BakerHostetler

2019 DATA SECURITY INCIDENT RESPONSE REPORT

Managing Enterprise Risks in a Digital World

Privacy, Cybersecurity, and Compliance Collide

Key Findings

Please enable MFA! Make sure multifactor authentication (MFA) is enabled before you move to the cloud. Use a prioritized approach to identify cloud resources (approved and shadow) employees are using and put them behind MFA or your enterprise SSO.

The cloud is bigger than you think. It is anywhere you store data accessed with a username and password. And that means data is one phishing email away from unauthorized access.

Incidents won't go away. Simple issues still cause incidents – misconfigured cloud instances, open FTP servers, servers with sensitive data indexed by search engines, and inadvertent disclosures.

Basic hygiene. Despite efforts, large incidents are still occurring. How much old data is sitting around in your network waiting to be taken?

Get ahead of the compliance curve. New laws are inevitable, so work on the lowest common denominator. Anticipate what will be enacted, because most new laws borrow heavily from existing laws and core privacy and security principles – risk assessments, transparency, confidentiality, integrity, availability, fairness, and data minimization.

Use "compromise threat intelligence." Leverage the misfortune of others to identify emerging risks: determine if the issues affecting other companies apply to you and address them before you become a victim.

Focus on effective cybersecurity. Use security risk assessments to build a prioritized plan to mature your security posture. If you stop at just getting an industry benchmark score, invest in enhancements without considering practical threat assessments, or take on too much just to improve your overall score, you may do more harm than good.

Phishing is remarkably effective. So, attackers will continue to phish away. Reduce risk by raising employee awareness and training everyone on how to respond to a "phishy" request. This includes email, text messages, social media messages, and phone calls/voicemails. Also, leverage technology solutions such as anti-phishing toolbars and applications that verify a site's security certificate.

Digital risk (privacy and security issues) management requires an enterprise approach. Form a committee, look at issues that have affected others, and tackle the risks in a prioritized manner.

Do M&A due diligence. Build in an evaluation of digital risks to assess the target's privacy compliance and security posture before the acquisition. Compromise assessments before or immediately after acquisitions of new entities help find undetected issues and support integration efforts.

GDPR significantly changed incident response for global companies. In addition to the short time to notify a supervisory authority, the complexities of cross-border breaches include the impact on attorney-client privilege, post-disclosure regulatory approaches, and an increase in data subject rights requests. As laws modeled on GDPR spread to other countries, the globalization of GDPR will further complicate incident response.

Regulators are working together and working on their own. Overall, they continue to be active. Know what is likely to put you in their crosshairs, and build that into your compliance road map.

Class actions arising from data breaches or that allege violations of privacy laws continue. Outcomes remain inconsistent, with outliers in both court rulings and settlements. Derivative actions are becoming more popular, based on both data breaches and statutory compliance grounds. The plaintiffs' bar continues to be creative to survive motions to dismiss, and some are coordinating efforts with regulators.

CONTENTS

02 Incident Response Trends
04 Compromise Response Intelligence in Action
06 Why Incidents Occur
08 Timeline Provides Context for Response Expectations
10 Forensics Drive Key Decisions
12 Regulators More Involved
14 Litigation
16 Leveraging Response Compromise Intelligence to Minimize Risk

Welcome to our fifth Data Security Incident Response Report. Each year, we analyze the data from incidents we helped companies manage over the prior year. This year, we discuss the insights gained from working on more than 750 incidents in 2018.

Because privacy laws globally (such as GDPR) are shifting the way companies need to prepare for and manage data breaches, we have highlighted the collision of data security, privacy, and compliance – a convergence that has led many companies to create enterprise risk steering committees with stakeholders representing each of these concerns.

Cyberattacks continue – whether motivated by monetary gain, to disrupt business operations, or to obtain information for a nation-state. Many attacks begin with a phishing email that seeks to obtain network-access credentials. Raising employee awareness and employing multifactor authentication are still two of the best defenses against these attacks.

Big breaches also continue, often the result of poor data hygiene practices or a failure to employ increased security around the company's "crown jewels." Last year, many of the incidents we managed resulted in access to a limited amount of personally identifiable information; however, the investigations were protracted and costly because of the need to review of thousands of emails (sometimes manually) for information that triggered breach notification laws. And because notification laws outside the U.S. are triggered by a broad definition of "personal information," the review is not always straightforward. Developing a calculated yet appropriate review protocol is critical.

