BakerHostetler

2018 DATA SECURITY INCIDENT RESPONSE REPORT

Building Cyber Resilience

Compromise Response Intelligence in Action

Key Findings

MFA is the gold standard. Much like encryption of external devices several years ago, multifactor authentication (MFA) has become an essential security measure and is increasingly becoming a regulatory expectation. However, MFA is not infallible, and not all MFA solutions are equally secure.

It's not the cloud, it's you. As entities migrate to the cloud, most security issues are not caused by the cloud service provider, but by how the entity or its service provider configures access to the cloud.

Rise of the regulator. Recent high-profile incidents have rekindled regulatory interest. And large multistate settlements have given state attorneys general the funds to hire experts and more aggressively investigate breaches.

New year, same issues. Entities still are not executing on the basics. Endpoint monitoring agents, security information and event management (SIEM) solutions, and privileged account management tools have become more common, but good hygiene could have prevented many incidents.

Everyone's involved. With incidents on the rise and the stakes higher than ever, senior management, boards, and external auditors are becoming involved in data breach prevention and response.

No one is "too small." Any entity, of any size, may become the victim of a cyber-attack. Hackers are happy to hit "singles" and take advantage of the lax security practices of small and medium-sized entities, and attacker techniques and tools simplify the process of finding even obscure targets of opportunity.

GDPR countdown drives uncertainty. With the May 25, 2018 effective date looming, entities have been racing the clock to get their privacy, data security and incident response practices in order. Expect adjustments to continue as the regulation is implemented.

Reading the litigation tea leaves is an inexact science. The line determining cognizable damages continues to blur. In addition, recent cases show that privilege may not apply to all incident-related communications, and that some entities choose to waive privilege.

CONTENTS

This is our fourth Report addressing the issues entities care about most when it comes to incident response. The Report's focus remains consistent with that of prior years, although this year we emphasize the importance of using Compromise Response Intelligence in addition to the measures necessary to be Compromise Ready.

2017 was another record-setting year for data security incidents. Attack groups continued to exploit vulnerabilities to gain access to valuable data, phishing remained prevalent and successful, and employees and their vendors made common mistakes that placed sensitive information at risk. But despite attackers' old tactics continuing to work, we saw them also develop new and innovative attacks, including those against supply chains and Internet of Things (IoT) devices. As regulator scrutiny increases and new international breach notification laws take effect, more entities will struggle with these issues globally.

560+
Incidents in 2017

While all incidents cannot be prevented, there are measures entities can take to minimize their attack surface and reduce the frequency and severity of incidents. Equally important, given the increase in attacks intended to disrupt operations, is a focus on building cyber resilience for an agile response. It can be hard to know where to begin, especially in an environment of constant change – but taking steps to proactively address these issues is what we call being Compromise Ready.

Our goal in publishing this Report is to offer practical steps you can take to reduce your risk profile, build resilience, and be better prepared to respond when an incident occurs. The data and experience behind the recommendations come from our work on more than 560 incidents in 2017 and more than 2,000 others in years past. Just as security teams use threat intelligence to prevent attacks, we hope you will use the Compromise Response Intelligence from this Report to prioritize and gain executive support for security spending, educate key stakeholders, fine-tune incident response plans, work more efficiently with forensic firms, assess and reduce risk, build scenarios for tabletop exercises, and determine cyber liability insurance needs.

Please continue to reach out and let us know what information you would find most useful in future reports.

