Be Compromise Ready: Go Back to the Basics

2017 Data Security Incident Response Report
Contents

01 Incident Response Trends
04 Companies and Industries
06 Why Incidents Occur
07 Ransomware
08 Importance of Forensics
10 Detection through Notification
12 State Attorney General Activity
14 How to Minimize Risks—Back to Basics
18 Data Security Litigation Trends
24 GDPR
We started analyzing data collected from the hundreds of security incidents we manage annually to provide a resource for businesses to help focus their time and budgets in the right places. Clients have used our reports to prioritize and gain executive support for their security spending, educate their board and executive leadership team, fine-tune their incident response plans, vet and select forensic firms, build scenarios for tabletop exercises, and determine the type of cyber liability insurance needed. Our third year of reporting takes a look at the more than 450 incidents we worked on in 2016.

Use this Report as a “crowdsourced” tool for identifying risks, response metrics and risk mitigation investment priorities.

The overarching takeaway is that companies need to continue focusing on the basics to become and remain “Compromise Ready.”

No one is immune. All entities face cyber risks because they have data that can be monetized or because they rely on technology to operate their business.

Operational resiliency. Theft of data is not the only risk. Ransomware and IoT-fueled DDoS attacks can shut down operations.

The people problem. Awareness and training help, but networks are built, maintained and used by people. People will continue to make mistakes and be phished or socially engineered.

Practice. Having an incident response plan is a good first step, but ongoing testing through tabletop exercises is better.

Response metrics. The time from incident occurrence to detection and from detection to containment show where improvement can be made. Identifying a forensic firm and onboarding that firm before an incident occurs is a primary way to improve.

Choose carefully. Not all forensic firms are created equal—vet them by experience, tools they use (e.g., image and analysis or endpoint agents) and approach.

Let the forensics drive the decision-making. Investigations take more than 40 days to complete, and what you know in the beginning is often incomplete or wrong. Unless you fall outside the normal range, timing of disclosure of an incident rarely is the sole source of a post-incident financial consequence.

Biggest consequences? Poor communications cause rifts in relationships with customers, stakeholders and employees. Although companies focus heavily on regulatory investigations and litigation, it is not a foregone conclusion that these will occur.
Incident Response Trends

Causes

- **43%** Phishing/Hacking/ Malware
- **32%** Employee Action/ Mistake
- **18%** Lost/Stolen Device or Records
- **25%** of these involved phishing
- **23%** of these involved ransomware
- **4%** Other Criminal Acts
- **3%** Internal Theft

10% of all incidents involved ransomware

Incident Response Timeline

- **61 DAYS** Occurrence to discovery
- **8 DAYS** Discovery to containment
- **40 DAYS** Engagement of forensics until forensic investigation complete
- **41 DAYS** Discovery to notification

OCCURRENCE | DISCOVERY | NOTIFICATION

CONTAINMENT | FORENSIC INVESTIGATION COMPLETE
Industries Affected

- 35% Healthcare
- 16% Finance & Insurance
- 14% Education
- 13% Retail/Restaurant/Hospitality
- 9% Other
- 8% Business & Professional Services
- 5% Government

Company Size by Revenue

- 39% <$100M
- 33% $100–$500M
- 17% $500M–$1B
- 11% >$1B

Breach Discovery

- 64% INTERNALLY DISCOVERED
- 36% EXTERNALLY DISCOVERED

Forensic Investigation Cost

- $62,290
- $257,602 (Average of 20 most costly investigations)

Notifications vs. Lawsuits Filed

- 257 NOTIFICATIONS
- 9 LAWSUITS FILED

How Often an AG Inquired After Notifications Were Made

- 29%
Our 2016 data continues to show what most have now accepted—no industry is immune from data security incidents. All industries are faced with the task of managing dynamic data security risks. The risk landscape is changing, but due only in part to increased sophistication of some attackers. Risk profiles change as organizations adopt new technologies, use existing technologies in novel ways, collect and share more data, and increasingly rely on vendors to conduct business. As the risks become more challenging, there continues to be heightened regulatory and public scrutiny of data security practices.

For the second year in a row, the three industries that took the most frequent number of hits were healthcare, finance and insurance, and education.

The retail/restaurant/hospitality industry was right behind education. These industries were more impacted and yet operate under some of the most rigorous data security regulations. This highlights the obstacles all companies face in data security.

Companies of all sizes were impacted in 2016. The frequency of incidents had little correlation with the size of the company. Indeed, the frequency with which the largest and smallest companies were affected was similar, with 28% involving companies with more than $500 million in revenue and 39% involving companies with less than $100 million. There appears to be a lot of opportunity for cyber insurance in small and middle markets.

The frequency of healthcare breaches continues to rise—up from 23% in 2015 to 35% in 2016. The increase appears to be attributable to the increase in ransomware attacks and the associated Office for Civil Rights guidance. Although the average size of healthcare incidents decreased from 2015 to 2016, the 2015 data included several incidents that affected tens of millions of people. However, three 2016 incidents are included in the top 10 list of largest HIPAA breaches ever reported. Another factor contributing to a lower average is that ransomware attacks typically do not involve a large patient population.
### Frequency
Percentage of Incidents by Industry

<table>
<thead>
<tr>
<th>Industry</th>
<th>Frequency</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>HEALTHCARE</td>
<td>35%</td>
<td>61K</td>
</tr>
<tr>
<td>FINANCE &amp; INSURANCE</td>
<td>16%</td>
<td>7K</td>
</tr>
<tr>
<td>EDUCATION</td>
<td>14%</td>
<td>4K</td>
</tr>
<tr>
<td>RETAIL/RESTAURANT/HOSPITALITY</td>
<td>13%</td>
<td>297K</td>
</tr>
<tr>
<td>OTHER</td>
<td>9%</td>
<td>5K</td>
</tr>
<tr>
<td>BUSINESS &amp; PROFESSIONAL SERVICES</td>
<td>8%</td>
<td>8K</td>
</tr>
<tr>
<td>GOVERNMENT</td>
<td>5%</td>
<td>134K</td>
</tr>
</tbody>
</table>

More frequent incidents but not always as large

Most were payment card incidents

More frequent incidents but not always as large
Why Do Incidents Occur?