International laws have made incident response more complex because of new and detailed regulatory reporting requirements. More than 25% of the incidents we worked on involved international laws and reporting requirements.

Notifications of security incidents have often been followed by an increase in access rights requests. So, having an established and scalable access rights request process becomes critical to enable you to address the increase in requests.

To help companies manage both the U.S. and international reporting processes, we have published the U.S. Breach Notification Law Interactive Map and the EU GDPR Data Breach Notification Resource Map.

Experience matters in incident response. The vendors you choose, including your legal counsel, need the benefit of Compromise Response Intelligence gained from managing thousands of incidents. Clients continue to seek guidance on metrics for security spend, incident response planning and tabletop exercises, security assessments, and board oversight guidance. We hope this Report will help you address these complex issues.

Sincerely,

Ted Kobus
Chair, Privacy and Data Protection Team

750+

Incidents in 2018

U.S. Breach Notification Law Interactive Map

bakerlaw.com/BreachNotificationLawMap

EU GDPR Data Breach Notification Resource Map

bakerlaw.com/EUGDPRResourceMap

Incident Response Trends

Top 5 Causes

1

37%
Phishing

After phishing occurred, more than 30% of the time a takeover of an Office 365 account occurred

2

30%
Network Intrusion

3

12%
Inadvertent Disclosure

4

10%
Stolen/Lost Device or Records

5

4%
System Misconfiguration

Incident Response Timeline

66 Days
Occurrence to Discovery

8 Days
Discovery to Containment

28 Days
Time to Complete Forensic Investigation

56 Days
Discovery to Notification

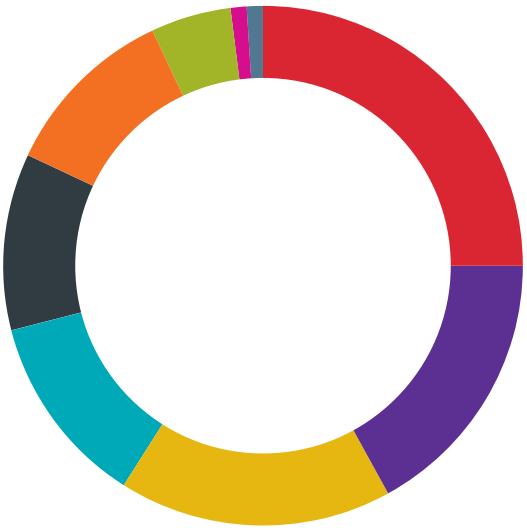
Average Forensic Investigation Costs

$63,001
All Incidents

$120,732
Average Network Intrusion

$350,576
Average of 20 Largest Network Intrusions

Industries Affected



25% Healthcare (including Biotech & Pharma)

17% Finance & Insurance

17% Business & Professional Services (including Engineering & Transportation)

12% Retail, Restaurant & Hospitality (including Media & Entertainment)