Sincerely,

Ted Kobus
Leader, Privacy and Data Protection Team

Incident Response Trends

Top 5 Causes

34% Phishing

- **32%** Involved Remote Access
- **18%** Involved Ransomware

19% Network Intrusion

- **38%** Involved Ransomware
- **17%** Involved Automated Data Exfiltration

17% Inadvertent Disclosure

11% Stolen/Lost Device or Records

6% System Misconfiguration

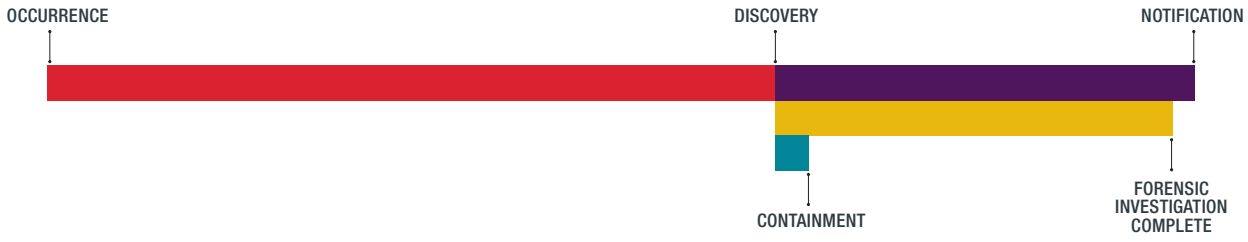
Incident Response Timeline

66 Days
Occurrence to Discovery

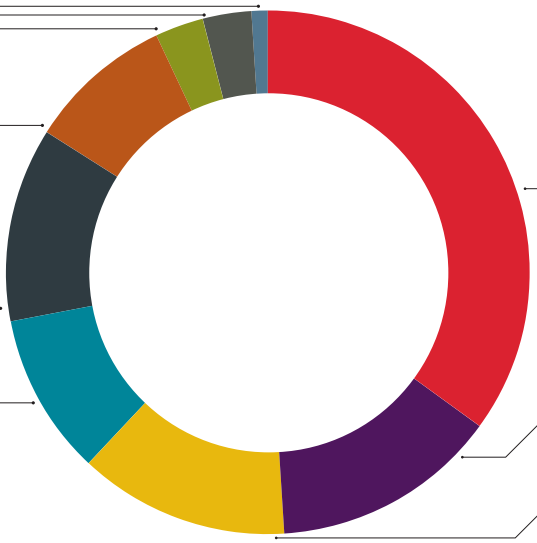
3 Days
Discovery to Containment

36 Days
Time to Complete Forensic Investigation

38 Days
Discovery to Notification

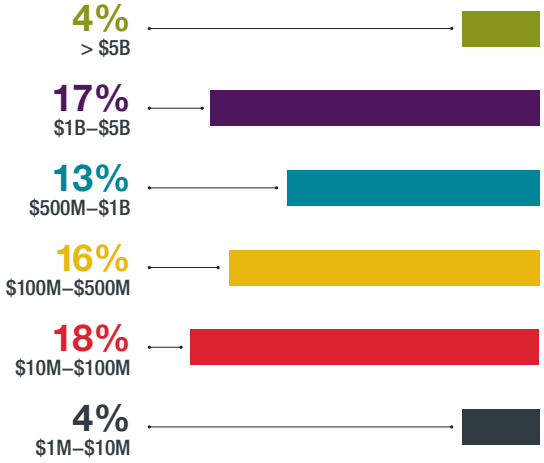


Industries Affected



- **1%** Nonprofit
- **3%** Aerospace & Defense
- **3%** Government
- **9%** Finance & Insurance
- **10%** Other
- **12%** **Hospitality** (including Retail, Food & Beverage, Media & Entertainment)
- **35%** Healthcare
- **14%** Education
- **13%** **Business & Professional Services** (including IT, Legal, Engineering, and Transportation)

Entity Size by Revenue



- **4%** > $5B
- **17%** $1B–$5B
- **13%** $500M–$1B
- **16%** $100M–$500M
- **18%** $10M–$100M
- **4%** $1M–$10M

Breach Discovery

65% Internally Discovered

35% Externally Discovered

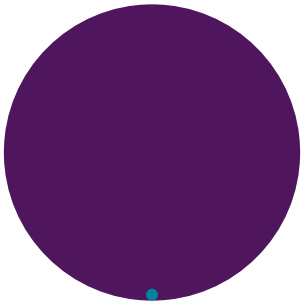
Average Forensic Investigation Costs

$84,417
All Incidents

$436,938
20 Largest Investigations

100%
Increase Over Last Year

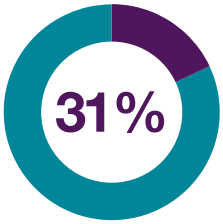
Notifications vs. Lawsuits Filed



350
Notifications

10
Lawsuits Filed

AG Inquiries Following Notification



Non-AG Inquiries

2016	2017
29	43

Why Incidents Occur

Phishing and Exploitation of Vulnerable Systems Top the List

Over one-third (34%) of the incidents we responded to began when an employee was phished – tricked by an email message into providing access credentials to an unauthorized party, visiting a phony website, downloading an infected document, or clicking on a link that installed malware. Both sophisticated and unsophisticated hackers use phishing to obtain direct network access, convince employees to wire money, enable remote access with compromised credentials, or deploy malware and ransomware. These incidents can be costly and difficult to investigate.

Exploitation of vulnerable systems to gain network access was the second-most frequent tactic used by attackers to obtain initial access, accounting for 19% of the total. After gaining access, deployment of ransomware was the most likely next occurrence.

Ransomware Attacks Continue
Ransomware attacks continued to grab the spotlight with their frequency, occasionally dramatic demands for payment, and headline-ready names like WannaCry. Increasingly, the more traditional ransomware incidents occurred through poorly configured Remote Desktop Protocol services – which are susceptible to default-password guessing or brute-force attacks – rather than traditional phishing links. The attacker remains undetected while conducting reconnaissance and can launch a more devastating attack by encrypting critical data (and, in some instances, deleting backup files). In many cases, victims successfully restore data without paying a ransom, thanks to increasingly maintaining robust off-site backups.

Cloud Misconfigurations: A Growing Trend
System misconfiguration is a new category we tracked this year to reflect the growing number of incidents where unauthorized individuals gain access to cloud instances and storage devices because permissions are set to "public" instead of "private." Often the unauthorized persons are "security researchers" who will contact the media regarding what they were able to access. These incidents accounted for 6% of the total.

As the value of bitcoins rose, so did the number of crypto-miner attacks, when hackers install malware that uses the victim entity's computer resources to mine bitcoins or other cryptocurrencies for the attacker.

Phishing for Mail Access

As entities continued moving to cloud-based email systems like Office 365 without enabling MFA, we saw a surge in phishing incidents targeting Office 365 login credentials. Often multiple employees, sometimes 20 or more, were phished at the same time, giving the attacker access to all the compromised accounts. The default log settings for most Office 365 instances are not granular enough to show which emails and data an attacker accessed, complicating notification determinations. To address this concern, several forensics firms have developed custom scripts to extract logs with sufficient detail to support notification determinations. Some entities experienced multiple incidents before enabling MFA.