Network Intrusion and Data Theft

We combine phishing/hacking/malware in one category because they are often used in tandem. For example, opening an attachment to a phishing email often installs malware that facilitates initial access to the network.

Approximately 22% of all incidents were due to computer network intrusions and malware. These incidents involved individuals or groups finding a way to gain unauthorized access to clients’ computer networks, conducting reconnaissance across the networks to identify valuable data and then attempting to exfiltrate the data. The attackers targeted payment card data in 38% of these attacks and health information in 20%.

Our clients notified individuals of the incident in 65 of the 104 (62%) network penetration intrusion and malware attacks. This shows that not all network intrusions result in notification. Each incident needs to be thoroughly investigated.

The number of individuals notified in all incidents we worked on ranged from one person to over 8 million. The average number of persons notified when a network intrusion occurred was three times higher than the average for all incidents.

It took an average of 41 days after the discovery of a network penetration intrusion and malware incident to mail notifications. That is a quick response time, considering that it took the forensic investigators an additional eight days to complete their investigations. Although that is quick, there are state laws with a 30-day notice obligation.

There is a 72-hour deadline in the New York Department of Financial Services’ cybersecurity rules and a similar deadline in the European Union’s new General Data Protection Regulation (the GDPR). Panic or early over-notification is not the answer. Working with experienced counsel is beneficial because there are proactive steps that can be taken to provide timely notice in a way that is designed to avoid a regulatory nightmare.

Phishing/hacking/malware kept the No. 1 spot, accounting for about 43% of incidents. Non-healthcare entities accounted for 69% of these incidents, and healthcare entities accounted for 31%.

Causes
- Phishing/Hacking/Malware
- Employee Action/Mistake
- Lost/Stolen Device or Records
- Other Criminal Acts
- Internal Theft
- Unknown

HEALTHCARE

OVERALL

3% Internal Theft
4% Other Criminal Acts
18% Lost/Stolen Device or Records
32% Employee Action/Mistake

FINANCE & INSURANCE

1% 4%
11% 18%
27%

RETAIL/RESTAURANT/ HOSPITALITY

9% 12%
14%

23% of these involved ransomware
25% of these involved phishing

Employees are often cited as a company’s greatest asset. In the cybersecurity arena, they can also be a liability. While these numbers reinforce the ongoing need to focus on effective employee awareness and training, they also show that a defense-in-depth approach is necessary because even the best-trained employees can make mistakes or be tricked.
Ransomware Frequency and Variety on the Rise

While ransomware has existed in one form or another since 1989, the past two years have seen a tremendous increase in the frequency and variety of attacks. Researchers have noted up to 500% year-over-year increases in ransomware incidents. Our clients have had similar experiences. In 2016, we responded to 45 ransomware incidents. For clients that do not have backups available and that do not have a funded Bitcoin wallet, these incidents create operational resiliency issues. Bitcoin was the form of payment that was demanded in almost all of these incidents. But making the ransom payment doesn’t guarantee a quick return to normal operations—after payment was made and the encryption key was provided, sometimes the data could not be fully restored.

Client Responses to Ransomware

Our clients’ experience reflects the varying challenges and unknowns that ransomware presents. On one end of the spectrum are attacks by sophisticated parties that break into the network and then broadly deploy ransomware to hundreds of devices, while others are carried out by rookies who bought a ransomware kit.

Ransomware demands ranged from a few hundred dollars to several thousands of dollars. We saw several demands in excess of $25,000, and almost all demands were for payment in Bitcoin. It took several days for companies that did not have a Bitcoin wallet to create and fund their wallet to make the ransom payment.

After dealing with recovering access to the data, clients then have to assess whether the incident triggered any notification obligations, especially after the July 2016 Office of Civil Rights (OCR) guidance. Steps in this analysis include (1) identifying the variant of ransomware used (i.e., does it just encrypt files, or does it provide the ransomware operator with access to the files?) and (2) determining what host and network logs exist to provide information about what occurred.

There may not be any one measure that can guarantee a successful defense against ransomware. If your preventive measures fail, the choice is usually between using available backups to quickly restore the system or paying the ransom. And if backups are not available or they were stored on the affected system, paying the ransom is often the only choice.

Ransomware Is Not Going Away

We expect ransomware incidents to continue to rise because of:

- Critical reliance on technology and data for operating the entity, and poor backup practices;
- New iterations of ransomware that are affecting mobile and Internet of Things (IoT) devices (these might include, for example, hotel key locks, home security and network devices, and even refrigerators);
- Low cost to enter the market as an entry-level cybercriminal employing ransomware; and
- New business-oriented ransomware models that the more sophisticated cybercriminal enterprises are investing in
  - Developing new strains of ransomware
  - Supporting existing infrastructure for payment processing
  - Engaging in customer service (May I help you with your decryption key?)
  - Data mining (If a victim suffers this intrusion, might they be susceptible to a future one? If a victim becomes a paying customer, are they more likely to pay in the future?)