11% Education

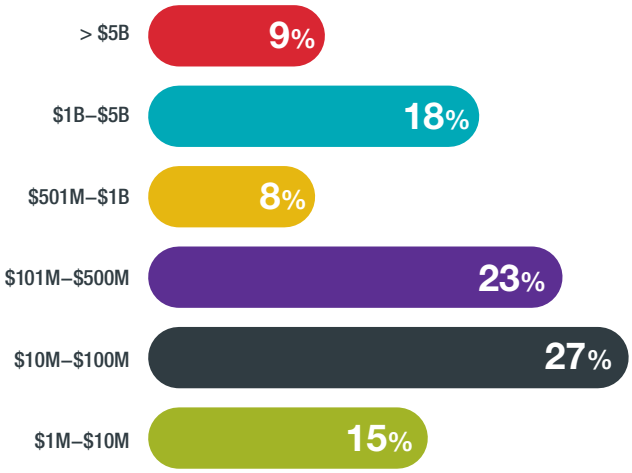
11% Other

5% Government

1% Nonprofit

1% Energy

Entity Size by Revenue



Breach Discovery

74% Internally Discovered

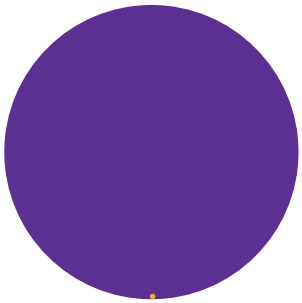
26% Externally Discovered

25% of incidents involved international reporting requirements

Encryption key received and data restored

91% of the time after paying ransom

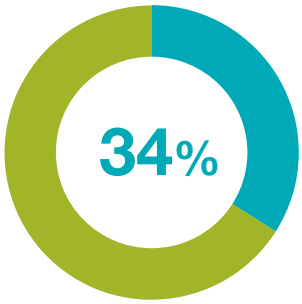
Notifications vs. Lawsuits Filed



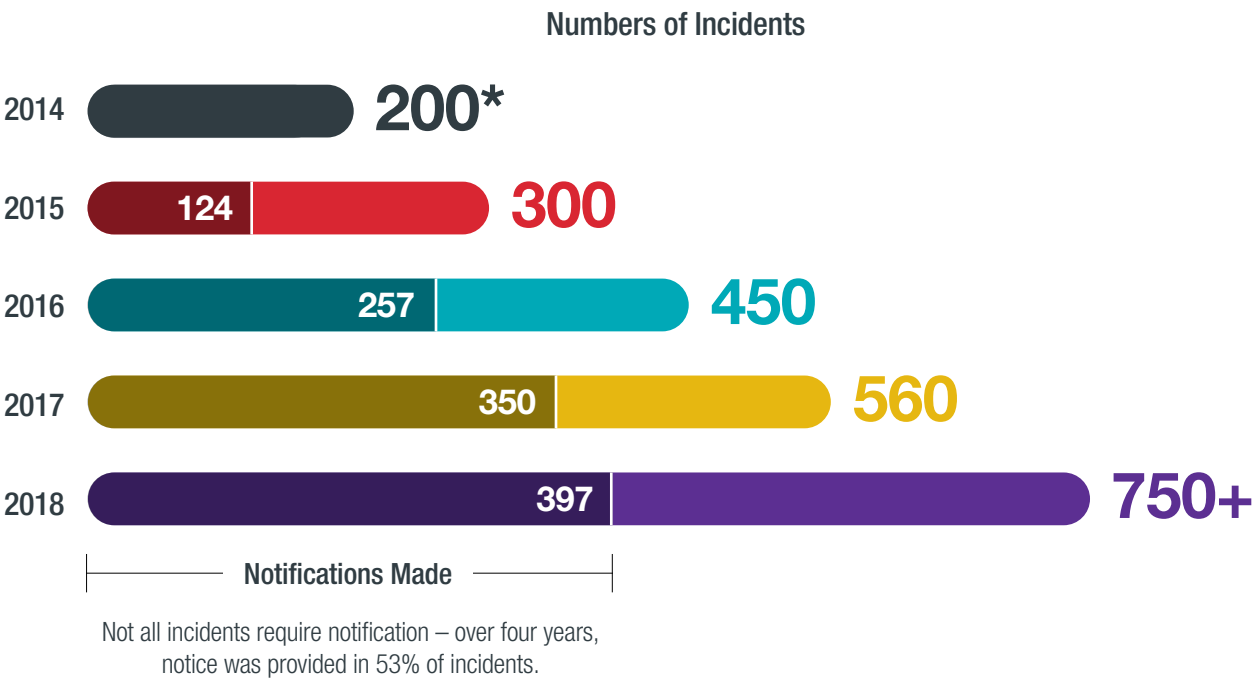
397 Notifications

4 Lawsuits Filed

AG Inquiries Following Notification



Compromise Response Intelligence in Action



Not all incidents require notification – over four years, notice was provided in 53% of incidents.

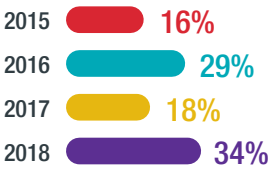
*Not all data sets mentioned were measured in the 2014 DSIR Report, our first edition.

Credit Monitoring Offered

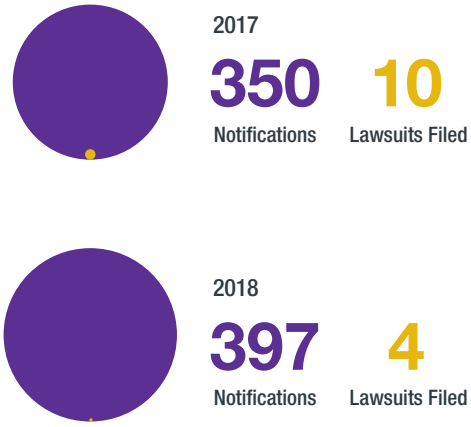
The high percentage of times that credit monitoring is offered shows that SSNs have consistently been involved in notifications.