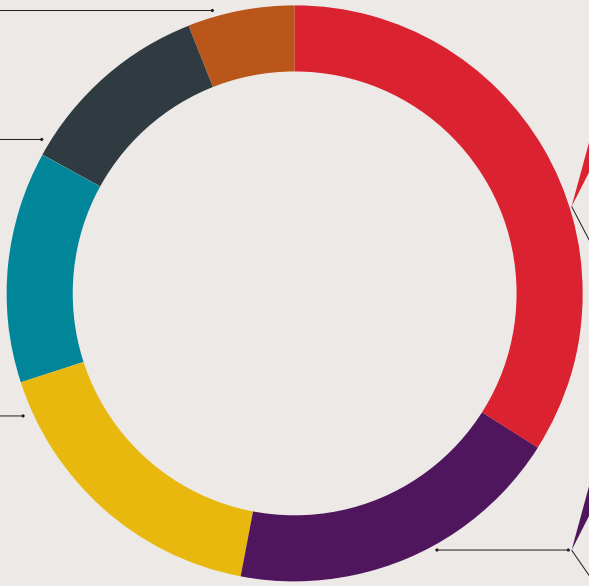
One tactic used by attackers to avoid detection was so common that it is worth a special note. After compromising a user's mail account and using the target's account to send fraudulent emails (in furtherance of a wire fraud scam, W-2 theft or some other fraud), an attacker will typically add mailbox rules to ensure that replies to the imposter emails are forwarded to the attacker and deleted from the mailbox, preventing the real user from seeing replies to the imposter's emails. Thus, merely changing passwords is not enough to contain an incident. Entities must search for and deactivate unauthorized rules changes immediately upon learning of an incident. **Important: Do not delete these rules – they must be preserved for forensic investigation.**

Take Action: Close the Employee Loophole

The number of phishing incidents, inadvertent disclosures, and cloud misconfigurations shows that employees and third-party vendors continue to cause incidents. Effective training can reduce the frequency and severity of these incidents. Because people are fallible, training is not enough and technological safety nets are needed. For incident prevention, a strong training and technology mix includes:

- **Phishing training, including test phishing campaigns, to increase awareness.**
- **Educating employees to not provide login credentials or use the same credentials for multiple sites or services.**
- **Enabling MFA throughout the entity.**
- **Deploying endpoint security agents and advanced email threat protection tools.**
- **Developing effective network segmentation.**

Overall



6% System Misconfiguration

11% Stolen/Lost Device or Records

13% Other

17% Inadvertent Disclosure

Phishing Breakdown

34% Phishing

- **32%** Remote Access
- **24%** Other
- **20%** W-2 Scam
- **18%** Ransomware
- **6%** Automated Information Exfiltration

Network Intrusion Breakdown

19% Network Intrusion

- **38%** Ransomware
- **29%** Other
- **17%** Automated Information Exfiltration
- **16%** Remote Access

Responsible Party

53%
Employees (includes employee error such as mistakenly providing information in a phishing scam)

31%
Unrelated Third Parties
(e.g., security researchers)

16%
Vendors/Service Providers

Breach Discovery

65%
of Breaches Internally Discovered

35%
of Breaches Externally Discovered

Ransomware

$40,000
Average Payment

100% relied on vendor when payment in bitcoins requested

Timeline Provides Context for Response Expectations

When an incident occurs, entities often want to notify regulators and affected individuals as quickly as possible. However, it is critical to first take the time to contain the attack. The forensic, legal and in-house team will then work to determine who is affected, identify measures to prevent a reoccurrence, and mitigate potential harm. To help you set realistic expectations, we looked at the timing of the incident response life cycle's core elements: detection, containment, analysis, and notification.

Network Intrusion Timeline
Network intrusions tend to take longer to detect and contain than other types of attacks, because multiple steps are involved. However, the timeline follows the overall pattern of other types of attacks. More than 90% of all network intrusions were detected in less than six months and contained in less than a week. More than half of all forensic investigations were completed within a month, with only 4% taking longer than three months.

Overall Incident Response Time

Detection

The time from initial occurrence to detection continues to be where entities have the most room to improve. Earlier detection usually means more forensic data is available, which leads to more effective mitigation efforts and more certainty about what occurred. Good logging and visibility are also critical.

Entities are more aware than ever of the importance of constant vigilance. Of the data breaches in this year's survey, 65% were detected internally. Only 8% remained undetected for more than six months, and only 4% for more than a year.

Occurrence to Discovery

NETWORK INTRUSION
84 Days

Containment

Ending the attack is critical to reducing exposure, and incident response teams continue to find faster containment strategies. Time to containment was less than a week in 97% of incidents; only 2% took more than a month to contain. Key factors in time to containment are as follows: (1) an existing relationship with a forensic firm, (2) quick access to forensic data such as logging and endpoint information, and (3) effective project management to build and execute the containment plan.

Discovery to Containment

HEALTHCARE
1 Day

NETWORK INTRUSION
5 Days

Number of Individuals Notified

AVERAGE:

87,952

Notifications by Industry

Hospitality (Food/Beverage, Retail)	627,723
Education	46,783
Business & Professional Services	8,284
Healthcare	6,470
Finance & Insurance	3,572
Other	2,729
Nonprofit	957
Government	927
Aerospace & Defense	275

Take Action: Keys to Shortening the Timeline

- **Increase SIEM log storage to look back at incidents.**
- **Identify a forensic firm in advance, and conduct onboarding to speed the process later.**
- **Use endpoint security tools to get visibility faster.**
- **Be mindful that the pressure to move quickly must be balanced with the need for a complete, thorough investigation and effective containment.**

Analysis

Forensic analysis is getting faster and more sophisticated, with new tools and increased personnel. This year's analysis period was shorter than last year's, with 55% of investigations completed in less than one month and 87% in less than two. Only 4% of investigations took more than three months from start to finish. Despite the understandable desire for speed, it is important to let the forensics process run its full course to determine the actual scope of the incident. Entities that rush or skip this important step and simply assume the worst-case scenario run the risk of making a broader notification than is necessary or appropriate.