Why Network Attacks Succeed

<table>
<thead>
<tr>
<th>51%</th>
<th>15%</th>
<th>9%</th>
</tr>
</thead>
<tbody>
<tr>
<td>technical security failures</td>
<td>vendor wrongdoing</td>
<td>employee wrongdoing</td>
</tr>
</tbody>
</table>

These incidents are criminal attacks. The same Russian-based attack group, referred to as “Fin5” by FireEye’s Mandiant unit, was identified as being responsible for five of the 10 largest network intrusion incidents we helped clients address in 2016.
Forensics Proves Invaluable

Detection is a critical first step. A fast and efficient investigation that provides information necessary to implement an effective containment plan and assess notification obligations is the next major step. Companies that are prepared for the containment phase have taken these critical steps:

1. Identified the primary forensic firm they will use, and negotiated a service relationship.
2. Conducted onboarding work with that firm.
3. Collected good log data accessible from a centralized source.

Companies that have good forensic data available are often able to better determine whether notification is appropriate. When good forensic data is not available, and because most breach notification laws implicate consumer protection statutes, companies often choose to err on the side of caution and assume the worst case occurred. Contrary to what many people think, this is not proving the negative. Depending on the applicable law, the company must assess whether there are sufficient facts to support a position that something did or did not happen. Working with an experienced and confident privacy/data security lawyer is critical to help support the company through this process. Additionally, having good and reliable forensic data makes a critical difference. It will help you craft better communications about what happened and help reduce negative consequences that can result from disclosing incidents.

A forensic investigation occurred in 34% of the incidents we worked on in 2016. Healthcare entities used forensic investigations at a higher rate this year, probably due to the rise in ransomware incidents and the OCR guidance related to ransomware. A forensic investigation occurred in 27% of the incidents involving healthcare entities in 2016—versus only 13% in 2015.

The average total cost of a forensic investigation in 2016 was $62,290, with the highest cost in excess of $750,000. The overall average cost of forensics appears to have dropped between 2015 and 2016. We attribute the drop to the increase in ransomware investigations, which are not as costly as other types of network intrusions.

Forensic firms use a variety of tools to determine the scope of information affected and the extent of the incident. But the tool that often leads to the quickest identification of a potential issue is an endpoint agent. For incidents in 2016 in which a forensic firm was used, the most common type of investigation was imaging devices and log review. We saw a substantial increase in the use of endpoint tools to look for indicators of compromise. When these tools are used depends on the type of investigation. Log review is typically carried out when a company is trying to determine whether exfiltration of data occurred, when and how data in a database was accessed, or how and when remote access credentials were used.

Device imaging is most common when servers and desktops are being evaluated for malware and other forensic artifacts. And endpoint tools are used to review numerous devices (such as desktops, laptops and point-of-sale devices) for both historical and current activity. Before a forensic firm deploys an endpoint tool, it is important for the client to fully understand how it operates. In some cases, the tool can conflict with critical company applications. Not all endpoint tools are created equal—some provide only a snapshot of what is happening once deployed (e.g., what programs are currently running), and others look back in time and are able to provide insight about what happened prior to the tool being installed.

It took forensic firms an average of 44 days after they were hired to complete their investigations of network intrusion incidents. The cost for the investigations ranged from several thousand dollars to in excess of $750,000. The average cost of a network intrusion investigation was $93,322.

Investigators found evidence of data exfiltration in 34% of the network intrusion incidents. A failure to find evidence of exfiltration does not always mean that data wasn’t stolen. Some attackers carefully remove evidence of their activities, and in other scenarios there is not sufficient logging.
Data at Risk

Over half of the incidents last year, 55%, involved data subject to U.S. state breach notification statutes, e.g., Social Security Numbers (SSNs), driver’s license numbers, credit card/debit card account information, bank account numbers, usernames/passwords, health information, etc. These numbers are slightly down from 2015, which may be because more and more companies are masking (or partially masking) sensitive information that triggers breach notification laws. Additionally, more companies are employing “minimum necessary” concepts used in HIPAA. Minimum necessary requires the person handling the information to consider whether the information is actually necessary to complete the desired function. For example, does a spreadsheet of employees assigned to a department require inclusion of the SSN?

Self-detection Continues to Rise

Detecting the incident soon after it happens is a critical first step. Last year, we reported that more incidents were being detected by the entity than by third parties. The improvement continued this year. The increase from 52% last year to 64% this year is, in part, due to the number of W-2 phishing incidents, which are usually discovered internally. When isolating the data for network intrusion attacks, we found that those were self-detected 55% of the time. This relatively high number is probably due to more and more companies employing endpoint monitoring, which increases a company’s ability to detect incidents more quickly.

Notification Summary

For incidents in 2016 when notification was made to individuals, the average number of individuals notified was 77,230. For the 10 largest notifications our clients provided, the average number of individuals notified was 2 million.

Out of all the incidents we helped manage in 2016, notification to individuals was made 56% of the time (257 times). This means that in 44% of the incidents, we were able to work with the company to determine that notification was not required.

After companies notified individuals, only a small percentage of incidents—under 5%—actually led to lawsuits being filed. For healthcare matters, notification to individuals was made 56% of the time (91 times), with lawsuits filed in only three incidents.

