerlaw.com
713.646.1352

Alan L. Friel
Los Angeles
afriel@bakerlaw.com
310.442.8860

M. Scott Koller
Los Angeles
mskoller@bakerlaw.com
310.979.8427

Paulette M. Thomas
Cincinnati
pmthomas@bakerlaw.com
513.929.3483

BakerHostetler

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

www.bakerlaw.com

© 2016 BakerHostetler®