AG Inquiry After Notice

After notification occurs, a regulatory inquiry is the most likely next development (more likely than a lawsuit).

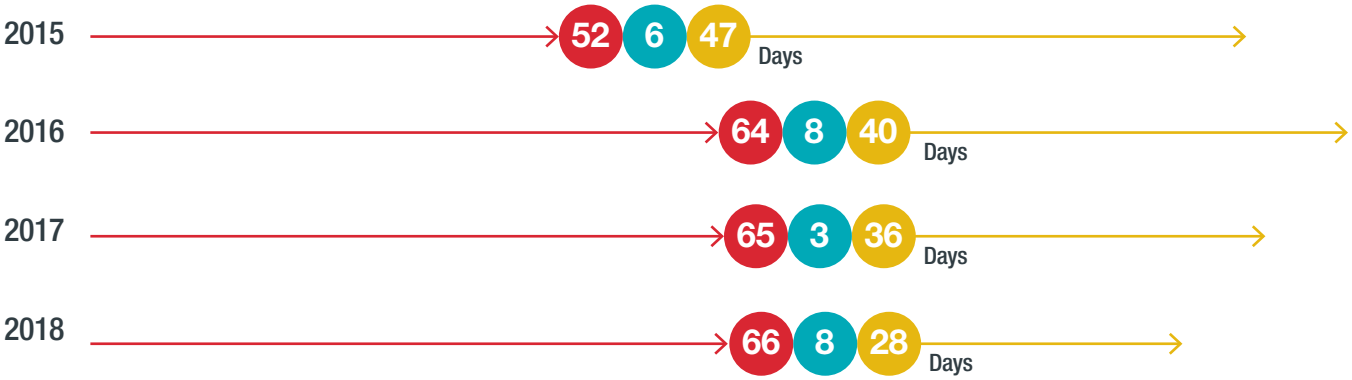


How Likely is a Lawsuit?



Timeline

We have seen improvement in containment and time to complete forensics. Although more entities are self-detecting, time to detection is still an area for improvement.



Detection

Occurrence to Discovery

Entities still have room to improve here. The average time in 2018 from first awareness to first scoping call was 11 days. Entities have improved their ability to detect – self-detection has gone from 52% of incidents in 2015 to 74% in 2018.

Containment

Discovery to Containment

Although the average time to contain has stayed in the six-to-eight-day range over five years, realistically it is improving by holding steady. This is because the number of network intrusions we handle has increased, and network intrusions generally take longer to contain than other incidents.

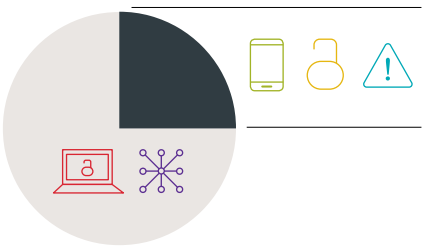
Analysis

Engagement of Forensics to Completion

The time to complete a forensic investigation has improved significantly.

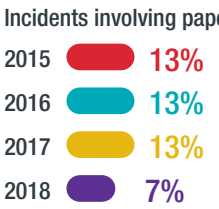
Causes

As the number of incidents that involve phishing and network intrusion has increased, focusing on the basics has driven down the number of avoidable incidents. But lost devices, inadvertent disclosure, and system misconfigurations still cause one-fourth of the incidents we respond to, so there is more room for improvement.



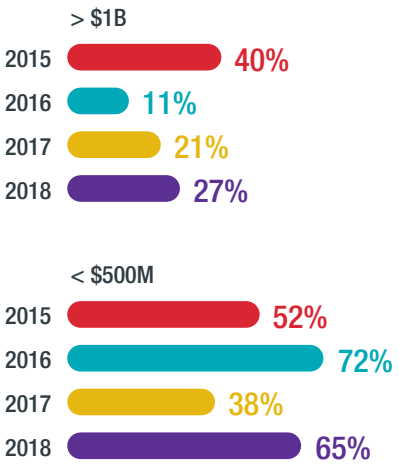
Data Involved

We have been reminding clients not to ignore paper records.



Demographics

Incidents do not discriminate by entity size.