We believe there are a few reasons for the relatively low number of lawsuits. First, companies are better managing incidents. Communications are more clear and consistent and answer the basic questions that a person affected wants to know: (1) What happened? (2) How did it happen? (3) What are you doing to protect me? (4) What are you doing to stop this from happening in the future? Companies are also proactively providing services to help mitigate the impact. For example, in payment card data security incidents, companies are reimbursing customers for actual losses. And finally, the defense bar is successfully making these claims more difficult for plaintiffs to litigate.
Detection Through Notification

The core of the incident response life cycle is detection, containment, analysis, and notification. One of the first issues many companies ask about 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 initial occurrence to detection continues to be the area where companies have the most room to improve. Faster detection usually means there will be more certainty about what occurred due to better available forensic data. It also aids better mitigation of post-incident consequences. Network intrusions were self-detected 64% of the time. Are you trying to determine how many months of logs to archive to a Security Information and Event Management system (SIEM) so you can look back and determine what occurred if an incident went undetected that long? You may want to increase your storage, because 18% of the incidents involving a network security attack went undetected for more than six months. Six incidents went undetected for more than a year.

Containment

Entities were able to contain incidents within eight days of initial detection. However, network attacks had a longer containment time. For network attacks where the fix was not one simple step, the average containment time was 13 days. Time to containment exceeded 30 days in 16% of these network attacks. Three factors are key to the length of time to containment: (1) an existing relationship with a forensic firm to ensure rapid engagement, (2) quick access to forensic data (e.g., logs from a SIEM, live response data from an endpoint security investigation tool), and (3) effective project management to build and execute the containment plan.

Analysis

While everyone wants answers immediately, forensic investigations take time. The average time to complete an investigation was 40 days, with 26% taking longer than 45 days.

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

- All Matters: 40 days
- Healthcare: 36 days
- Non-Healthcare: 42 days
Tailoring Offerings to Data at Risk

The percentage of individuals redeeming complimentary credit monitoring and identity theft protection after a breach rose from 10% in 2015 to 26% in 2016. This significant increase is primarily attributable to the more than 50 W-2 incidents we responded to in 2016. Employer data security incidents always have a significantly higher rate of uptake of credit monitoring. This is in part due to the “watercooler” effect. We typically recommend offering credit monitoring when SSNs or driver’s licenses are affected. Other data monitoring products are becoming available for non-credit related incidents. The offering of any product should be done only after carefully considering the facts and applicable law. At this point, only one state, Connecticut, specifically requires that one year of credit monitoring be offered when SSNs are involved. Although the redemption rate we are reporting seems high due to the number of W-2 incidents we worked on, our experience in large non-employee data breaches is that redemption rates are generally less than 5%.

Number of Individuals Notified

The average number of individuals notified in 2016 was 77,230, which is down from 269,609 reported in 2015. This drop is primarily due to the high number of W-2 income tax phishing incidents, which typically involve a population of thousands rather than millions of employees.

Notification

The average time from initial awareness of a potential issue (a date that is different than “discovery”) to notification of affected individuals was 41 days. With forensic investigations taking 40 days on average, this means companies are preparing to notify on a parallel track to the forensic investigation to be prepared to notify as close in time as possible to when there is certainty about who may have been affected.

Average amount of time from discovery until notification

<table>
<thead>
<tr>
<th></th>
<th>ALL MATTERS</th>
<th>HEALTHCARE</th>
<th>NON-HEALTHCARE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>41 days</td>
<td>44 days</td>
<td>39 days</td>
</tr>
</tbody>
</table>

More individuals are taking advantage of free credit monitoring services

- **26%** Average credit monitoring redemption rate
- **64%** Credit monitoring offered
Why are attorneys general (AGs) making more inquiries? It appears that some of this may be driven by changes to breach notification laws and reported increased funding to AGs’ offices for investigations. More states are requiring notice to regulators when any individuals in the state are notified of a breach. In states that already had existing regulatory notifications, the AGs are getting more aggressive and asking more questions—in part because they are becoming more knowledgeable after completing so many investigations. As more states publicly report settlements arising from these incidents, and as the federal government throttles back on regulation, it is likely that other states will want to be seen as enforcing consumer rights. Accordingly, incident response is not just about following breach notification laws but also carefully crafting an incident response strategy that takes into account the possibility of a regulatory investigation. States often seek the following information:

- A detailed timeline of the incident (particularly if notification occurred more than 30 days after discovery of the incident).
- A narrative describing the incident.
- Details of how the incident was discovered and the vulnerability that caused the incident.
- Copies of policies/procedures addressing information security (including your written information security plan).
- Safeguards put in place and corrective action taken as a result of the incident.
- Complaints received by affected individuals.
- Details of mitigation efforts for affected individuals, including credit monitoring services.
A Merchant’s Largest Financial Exposure—the Card Network

Merchants that have “card present” payment card data stolen from them or their vendor may face noncompliance 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 Payment Card Industry Data Security Standard (PCI DSS) noncompliance fees may range from $5,000 to $50,000. 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 larger 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 with from 500,000 to 2 million at-risk accounts are often in the $5–$10 per-card range, and larger incidents usually approach the $4–$5 per-card range.

1 Timing? While assessments are often received from one or two networks approximately six months after the final PCI DSS Forensics Investigator (PFI) report is submitted, it usually takes 12 months or more before all network assessments are known.