Engagement of Forensics to Completion

HEALTHCARE
29 Days

NETWORK INTRUSION
36 Days

Notification

With local, national, and internet media continuing to make data breaches headline news, entities feel increased pressure to make notifications quickly. In response, notification times dropped in 2017. As in the past, entities are preparing to notify as close in time as possible to when a complete forensic investigation reveals who may have been affected.

Discovery to Notification

HEALTHCARE
43 Days

NETWORK INTRUSION
45 Days

Forensics Drive Key Decisions

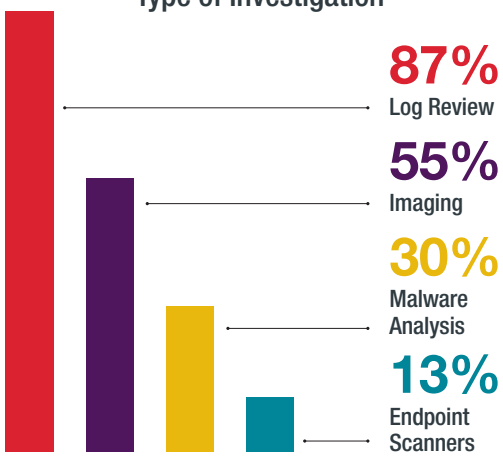
In the first days after an intrusion is discovered, the ability to quickly and efficiently conduct a forensic investigation is critical. A focused forensic investigation can help you answer the essential questions: What happened? How did it happen? How do we contain it? Whom do we need to tell? How can we protect affected individuals? Getting fast, accurate answers is especially important when the compromised data includes personal information that may trigger a reporting requirement.

In 2017, forensics were used in 41% of intrusion incidents overall, compared with 34% in 2016, showing that entities are realizing the value of hiring outside investigators with broad experience and resources. Forensics were used in 65% of network intrusion incidents, probably due to the inherent complexity of those investigations.

Forensic investigators use a variety of tools to determine the scope of information affected and the extent of the incident. Depending on the situation, they may analyze information from an entire network, a specific application, or a particular computer, mobile device, or other endpoint. In 2017, the most frequently used tool was log review, which enables the investigator to reconstruct how data was accessed and to determine whether it was exfiltrated. It can tell you who clicked on a phishing link, and how effective your defenses are. Log review was used in 87% of forensics investigations this year, probably due to the increase in Office 365 incidents involving attackers gaining access to different accounts. This trend further demonstrates how critical it is for entities to collect and retain robust logs in both on-premises and cloud environments.

Device imaging, used in 55% of investigations in 2017, helps evaluate servers and databases for malware and other forensics artifacts. Malware analysis, used 30% of the time, looks at the specific types of malware – where they came from, how they work, and whom they may impact. And endpoint scanners, which review activity in desktops, laptops, and point-of-sale devices, were used in only 13% of investigations, down from 28% in 2016.

Type of Investigation



Forensic Investigation Costs

$84,417
for All Incidents

$86,751
for Network Intrusion Incidents

$436,938
for 20 Largest Investigations

Use of Outside Forensics

65%
of Network Intrusion Incidents

41.5%
of Data Breach Incidents

36
Days
Average Completion Time for Forensic Investigation

24%
Evidence of Data Exfiltration in Network Intrusion Incidents

Data at Risk*

46% Social Security

39% Health Information

26% Other Confidential Information such as student ID numbers, usernames and passwords, and intellectual property

24% Birthdate

15% Financial Data

12% PCI Data

10% Driver's License

** These amounts total more than 100% because many incidents involved multiple types of data.*

Latest Trends in Forensics

Forensic investigators have been creative in developing tools that respond to new types of attacks. For example, faced with a huge jump in Office 365 intrusions, some firms have developed tools that can determine which emails were opened and which objects the attacker accessed. This information can significantly limit the scope of review, as well as the number of required notifications.

Investigating in the Cloud

Although forensic techniques and principles are generally the same in cloud investigations, cloud environments raise some special challenges. In a Software as a Service (SaaS) environment, the vendor – not the entity – controls the underlying infrastructure, including logging. Because logs are so often critical to investigations, make sure to understand a vendor's log detail, obligations, and preservation practices well in advance of an incident.

An Infrastructure as a Service (IaaS) arrangement moves some or all of an entire entity's infrastructure into a cloud environment. Forensic investigators typically cannot connect to physical machines to collect images and data. Instead, they must have processes in place to collect and analyze data in cloud environments. Some forensic firms have overcome this challenge by creating their own virtual systems with forensic tools in the cloud, which they use to connect to and analyze client storage devices.

Take Action: Choose the Right Forensic Firm

In considering whether to hire an outside forensic firm or deciding between possible firms, consider the 3Cs:

- **Capability:** What tools does the outside firm use to conduct investigations? Will its tools work in your environment? Can it quickly provide visibility to endpoints, capture network traffic, and search for current indicators of compromise? Or will it want to forensically image all devices and conduct manual analysis?
- **Capacity:** What's their – and your – bandwidth? Will the firm have a competent team available when you call? Do you have enough resources to deploy the tools, support the investigation, and carry out containment and remediation actions while still doing your day job?
- **Credibility:** Will stakeholders (e.g., regulators, customers, board members, shareholders) expect you to have engaged an external firm? And will they have confidence in the forensic firm's findings? Does the firm have experience responding to the types of incidents you are likely to face?