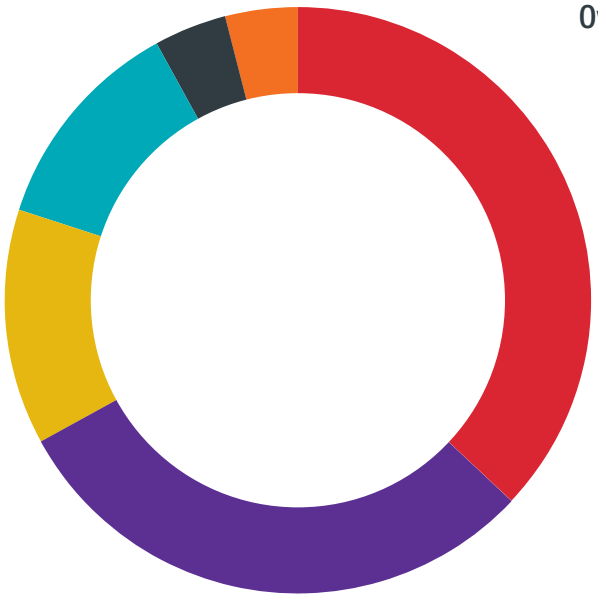


Why Incidents Occur

As in prior years, phishing and vulnerable systems are behind two-thirds of all incidents. Attackers – from the most sophisticated to the run-of-the-mill – continue to use phishing as the primary means of gaining access to an asset. It is simple and effective, and it often goes undetected. Phishing was the attack vector in 37% of incidents. The most common phishing scenario we saw was a message designed to trick a user into providing Office 365 account credentials.

Network intrusions followed closely as the second leading cause, with some form of intrusion occurring in 30% of incidents. Unpatched servers accessible from the internet and open FTP/RDP devices were common first points of entry.

Overall



37% Phishing

30% Network Intrusion

13% Stolen/Lost Device or Records

12% Inadvertent Disclosure

4% System Misconfiguration

4% Other

Other Incident Aspects

After gaining access to a device or account, the most common next steps were:

34% Accessing an Office 365 Account

30% Roaming Network to Find Available Data

12% Dropping Ransomware

8% Obtaining a Wire Transfer to the Attacker's Account

- 1% of phishing or network intrusions were followed by the installation of malware to use system resources (e.g., cryptomining).
- Less than 1% of incidents were attributed to a nation-state actor.

Take Action: Stop Phishing

Phishing remains the most common method used by all attackers – from the most to the least sophisticated – to gain access to a target. And as more assets are moved to the cloud, where they can be accessed with just a username and password, the importance of using a multi-pronged approach to address this risk is critical. The key elements of phishing prevention include:

- **Employee awareness and training.**
- **Enabling MFA (if you cannot do this everywhere immediately, start by prioritizing accounts with access to sensitive data).**
- **Disable or set alerts to identify suspicious activity, such as authentication from IP addresses in high-risk regions, mail forwarding, and legacy connection protocols.**
- **Information governance – pay attention to what data is in the cloud and how long it is kept there, especially email.**
- **Separate administrative accounts from user accounts, and segment sensitive data.**
- **Enforce an account lockout after a specific number of failed attempts.**

Take Action: Address Ransomware Risk

Ransomware and its often-devastating impact on business operations will not go away on its own. When an infection occurs, an entity has three choices:

1. **Restore from an available backup,**
2. **Pay the ransom, or**
3. **Suffer the impact of downtime while rebuilding the affected device(s)/systems.**

Entities continue to overestimate the ability to restore and the time to restore. Consider your entity's approach to paying a ransom before a ransom scenario occurs, including under which scenarios you would pay and how you would pay.

91%
Percent of time when ransom was paid that a decryption key was received

$28,920
Average ransom paid

94%
Percent of time entity used a third party to pay ransom

$250,000
Largest ransom paid*

*In 2019 our clients have already paid three ransoms of $1 million or more

Responsible Party

55%
Employee

Often there is a combination of an employee mistake exploited by a non-vendor unrelated third party (i.e., a threat actor).

27%
Non-Vendor Unrelated Third Party

11%
Vendor

3%
Non-Vendor Related Third Party

2%
Unrelated Third Party

2%
Not Applicable

5% of the time the responsible party was a malicious insider.