2 How Much? The range of the initial demand for operating expense and fraud assessments was $1.40 to $36 per at-risk card. The median assessment amount was $15.25 per at-risk account, and the median number of at-risk accounts was 55,460.

3 Fines? When the forensic investigation determines that a merchant was not PCI DSS compliant at the time of the breach, networks may assess noncompliance fees. However, these fees are not always assessed, and last year they ranged from $2,500 to $5,000.

4 Trends? Across three networks, the average amounts per card of the operating expense reimbursement component of the assessments were $2.49, $3.04 and $1.40. The average amounts per card of the fraud reimbursement component of the assessments across two networks were $9.36 and $4.74. Prior year assessment ranges were $3–$25 in 2014 and $3–$65 in 2015. Aside from an outlier in 2015, assessments have been pretty consistent across the tiers of at-risk account scenarios. Two networks have increased the operating expense reimbursement amounts based on issuer concerns, in part related to the cost to issue an EMV card compared with that of a magnetic stripe card.

Beware of Paper Records

While most breach notification laws focus on incidents affecting electronic data, a few state and federal laws (e.g., HIPAA) require notification when an incident involves hard-copy records that contain personal information. Consistent with our report last year, paper records were involved in 13% of our 2016 incidents (an additional 4% involved paper and electronic). Our advice from last year remains the same—don’t forget about paper records when addressing information governance and incident response preparation.

Healthcare Investigations Occur on Multiple Fronts

OCR is commencing investigations slightly more slowly than in prior years. Of the 35 healthcare breaches involving 500 or more individuals we helped clients report, OCR initiated an investigation before the end of 2016 in 13 of those incidents. We still expect OCR to ultimately investigate 100% of all incidents affecting 500 or more individuals. There is a time lag (sometimes more than a year) before OCR sends its first data request. Due to the change in the administration and the onboarding of Tom Price as Health and Human Services secretary and Roger Severino as head of OCR, we may see a slowdown in how quickly investigations commence in 2017.

State AGs are also piling on when it comes to healthcare breaches. State AGs opened investigations 25% of the time in 2016 on matters where we reported incidents to both OCR and AGs. Although it seems like “double-dipping,” state AGs are authorized to enforce HIPAA, as well as their state laws, along with OCR. Healthcare entities can, therefore, face multiple regulatory investigations arising from the same incident. States may attempt to claim that a violation of HIPAA is also a violation of state consumer protection laws. By using the often broad and vague consumer protection laws, some states attempt to assess significant fines.

It is imperative that companies plan their regulatory response approach from the start by focusing on how regulators will view their incident response, including mitigation and remediation efforts.
2016 was a record-breaking year for the number of data security incidents disclosed. And for the first time, an incident reportedly affected 1 billion accounts. Still, the preparation and response landscape has not changed dramatically. Regardless of an entity’s risk profile, there are core steps most should take to mitigate risk and be prepared if an incident is detected. Our experience with responding to security incidents over the past decade reveals several constants to keep in mind:

- Skilled and unskilled attackers are still able to find a way in to networks whether the network has little or “next gen” security.
- Networks are as fallible as the people who build and maintain them. People inside and outside the organization make mistakes, respond to phishing emails and are socially engineered.
- Most incidents are not the result of a sophisticated, never-before-seen, unpreventable, zero-day attack.

The Form 10-K cyber risk disclosures of many public companies state that the company relies on technology to operate its business and a failure of that technology could have a material impact. While most of the security incidents reported in 2016 related to theft of data, the surge of ransomware and emergence of DDoS tools fueled by compromised IoT devices demonstrate that maintaining operational resiliency is as important as preventing data theft. Following are recommended steps to minimize risk of an incident while best positioning the company if one happens.

1 Increase Awareness of Cybersecurity Issues

Training and education on cybersecurity issues are not just important to satisfy regulators but also may very well prevent a costly data security incident from occurring. If employees aren’t aware of threats, they won’t take appropriate action to avoid an incident. Phishing emails continue to be a significant threat that can lead to compromised credentials and the insertion of malware, including ransomware. We recommend both new hires and current employees receive annual training regarding the dangers of phishing emails.

- Focus on what phishing emails look like and what they might ask for.
- Use services that periodically test employees by sending “fake” phishing emails, so employees who respond can receive additional training.
- Alert all employees via training and posted reminders that any requests to send W-2 tax forms or other highly sensitive information to anyone should be confirmed via a telephone call or in person with the person making the request. Never seek confirmation of the request by replying to the email received.
- Make sure all staff is on the lookout for other employees using their cellphone to photograph documents or their computer screen or who are printing out sensitive documents with no reason for doing so.
- To stay on top of new cybersecurity threats and new threat actors, IT staff should consider participating in public and private sector threat information sharing programs, including programs sponsored by the Department of Homeland Security. More information on these programs can be found at [www.dhs.gov/topic/cybersecurity-information-sharing](http://www.dhs.gov/topic/cybersecurity-information-sharing).
Identify and Implement Basic Security Measures

Many data security incidents occur when criminals find a weakness in a company’s internet-facing network and then penetrate the network, conduct reconnaissance to find valuable data, and export the data before they can be detected and stopped. If a company implements basic data security measures, it can make it more difficult for opportunistic criminals to succeed. Companies should consider taking the following steps:

- Implement multifactor authentication to remotely access any part of the company’s network or data, including email platforms such as Outlook Web Access.
- Disable remote desktop protocol on internet-facing systems.
- Segregate subnetworks that contain valuable data from other parts of the network, and require users who need to access such data to use multifactor authentication or one-time passwords to access the subnetworks.
- Implement and monitor a software patch management system that requires critical patches to be installed promptly.
- Require users to use complex passwords and to change them at least every 90 days.
- Remove administrative rights from normal users, and limit the number of accounts with administrative privileges.
- Implement a web proxy that can block access to untrusted websites.
- Utilize threat intelligence and endpoint protection tools that use reputational searches and behavioral patterns.
- Deploy an intrusion detection and prevention system that aggregates logs to a SIEM tool that sends real-time alerts.
- Hire qualified staff or engage a vendor to monitor SIEM and endpoint protection alerts.
- Ensure that all internet-facing and core infrastructure systems and systems that store or have access to sensitive data have logging enabled.
- Retain the logs for at least a year, preferably longer.
- Do not allow employees to access personal email accounts from the company’s network.
- Use security firms to conduct periodic, credentialed vulnerability scans, to help correct vulnerabilities discovered and to conduct periodic penetration tests on internet-facing applications that contain sensitive data or provide access to internal networks.

These security measures may not prevent sophisticated attackers, such as state-supported groups and highly capable cyber criminals, from stealing valuable data. However, they can prevent thefts by more common attackers, and they will position the company better in the event of regulatory investigations or litigation.
Create a Forensic Plan

A company’s ability to quickly and effectively conduct a forensic investigation is critical to limiting the impacts of a data security incident and determining the scope of the incident. More robust forensic data allows the company to more precisely determine the scope of the affected systems and data. This in turn enables the company to build better communications about the incident and to develop and implement a containment strategy to limit the impacts of the compromise. In contrast, delays in conducting the forensic investigation can create numerous challenges for the company, such as providing time for the attackers to conduct anti-forensics tactics to destroy valuable forensic data, forcing the company to err on the side of a more expansive group of impacted individuals and increasing the chances of public awareness about the incident before the company has developed a communications plan. Creating a forensic plan is thus vital to a company’s incident preparedness.

Developing a forensic plan begins with ensuring that the internal IT team has a precise understanding of the company’s environment, which often entails developing and maintaining accurate network diagrams, device inventories and data maps. Companies that lack this understanding lose precious time and resources developing it during incident response. The forensic plan should also address the organization’s internal procedures and tools for collecting forensic evidence to ensure that valuable forensic data is preserved before a system is remediated and put back into production. One of the most important steps is identifying an external forensic firm, negotiating the terms of a master service agreement, and meeting with that firm to discuss how it will investigate and what data is needed to facilitate a faster response, investigation, containment, and final analysis. Meeting with the forensic firm and conducting tabletop exercises together can help ensure that the company is maintaining appropriate logs, collecting and preserving evidence in a forensically sound manner, and able to deploy the forensic tools throughout the company’s environment. Companies that create a forensic plan and work with their external forensic firm in advance are in a far better position to respond quickly and effectively to a data security incident.

Build Business Continuity Into Your Incident Response Plan (IRP)

Cyberattacks and data security incidents can involve the loss of data or the unavailability of servers, computer hard drives, email systems, phone systems, and other hardware. For example, DDoS attacks have targeted computing and network systems, including Voice-over-IP (VoIP) phone systems. Ransomware attacks have targeted files and systems including key health records, human resources and trade secret databases. Business continuity considerations must be built into your IRP. If the affected device supports a critical business function, its unavailability can shut down a business. As you ensure that business continuity is built into your IRP, you can rely on existing business continuity plans, but ensure that you address the following issues:

- Has your organization conducted a business impact analysis that identifies the organization’s most critical systems and impact downtime?
- What are your systems backup procedures, and how often are the full systems backed up?
- Where are the backups held, and how are they stored (e.g., are backups stored locally on each device or a separate device; are there off-network copies)?
- How long is backup media maintained, and how quickly can you access the backups when needed?
- Once accessed, what are the procedures for restoring systems and testing systems to ensure they are functioning properly?

The next step is to test business continuity during your full-scale tabletop exercises.
Manage Your Vendors

Every company uses vendors, and a significant percentage of data security incidents are vendor related. It is critical to understand who your vendors are and how they work with your company. Technical capability, reputation and financial solvency are important. However, there are other considerations:

• Do you fully understand their information security practices?
• Do they have an incident response plan, and will they share it with you?
• Do you really understand what information is being provided to them and by whom?
• Are certain company contacts giving them too much information and not following “minimum necessary” principles?
• Are you ensuring that vendor contracts include key provisions such as confidentiality, limitation on usage and transfer of data to only specified purposes, and information disposal upon project completion (return or destroy)?
• Are you signing HIPAA business associate agreements when you aren’t a business associate or covered entity under HIPAA?
• Are you agreeing or invoking laws that really do not apply to either contracting party?
• Are you setting standards that may be reasonable on the date that the contract is signed, but are outdated soon after execution?
• How are you auditing or monitoring your vendors?
• Are you employing self-questionnaires, or are third parties being engaged?

The answers to these questions will vary from company to company depending on the type of vendor being engaged and for what purpose. The key is to focus on the individual relationship and ensure that you understand what data is being shared, how it is being secured and whether you will lose control when something goes wrong.