Even if you have preselected a forensic firm, when an incident arises you should take a close look at whether that firm is best-suited for the particular investigation. Some investigations call for a firm that can tell you exactly what attackers did within your environment. Others require specialized knowledge of a particular application or system. Consult with experienced counsel and your cyber carrier to leverage their experience – their Compromise Response Intelligence – with the options you are considering.

Regulators More Involved

In the wake of several recent high-profile incidents, regulators are taking a more aggressive role in investigating data breaches. We are seeing increases in both the number of inquiries and the speed with which the inquiries are made. No longer confined to a few active state attorneys general (AGs), investigations may be opened by any AG whose state's residents are affected. Additionally, although the number of resolution agreements has dropped, the Office for Civil Rights (OCR) continues to heavily investigate HIPAA (Health Insurance Portability and Accountability Act) compliance following breaches affecting more than 500 people, and more quickly than in years past.

Higher Budgets, Higher Stakes
Regulatory investigations are no longer just informal inquiries that seek voluntary cooperation. More and more, we are seeing agencies issue subpoena-like civil investigative demands (CIDs) that require significant effort to respond.

State AGs and other regulators, well-funded by large multistate settlements, are combining their power to compel testimony and documents with more experts to help them dive deeper into your operations than ever before. CIDs and informal letters now request not only your entity's information security plan and remediation steps, but also more burdensome technical requests, including details about your environment and its physical, technical, and administrative controls. OCR in particular has added instructions to its data requests that may change existing assumptions about how long and in what format an entity must hold and preserve data.

Outcomes of these inquiries often go well beyond the incident itself. While settlement proposals often contain a monitoring component and a corrective action plan, regulators are also beginning to issue closing letters. These letters do not support enforcement action, but contain certain findings and require the entity to acknowledge that it must comply with all statutory obligations. OCR can use this acknowledgment against the entity in a future incident. Similarly, after a complaint investigation or compliance review, OCR may negotiate a resolution agreement requiring an entity to take corrective action to comply with HIPAA. These can be far-reaching agreements that call for a systemic change in the way a state operates, or they may cover a single healthcare provider or hospital.

Size Doesn't Matter
AGs are looking beyond the number of affected residents to explore an entity's "systemic issues." Those that are slow to investigate, are slow to notify and experience repeat data incidents may be especially vulnerable.

AG Inquiries Following Notifications

2016	2017
37	64

Non-AG Inquiries

2016	2017
29	43

OCR Inquiries Where Notice in a Healthcare Incident Exceeded 500

2016	2017
13	22

What an AG Wants


Incident Response Plan


Employee Training Manual


Policies and Procedures


Forensic Reports


Information on Specific Data Loss Prevention


Information on Use of MFAs

Technology Helps Protect Payment Cards

Adoption of EMV technology is making it harder to use stolen card data, and point-to-point encryption use is reducing the number of large card-present theft incidents. When they do occur, because Visa and Mastercard raised the operating expense reimbursement rates across all card types, the baseline expectation for the combined network liability assessment (recovery of operating expense and counterfeit fraud) increases. On average, the lowest expectation starts at $4 per at-risk account. The per card assessment amount can climb to $20 or more based on the amount of fraud that issuing banks report. Generally, larger incidents will be on the low end of the range because the percentage of cards with attributable fraud will be lower than small incidents where the attacker may be able to sell a larger percentage of the cards on a forum. American Express changed its Data Security Operating Policy (DSOP), so when it decides its DSOP applies the opening demand from American Express will be $5 per at-risk account.

As experts predicted, EMV adoption has caused attackers to more frequently target e-commerce sites, and we saw a resurgence in these attacks. Even if a site uses tokenization, an attacker with access to the site's administrative console or checkout-page code can bypass tokenization and capture payment card data. Liability assessment programs apply to these incidents now too.

EU Update: Preparing for GDPR Notification Requirements

The EU's General Data Protection Regulation (GDPR), effective May 25, 2018, addresses personal data breach notification in Article 33 (notifying authorities) and Article 34 (notifying individuals). The harm threshold for notifying regulators is lower than the threshold for notifying individuals – notification to authorities should occur within 72 hours after the entity has "become aware" of a personal data breach that is likely to result in a "risk to the rights and freedoms of natural persons." By contrast, notification to individual data subjects must occur when the breach is likely to result in a high risk to the rights and freedoms of natural persons. In both cases, the risk analysis must broadly consider the confidentiality, integrity, and availability of data.

Because the GDPR's definitions of "personal data" and "personal data breach" are broader than those in the United States, a notifiable breach may be triggered by different incidents. For example, unauthorized disclosure of a list of names and addresses with religious affiliations and church attendance frequency might be perceived as threatening to the rights and freedoms of EU data subjects, but would not trigger a U.S. notification requirement.

Multinationals must plan to manage incidents that affect multiple jurisdictions, as notification under one regulatory regime could create legal risk in another. For example, providing notice to an EU regulator within the 72-hour window could prompt questions about notification timing in the United States. Incident response plans should designate a single decision-maker or a central team to manage potential conflicts. Our incident response tabletop exercises for global entities help their distributed teams take a collaborative and consistent approach to managing multijurisdictional events.

2017 Per Card Assessment Range for Operating Expense and Fraud

$4-$20

Credit Monitoring Offered When Notification Occurred

60%

Average Redemption

35%

Take Action: Manage Regulatory Risk

- **Have a response plan and team in place and practice.**
- **Investigate incidents expeditiously and notify as soon as possible, ideally within 30 days of discovering the incident.**
- **Communicate a culture of transparency and compliance when responding to regulatory inquiries.**

Prepare for Privilege Challenges

Motions to dismiss can still help defendants reduce exposure and limit the scope of discovery. In 2017, courts appeared to favor dismissing specific causes of action while allowing others to proceed. For example, in *In re: Banner Health Data Breach Litigation*, an Arizona federal court dismissed breach of contract, good faith and implied duty of care claims, but allowed others to move forward.