Timeline Provides Context for Response Expectations

Speed of notification is a much-watched metric, and there is increased pressure due to new regulations about timing of notice. Entities also feel compelled to be "transparent" by making an external statement early in the investigation of an incident.

Unfortunately, these early statements are often wrong. Within the first 72 hours of awareness, most entities have not even contained the incident, let alone learned its scope. By tracking the timing associated with the core life cycle of incident response – detection, containment, analysis, and notification – we help entities use our Compromise Response Intelligence to enhance preparedness and aid in decision-making during an incident.

The timing of these four areas has remained fairly consistent, with some improvement, over the past four years. This consistency in the face of laws with shorter notification timelines reflects the practical reality of what it takes to get from first awareness of a potential issue to notification. There is always room for improvement, but getting to notification in less than 30 days (a growing expectation of regulators and individuals) is extremely difficult.

Detection

The time from initial occurrence to detection continues to show room for improvement. It decreased slightly for non-network intrusions (from 66 days to 64 days) and increased by five days for network intrusion incidents (from 84 days to 90 days). The earlier an incident is detected, the more forensic data is usually available, which leads to more effective mitigation efforts and more certainty about what occurred. Implementing monitoring tools on systems holding sensitive data and for anomalous user activity goes far in identifying activity – as long as they are configured correctly. Of the data breaches in this year's survey, 74% were detected internally (an increase of 10% over last year). Only 3% of incidents went undetected for more than six months, and only 5% went undetected for more than one year.

Occurrence to Discovery

HEALTHCARE
36 Days

NETWORK
INTRUSION
95 Days

Containment

Sometimes containing the incident is a quick fix. Often it is not. Containment measures range from confirming deletion by an inadvertent recipient to changing the password of a compromised account to working with a forensic firm to build a multifaceted plan to lock out the attacker. This time frame is tense, and the stakes are high – if you don't learn enough about how the attacker is accessing the environment, you may be playing whack-a-mole for days or weeks. On average, it took almost eight days to learn enough about what occurred to build and implement an effective plan to stop the incident. For network intrusions, the average was longer, at 10 days. Three factors are key to shortening the containment period: (1) an existing relationship with a forensic firm, (2) easy access to forensic data (e.g., logs from a SIEM tool, live response data from an endpoint security investigation tool), and (3) effective project management to build and execute the containment plan.

Discovery to Containment

HEALTHCARE
10 Days

NETWORK
INTRUSION
10 Days

Number of Individuals Notified

2018 AVERAGE: **6,977**

2017 AVERAGE: **87,952**

Average Number of Individuals Notified by Industry

Retail, Restaurant & Hospitality (including Media & Entertainment)	10,000
Healthcare (including Biotech & Pharma)	5,751
Education	4,242
Finance & Insurance	4,177
Other	888
Business & Professional Services (including Engineering & Transportation)	873
Energy	851
Government	239
Nonprofit	46

Take Action: Shortening the Timeline

- **Improve event triage to escalate and engage the right internal and external resources faster. Entities are using three-to-five-person "Triage Incident Response Teams" representing different parts of an organization to ensure the right response plan is built from the start.**
- **Establish key third-party relationships (legal and forensic) before an incident occurs. Go beyond identifying and having engagement letters in place by doing onboarding and training (e.g., tabletops).**
- **Know how to get visibility – have a plan for identifying indicators of compromise across endpoints and accessing host and network logs. Using endpoint agents for digital forensics and reviewing logs aggregated to a SIEM should be part of your plan.**

Analysis

This area shows both consistent improvement and a need for even more. The average time to complete the forensic investigation shrank by a full week last year compared with 2017. Factors behind this improvement include building relationships with forensic firms before an incident, more prevalent use of security endpoint agents for digital forensics, and better logging practices. But some entities are still facing challenges in properly triaging newly discovered incidents. On average, 11 days elapsed between an entity's first awareness of the potential incident and the first phone call with the forensic firm.

Engagement of Forensics to Completion

HEALTHCARE
32 Days

NETWORK INTRUSION
36 Days

Notification

Despite the forces pushing entities to notify quickly, we saw a 67% increase in the time from discovery to notification, going from an average of 40 days over the past few years to 56 days in 2018. The surge in Office 365 account takeover incidents was a primary driver of this increase. If a criminal accesses an Office 365 inbox, the entity may need to run programmatic searches followed by a manual review to identify messages and attachments that contain the type of information that requires notification to individuals. This process is expensive and can take weeks, especially if the searches involve personal data requiring notification under HIPAA or GDPR.