Prepare for Ransomware

Ransomware has quickly grown to be one of the most prevalent threats facing organizations today. And yet prior planning and preparation can greatly reduce its potential impact. Since ransomware primarily targets your data, the best defense is a full and complete backup. The use of off-site or air-gapped backups is critical because newer ransomware is specifically targeting those backup systems. Also consider incorporating ransomware scenarios into your incident response training to help identify potential deficiencies in your restoration procedures. Companies are also starting to realize that even with complete backups, the system downtime is a greater threat. Therefore, enterprising organizations are creating Bitcoin wallets in advance and pre-funding them to minimize potential downtime if critical data is impacted. For mission-critical systems and data, we have seen an increase in the use of “hot sites,” where redundant systems provide immediate coverage if a ransomware infection occurs.

Purchase the Right Cyber Insurance Policy

Cyber insurance has become more than just a mechanism to offset the costs of breach response, regulatory investigations and litigation. It is critical to work with a knowledgeable insurance broker to find the policy right for your company. As you decide which insurance policy is right for you, consider the following:

• Is business interruption insurance appropriate for your business, and will it cover the types of losses that may be unique to your company or industry?
• Is the carrier established, and does it have a history of helping its insureds better manage large breaches?
• Does the carrier have risk management services that will help you better prepare the company and its employees?
• Which vendors are available or preapproved under the policy, and are those vendors you should work with?
• Is voluntary notification coverage by the policy?
• If a contractual agreement covers your need to notify, will the carrier cover that type of notification?
• Will the policy limits be sufficient to cover a catastrophic breach, or will they be exhausted and leave you bare in a third-party action?
• Is an excess policy something the company should consider?
AT A GLANCE

Data Security Litigation Trends

Industries Impacted by Data Breach Litigation

- **64%**: Healthcare
- **12%**: Supermarket Business
- **12%**: Hotel & Restaurant
- **8%**: Pharmacy & Retail
- **4%**: Education

Type of Data Breach

- **64%**: Network Intrusion
- **24%**: Lost or Stolen Computers
- **8%**: Phishing
- **4%**: Unauthorized Employee Access
### Targeted Data

- **52%** involved health information
- **36%** involved payment card data
- **32%** involved SSNs

Some cases involved multiple types of data, so there is overlap reflected in these figures.

### Causes of Action

- **92%** NEGLIGENCE
- **56%** BREACH OF CONTRACT
- **56%** VIOLATIONS OF STATE CONSUMER LAWS
- **36%** VIOLATIONS OF STATE DATA BREACH NOTICE STATUTES
- **32%** STATE PRIVACY STATUTES

### Injuries Claimed

- **80%** POTENTIAL IDENTITY THEFT
- **72%** ACTUAL FINANCIAL HARM
- **44%** ACTUAL IDENTITY THEFT
- **36%** OVERPAYMENT FOR SERVICES/UNJUST ENRICHMENT
- **32%** LOSS OF INHERENT VALUE OF INFORMATION
Standing Still at the Heart of Class Action Litigation (But for How Long?)

Standing to sue continues to be one of the most prevalent issues in privacy litigation. The most common reason data breach lawsuits have been dismissed for lack of standing is because the party who filed the lawsuit hasn’t yet suffered any injury and is exposed only to the possibility of a future injury. Standing is required under Article III of the United States Constitution.

Given the increasingly varying opinions in the lower courts on standing issues, there was great interest in the U.S. Supreme Court’s decision in Spokeo v. Robins, which was decided in May 2016. Spokeo did not resolve the split in the Federal Circuits on the question of future injury, but it did address another important standing question: whether a plaintiff can sue under a federal law that provides for statutory damages of a specified amount even if the plaintiff cannot show that he or she was harmed by the statutory violation. The Supreme Court answered this question by recognizing that an alleged injury has to be sufficiently “concrete” to give rise to standing to sue in the federal courts. While merely alleging that a defendant violated a procedural requirement of federal law is not sufficient to satisfy the concreteness standard by itself, the Court recognized that certain abstract harms, such as the deprivation of a constitutional right, can still qualify as “concrete,” so the plaintiff doesn’t necessarily have to show a physical injury or financial loss. The key, according to the Court, is whether the plaintiff can show that he or she suffered harm, even an abstract one, for which Congress intended to provide a remedy. What exactly this “concreteness” standard means in cases involving particular federal laws is going to be argued in the lower courts. Even in the Spokeo case, the Court declined to determine whether the harms alleged (reporting false information to a credit reporting agency that actually improved the plaintiff’s credit score) qualified as “concrete”, remanding the case to allow the lower courts to address that issue.

Because more data breach class actions have been surviving early standing challenges, more data breach class actions are now moving forward to the class certification phase. Up to this point, very few data breach class actions have reached this stage, with two notable exceptions being In re Hannaford Bros. Co. Customer Data Security Breach Litigation, in which the court denied a motion to certify a class of consumers who had used their credit or debit cards at Hannaford grocery stores, and In re Target Corporation Customer Data Security Breach Litigation, in which the court granted certification of a class of banks and other financial institutions that claimed damages arising out of Target’s payment card system breach. Several high-profile healthcare class actions are scheduled for briefing and hearings on motion for class certification over the next few months, so class certification is an issue to look out for in 2017.
The Federal Circuit courts have been busy evaluating the limits of Article III standing, and the rulings have not been in agreement.

Recent decisions by the Sixth, Seventh and Ninth Circuit Courts of Appeals found that the likelihood of future identity theft can be enough to support standing, at least in some circumstances.

By contrast, recent decisions by federal district courts in the Fourth, Fifth, Eighth and Eleventh Circuits took the opposite stance, applying a more exacting standard for what plaintiffs must provide to establish standing based on a future injury.
Privacy Litigation: Developing a Defense Strategy

Because the Article III standing requirements for data breach litigation remain in a state of flux, there are a variety of strategic questions that a defendant should consider in developing its early defense strategy. Here are some examples.