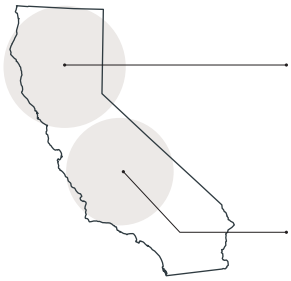
Data breach litigation is surviving motions to dismiss and proceeding to discovery, where plaintiffs seek breach investigation records and challenge defendants' assertions that the investigations are protected by various legal privileges. In 2017, three courts ruled on these challenges, with different results.

California Protects Forensics Documents

In a case involving a health insurance entity, a federal court in the Northern District of California held that the attorney work-product doctrine protected documents sent by a forensics vendor to its client. The key issue was whether the vendor created the documents in "anticipation of litigation." Although some documents had been created both to assist in litigation and to help the entity respond to the suspected incident, the court held that the "litigation purpose permeate[d] the documents" and warranted protection.

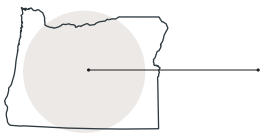
The United States District Court for the Central District of California reached a similar conclusion in a case involving a major consumer credit reporting agency. The plaintiffs argued that the forensic report and related documents were not protected by the attorney work-product doctrine because the company "had independent business duties to investigate data breaches and it hired [forensics vendor] Mandiant to do exactly that ..." But the court found that the company's duty to perform the work did not remove work-product protection. Instead, the court used a Ninth Circuit standard to analyze whether the documents were created "because of" litigation or the threat thereof. In ruling that the privilege applied, the court noted that (1) Mandiant was hired by a law firm to help it provide legal advice in anticipation of litigation; (2) Mandiant provided its report to the law firm, not to the entity; and (3) the form and content of Mandiant's report were largely dictated by the law firm's instructions.

Are Forensic Documents Protected From Discovery?



Northern District of California
Work-product protection exists for documents created in anticipation of litigation, even when they also serve another purpose.

Central District of California
Work-product protection exists for documents created because of litigation or the threat of litigation, despite independent business duty to investigate.



District of Oregon
There is no protection for documents not prepared by or sent to counsel, documents relating to third-party work, or communications with parties not involved in the breach.

Oregon Limits the Privilege

The United States District Court for the District of Oregon reached a different conclusion. That court required the defendant to show that each document it intended to withhold was specifically "legal advice." However, the facts of that case were unique. In October 2014, the entity had proactively engaged Mandiant to conduct a forensic investigation independent of counsel, and the court scrutinized the timing and scope of that engagement in its ruling.

The court focused on the requirement for the business entity to prepare most of the documents in response to the data breach (such as press releases and customer notices) regardless of the litigation. It said the entity's intention to have an attorney review the documents, and the possibility that attorneys advised on the drafting "[do] not make every internal draft and every internal communication relating to those documents privileged and immune from discovery." To maintain the privilege, the entity had to show that the communications were sent to or from counsel seeking or providing legal advice.

Take Action: Build the Paper Trail

- **Certain work performed during incident investigation and response serves a business purpose and therefore may not be privileged. Consider the timing and language of your vendor engagements and scope of work letters.**
- **Where vendors will have dual purposes, one of which is to assist counsel in litigation, use additional engagement letters or scope of work agreements to make that purpose clear.**
- **Assume communications with PR and crisis management firms are not privileged. Act and write accordingly.**
- **Consult with the litigation team early to develop a privilege strategy for confidential communications.**
- **Remember that privilege fights happen months or years after a communication is created. Develop a labeling strategy for privileged documents and emails that will streamline litigation review.**

Use Compromise Response Intelligence to Minimize Risk

Any entity, of any size, may find itself the victim of a cyberattack. Criminal organizations and security researchers constantly scan the internet for vulnerabilities and poorly configured systems. If your systems and data are exposed to the internet, it's only a matter of time before an attacker will target you.

While new threats continue to appear, the incident preparation and response landscape has not changed dramatically from prior years. Our recommendations from previous years still hold true, and we have added some new ones to reflect developing threats and updated strategies.

PREVIOUS RECOMMENDATIONS ARE STILL CRITICAL

1 Increase awareness of cybersecurity issues.

In particular, employees must receive training and education on the dangers of phishing emails and what they look like.

2 Identify and implement basic security measures.

- Segregate subnetworks that contain sensitive and valuable data from other parts of the network.
- Disable or harden remote desktop access on internet-facing systems.
- Ensure that patch management procedures are in place and critical patches are installed in a timely manner.
- Remove administrative rights from normal users, and limit the number of privileged accounts.
- Implement a web proxy that can block access to untrusted websites.
- Utilize threat intelligence and endpoint protection tools.
- Deploy endpoint monitoring and an intrusion detection and prevention system.
- Aggregate logs from critical sources into an SIEM tool, and configure properly tuned, real-time alerts.
- Retain logs for at least one year, preferably longer.
- Prohibit access to personal email accounts from the entity's network.

3 Create a forensics plan.

You can't protect what you don't understand. Create and maintain accurate network diagrams, device inventories, and data maps to ensure that the internal IT team knows your entity's environment. The plan should also address internal procedures and tools for collecting and preserving forensic evidence, and identify pre-vetted forensic firms and those for which a master service agreement is in place.