Discovery to Notification

HEALTHCARE
49 Days

NETWORK INTRUSION
50 Days

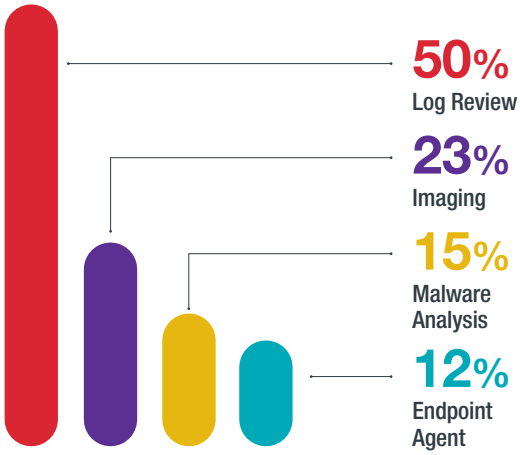
Forensics Drive Key Decisions

It is acutely important to quickly determine the scope of the incident and implement a plan to stop the attack. The regulatory landscape continues to ratchet up the pressure to disclose faster (sometimes within 72 hours), through regulations and after-the-fact enforcement. Whether the incident involves potential theft of data or affects business continuity (such as ransomware shutting down critical technology resources), fast and effective scoping and containment are critical. Visibility to the environment to determine how and what occurred is the crucial factor in stopping the attack and preventing immediate reinfection/access.

In 2018, some form of forensic investigation was used in 65% of incidents overall. Forensics were used in 79% of network intrusions, a 14% increase from 2017. Although more companies are investing in security tools that can assist in investigating security incidents, such as endpoint monitoring tools and security incident and event management tools (and SIEM tools), few companies have the experience, indicator of compromise/threat intelligence, and capacity to adequately investigate without third-party help. The executive teams and boards of entities recognize the credibility a leading forensic firm adds to investigation findings, and regulators have come to expect it. Entities are getting better at helping forensic firms complete their investigations faster – in 2018, the average number of days to complete an investigation dropped to 28 days, down from 40 days in 2016 and 36 days in 2017. This improvement makes it possible to notify affected individuals and appropriate regulators faster when required.

The average cost of the forensic investigations we managed in 2018 decreased as well. Across all investigations, the average dropped from $84,417 in 2017 to $63,001 in 2018. For investigations of network intrusion incidents however, the average was $120,732, up from $86,770 in 2017.

Type of Investigation



We engaged more than

20

different forensic firms.