How does the jurisdiction view standing?

In jurisdictions that apply a more lenient standard, it may be better to focus on the fact that a failure to allege a present injury also results in many causes of action to fail on their merits, since injury, causation and damages are common elements of many common law claims and many consumer protection laws.

Has the plaintiff suffered identity theft, fraud or other harm?

A defendant may be able to convince a court that the allegations aren’t enough to show a fraud is “fairly traceable” to the data breach incident, but many courts tend to apply a more lenient view of the “fairly traceable” standing element, especially at the beginning of a case. But in cases where some of the plaintiffs allege fraud and others do not, an effective strategy can be to seek dismissal of just those plaintiffs who do not claim any present harm. While a ruling on that motion may not resolve the entire case, it will lay the groundwork for a successful defense to a class certification motion later in the case, since the vast majority of absent class members will usually be more similar to those plaintiffs who can rely only on the possibility of a future injury.

What happens if the case is dismissed?

If all the plaintiffs are dismissed for lack of standing, then the federal case will go away. Standing is a jurisdictional issue, however, and the dismissal will be without prejudice. This means that it may be possible for the plaintiffs to file the same case in state court, which may not be subject to the same standing requirements that apply in the federal courts. In fact, this hollow victory may permit unsuccessful plaintiffs to pursue their claims on the merits in a more favorable state court forum.

In short, defendants should consider a variety of factors and weigh the pros and cons that may come out of making an early challenge to standing and plan accordingly.
Diminished Value of Personal Information and Invasion of Privacy

Plaintiffs often argue that data breaches cause injury under the theory that a plaintiff’s confidential information has monetary value, as evidenced by criminals’ willingness to pay for the information on the black market. But most courts have not bought that argument.

Plaintiffs also often argue that data breaches cause them to suffer an invasion of privacy. Most courts have rejected this theory outside the context of a breach followed by public dissemination or publication of the data. Courts have generally held that absent other allegations of injury, an alleged loss of privacy is “too abstract” to be a compensable harm. Most common law or statutory rights to privacy also require some intentional, affirmative disclosure of information on the part of the defendant. Plaintiffs are rarely able to prove intent in cases involving hacking or theft of computer equipment.

Plaintiffs Try New Angles in Data Breach Cases

Plaintiffs in at least 12 data security incident cases that we defended last year have alleged some variant of unjust enrichment. The general premise is that plaintiffs have overpaid for whatever it is they are purchasing because a portion of what they pay should go to data security measures. Some courts have rejected these claims at the motion to dismiss level. Why? Plaintiffs generally fail to prove what portions of what they paid were allocated for data security or exceeded the value of what they received. Other courts have denied motions to dismiss these claims, treating unjust enrichment as a catchall claim.

Breach of contract claims are common in data breach class actions. Last year, we defended companies in 14 data security incident cases where plaintiffs alleged breach of contract. Plaintiffs have attempted to repurpose privacy notices into a contract. However, many courts have found that notices and policy statements are insufficient to create a binding contract. Most lack the basic elements of a contract, including an offer, acceptance, consideration and sufficient specification of the essential terms. Courts have also found that a promise to pay for something that a party is already under a legal duty to do, such as provide security for individuals’ medical records under HIPAA, is not a binding contract because it lacks consideration. However, some courts do still allow these contract claims to survive a motion to dismiss.

FILED MOTIONS TO DISMISS

On average, it took approximately 303 days from the time a complaint was filed to the time the court ruled on a motion to dismiss.

53% GRANTED IN PART

33% GRANTED
EU Ramps Up Security Incident Response Rules

The enactment of the EU General Data Protection Regulation (the GDPR) represents the most significant change in European data protection law in more than 20 years. The GDPR goes into effect May 25, 2018.

The GDPR’s breach notification requirement to supervisory authorities and affected individuals in the EU is a critical aspect of the new rules. Article 33 of the GDPR provides that data controllers must notify the competent supervisory authority of a personal data breach “without undue delay and, where feasible, not later than 72 hours after having become aware of it.” A data controller’s notification to the competent supervisory authority must (1) describe the nature of the breach (including the types and numbers of individuals affected as well as how many data records were implicated), (2) include contact information for the organization’s Data Protection Officer (the DPO), (3) detail the likely consequences of the breach, and (4) list remediation and mitigation steps the organization has taken or will take in response.

Per Article 34, if the personal data breach “is likely to result in a high risk to the rights and freedoms of individuals,” the controller must also inform affected individuals without undue delay. Such notification must be “in clear and plain language.” Notification to individuals may not be required if the data controller (1) had implemented appropriate measures to protect the personal data so that it would be “unintelligible” to unauthorized parties (e.g., through encryption), (2) took subsequent steps to ensure that risks to individuals are not likely to materialize, or (3) individual notification would require disproportionate effort. If so, the organization would need to issue a public communication to inform data subjects of the breach.

As part of the notification requirements, data controllers are to document the breach response process, including discovery, investigation, notification, effects and remediation efforts. This documentation may be requested by the DPA to verify a company’s compliance with the GDPR’s personal data breach notification requirements. Companies that already have robust incident response policies and procedures in place may need only to update those materials to incorporate the new EU requirements. Organizations that do not have detailed data breach response plans should implement appropriate policies and procedures now to be fully ready when the new rules go into effect.