4 Build business continuity into your incident response plan.

With ever-growing ransomware and distributed denial of service (DDoS) attacks, business continuity should be built into your incident response plan and tested.

5 Manage your vendors.

Vendor incidents are still occurring. It is critical to know your vendors and how they operate. You must understand what data is being shared, how it is being secured, and what happens if the vendor has an incident. Explore what logs your vendor maintains, what level of detail they provide, how long they are retained, and your ability to access those logs to investigate an incident.

6 Combat ransomware.

The best defense against a ransomware demand is a full and complete backup that is readily available. Creating a Bitcoin wallet in advance and prefunding it can minimize impact if backups are unavailable; however, there are other considerations that need to be addressed before creating a wallet. Most entities engage a forensic firm with a funded Bitcoin wallet.

7 Purchase the right cyber insurance policy.

Look for risk management services and guidance from your carrier in addition to a solid policy, appropriate limits, and claims experience.

8 Implement a strong, top-down risk management program.

- Your entity's information security posture starts at the top. Unfortunately, senior executives are often the most vocal opponents of enhanced security measures. It is imperative for executives at the highest level to be "all in" and constantly project the importance of information security.
- Conduct a comprehensive risk assessment as the basis for your risk management program. This will help you identify and reduce legal risk in your information security practices, respond to regulatory and legal challenges, and focus information security resources on the most critical risk scenarios.
- Entities in every industry should look at the New York Department of Financial Services Cybersecurity Requirements for Financial Services Companies. Even if your entity is not covered by this regulation, experts believe it may be the model for future state or federal cybersecurity regulations.

9 Adopt updated password guidance, and implement MFA or other risk-based authentication controls.

Authentication by username and password alone can no longer protect sensitive information or secure remote access to network resources and third-party providers. This is true for several reasons. First, outdated guidance on password complexity and rotation (now updated) has inadvertently trained users to create bad passwords and share them across sites and services. Second, attackers have breached so many large stores of username and password combinations that billions of breached password records are now in the public domain. Third, attackers use simple tools to automate so-called credential-stuffing attacks, in which attackers use these stolen password databases to brute-force their way into poorly protected services and sites.

As with any good security solution, this problem calls for a layered approach tailored to your entity's risk scenarios and tolerance:

- **Adopt updated password guidance.** Consider updated password policies to match recent guidance published by the National Institute for Standards and Technology (NIST) and Microsoft, which eliminates complex, hard-to-remember passwords and arbitrary password-rotation rules in favor of rules that (1) encourage longer, easier-to-remember "memorized secrets"; (2) check proposed passwords against the corpuses of known breached passwords; (3) implement protections (like rate limiting) that mitigate brute-force attacks; and (4) rotate passwords only if there's a good reason to do so (e.g., password database stolen, password phished).
- **Use strong MFA or other risk-based authentication controls.** To mitigate phishing, credential-stuffing attacks and password reuse scenarios, implement strong MFA controls using software- or hardware-based tokens. Entities concerned about the business impact of full MFA can consider risk-based controls that require additional authentication steps only when suspicious activity is detected. Besides being a good security practice, MFA and other advanced authentication methods are on regulatory agencies' radars.

Consider implementing these controls in any scenario involving (1) remote access to email (on-premises or in the cloud); (2) remote access to network resources through VPN; (3) remote access to cloud resources, including third-party SaaS providers that handle sensitive information like HR or payroll data; and (4) login pages to customer-facing web applications containing sensitive data or processes.

10 Keep data secure in the cloud.

Migrating to the cloud is a great step to increase your entity's data security, but it doesn't mean you can let up on other security measures. Data in the cloud is more secure in some respects, but it is still vulnerable if the entity's overall security posture is weak. When considering a cloud solution, work with your risk management team to ensure that its security model works with your program.

Understand the shared-responsibility model, and ensure that you are doing your part to secure and monitor your data in the cloud. Different uses of the cloud – IaaS, SaaS or PaaS – carry different security obligations. All cloud deployments should be approved by management after being screened for security implications, and secured by personnel with the training and experience to secure data in cloud environments.

11 Prepare for more regulatory inquiries.

- Because of recent settlements between regulators and entities, regulators have more funds to investigate entities that suffer data breaches. As a result, expect more regulatory inquiries, including formal inquiries in the form of CIDs, and more extensive requests for information.
- Because of greater regulatory scrutiny as well as the potential for litigation, think strategically about the timing and language in investigation vendor engagements and scope of work

letters/documentation, especially when engaging existing vendors to assist with an incident investigation. Attorney-client and work-product privileges may not protect all communications.

- Focus on complete and timely remediation following an incident. Regulators want to know you have taken significant steps to prevent another incident from occurring.

12 If you are a publicly traded entity, update your Item 1A Risk Factors regarding privacy and security.

Based on the Securities and Exchange Commission's guidance on cyber risk factors, entities generally disclose three categories of risks: (1) operations/business resiliency – the entity relies heavily on technology to run the business, and if the technology fails, then there may be impact; (2) a data breach risk – what cyber risks the entity may face on a going-forward basis, and what material cyber incidents have already occurred; and (3) privacy/security regulatory compliance – the ability to adapt and comply with new laws as they are enacted and modified globally. Review your risk factors and ensure that these areas are covered.

Risk Assessments: An Essential Guide

Risk assessments are a critical foundation for any information security program. They help satisfy regulatory requirements, demonstrate a commitment to cybersecurity and suggest where to invest limited security resources. In fact, risk assessments have proven so valuable that many standards and regulatory frameworks now require them (HIPAA's Security Rule, the Payment Card Industry Data Security Standard [PCI DSS], NIST, and the New York Department of Financial Services Cybersecurity Requirements, to name a few).

Many entities, however, still do not incorporate true risk assessments into their information security planning, often because of confusion about what a risk assessment is – and is not.

- **A risk assessment identifies threats, vulnerabilities, likelihood and impact.** Risk assessments are often confused with other risk-management tools, such as vulnerability assessments, penetration tests and red-team exercises, compromise assessments, gap analyses, and compliance audits. These are valuable tools, but they do not accomplish the purposes of a true risk assessment. Indeed, they may be rejected by regulators evaluating an entity's compliance with risk assessment requirements.
- **A risk assessment prioritizes and tailors recommendations to a particular entity.** To be useful, a risk assessment must do more than merely catalog an entity's vulnerabilities. Nor can it base its recommendations on generic risk ratings that ignore environment, culture, and risk appetite. Rather, the assessment must tie known vulnerabilities to the threats and attack scenarios most likely to affect the entity.
- **A risk assessment is an ongoing process.** Entities often err by treating a risk assessment as a point-in-time compliance exercise. In fact, it's a continuous process of reflection and improvement. As part of its risk assessment program, an entity should establish a committee or group to meet regularly to evaluate emerging threats and vulnerabilities.
- **A risk assessment focuses on the entire entity, not just information technology.** True risk assessments evaluate all aspects of security management programs, including vendor-management policies and procedures, security awareness training programs, staffing and competence of security engineers and compliance officers, incident response programs, and the management structure of security teams.

About BakerHostetler

To receive an electronic version of this report, please visit **bakerlaw.com/DSIR**

BakerHostetler has more than 940 lawyers in 14 offices, and is widely regarded as having one of the leading data privacy and cybersecurity practices. Our attorneys have managed more than 2,500 data security incidents for some of the world's most recognized brands. Our Privacy and Data Protection team's work extends beyond incident response and is one of the largest of its kind. In addition to privacy and data breach issues, we handle regulatory compliance, GDPR and other cross-border issues, marketing and advertising, eDiscovery, regulatory, and class action defense.

To learn more about how to prevent, prepare for, or manage a data breach, contact BakerHostetler.

Editor in Chief
Craig Hoffman
Cincinnati
T +1.513.929.3491
cahoffman@bakerlaw.com

Janine Anthony Bowen
Atlanta
T +1.404.946.9816
jbowen@bakerlaw.com

David A. Carney
Cleveland
T +1.216.861.7634
dcarney@bakerlaw.com

Teresa C. Chow
Los Angeles
T +1.310.979.8458
tchow@bakerlaw.com

Casie D. Collignon
Denver
T +1.303.764.4037
ccollignon@bakerlaw.com

William R. Daugherty
Houston
T +1.713.646.1321
wdaugherty@bakerlaw.com

Gerald J. Ferguson
New York
T +1.212.589.4238
gferguson@bakerlaw.com

Amy E. Fouts
Atlanta
T +1.404.256.8434
afouts@bakerlaw.com

Alan L. Friel
Los Angeles
T +1.310.442.8860
afriel@bakerlaw.com

Randal L. Gainer
Seattle
T +1.206.332.1381
rgainer@bakerlaw.com

Lisa M. Ghannoum
Cleveland
T +1.216.861.7872
lghannoum@bakerlaw.com

Linda A. Goldstein
New York
T +1.212.589.4206
lgoldstein@bakerlaw.com

Patrick H. Haggerty
Cincinnati
T +1.513.929.3412
phaggerty@bakerlaw.com

John P. Hutchins
Atlanta
T +1.404.946.9812
jhutchins@bakerlaw.com

Edward Jacobs
New York
T +1.212.589.4674
ejacobs@bakerlaw.com

Laura E. Jehl
Washington, D.C.
T +1 202.861.1588
ljehl@bakerlaw.com

Andreas T. Kaltsounis
Seattle
T +1.206.566.7080
akaltsounis@bakerlaw.com

Paul G. Karlsgodt
Denver
T +1.303.764.4013
pkarlsgodt@bakerlaw.com

David E. Kitchen
Cleveland
T +1.216.861.7060
dkitchen@bakerlaw.com

Theodore J. Kobus III
New York
T +1.212.271.1504
tkobus@bakerlaw.com

M. Scott Koller
Los Angeles
T +1.310.979.8427
mskoller@bakerlaw.com

Aaron R. Lancaster
Washington, D.C.
T +1.202.861.1501
alancaster@bakerlaw.com

Melinda L. McLellan
New York
T +1.212.589.4679
mmclellan@bakerlaw.com

Holly A. Melton
New York
T +1.212.589.4208
hmelton@bakerlaw.com

Eric A. Packel
Philadelphia
T +1.215.564.3031
epackel@bakerlaw.com

Lynn Sessions
Houston
T +1.713.646.1352
lsessions@bakerlaw.com

James A. Sherer
New York
T +1.212.589.4279
jsherer@bakerlaw.com

James A. Slater
Cleveland
T +1.216.861.7885
jslater@bakerlaw.com

Paulette M. Thomas
Cincinnati
T +1.513.929.3483
pmthomas@bakerlaw.com

Daniel R. Warren
Cleveland
T +1.216.861.7145
dwarren@bakerlaw.com

Christopher A. Wiech
Atlanta
T +1.404.946.9814
cwiech@bakerlaw.com

BakerHostetler

bakerlaw.com

To receive an electronic version of this report,
please visit **bakerlaw.com/DSIR**