Use of Outside Forensic Firms

79%
Network Intrusion Incidents

65%
Data Breach Incidents in 2018

41%
Data Breach Incidents in 2017

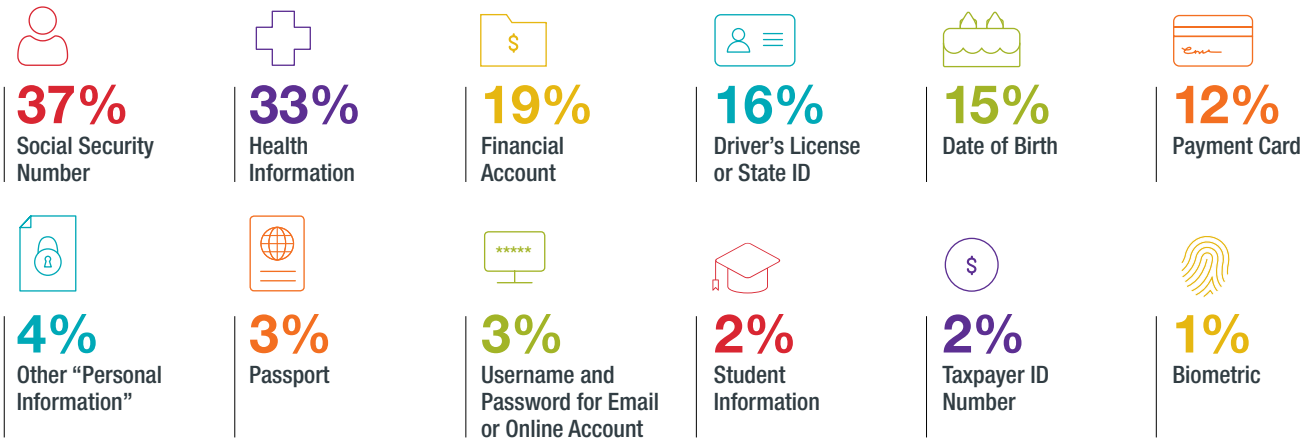
Forensic Investigation Costs

$63,001
All Incidents

$120,732
Network Intrusion Incidents

$350,576
Average of 20 Largest Network Intrusions

Data at Risk



Nation-State Attacks Drawing More Attention

Nation-state cyber operations continue to support espionage, economic development (through IP and trade secret theft), or sabotage. But the line separating traditional victims of nation-state activities from others faded years ago. And the collateral damage to unintended victims has been significant. Good data on how often true nation-state attacks occur is hard to find, in part because they go undetected or unreported. Less than 1% of our incidents in 2018 involved attribution to a nation-state actor.

Collateral damage. Several high-profile attacks attributed to nation-state actors – the WannaCry and NotPetya attacks being most prominent – demonstrate the threat that nation-state attacks pose to any entity, even those that are not intended targets.

Supply chain. The risk posed by vendors and third-party suppliers is heightened in this area, because attacks against these business partners look for the "weak link" and then exploit a trusted relationship between the vendor and customer.

Blending of nation-state and criminal TTPs. It has become increasingly difficult to differentiate between the tactics, techniques, and procedures (TTPs) used by nation-state actors (whose motives are usually some variation of espionage or sabotage) and criminal actors (whose motives are financially driven).

Who attacked me? Victim organizations often want to know who attacked them and why. This information can be useful for future network defense, to determine the potential risk of harm to individuals whose information may have been involved, and to defend against regulatory and private civil actions. But the blending of TTPs – and attackers' ability to conceal or fabricate an attack's source – make attacker attribution difficult even for the most well-resourced intelligence firms and government agencies. Where attribution is possible, it often lacks confidence, is later proven incorrect, or relies on a combination of highly sensitive and classified sources that cannot be shared publicly or with victim organizations absent special protections and approvals. There may also be insurance coverage implications.

Take Action: Forensics

- **Identify and engage with a forensic firm before an incident. Some may need or want the security of a retainer agreement with a guaranteed response time, but for many, simply negotiating the MSA pre-incident can be an effective pre-incident engagement step.**
- **When selecting a firm, assess the capacity and credibility needs you will have during an incident. Evaluate the endpoint and network tools firms under consideration would use and how they align with your network. If you have cyber insurance, make sure they are on your carrier's panel of approved firms (if there is such a requirement).**
- **Do onboarding with the firms after you select them. Determine how they will get visibility into your environment when you ask them to investigate, and determine how long that would take (e.g., whether you have an SCCM tool to deploy their endpoint agent, how you will get them access to logs in your SIEM).**
- **Consider having that firm help you build run books for common incident response scenarios. Talk with them about your logging practices to make sure you are logging the right details and retaining them for a long enough time. Use their response experience to help you prepare for the scenarios you are likely to face.**
- **Know your environment – how many endpoints, operating system types, key vendors, segmentation approach, data flows – so you can be in a position to help the forensic firm help you.**

Regulators More Involved

The Usual Suspects
Every state now has a breach notification law, and many have made revisions over the years. State attorneys general (AGs) view enforcement of data security incidents as one of their chief consumer protection priorities. Inquiries and investigations are coming from more AGs than just a few of the active state AGs. AGs also are expanding their enforcement regimes, either through new state laws or increased use of existing laws. For example, 2018 saw the first AG multistate lawsuit to enforce HIPAA. Meanwhile, the Office for Civil Rights (OCR) continues as the primary HIPAA enforcer, frequently investigating HIPAA-related incidents involving more than 500 people. And settlement amounts continue to trend upward. Whether initiated by OCR, a state AG, or international regulator, investigations almost invariably go beyond the facts of the incident itself, and a resolution likely will require significant changes to data security practices.

New Kids on the Block
Joining these traditional data privacy regulators are some other entities that have not traditionally been active in the data privacy sphere, including state and federal financial regulators and European Data Protection Authorities (DPAs).

State departments of insurance and financial regulation as well as the U.S. Securities and Exchange Commission are also active. A number of states have adopted or are adopting a model law promoted by the National Association of Insurance Commissioners that requires 72-hour notice of a cybersecurity event.

AG Inquiries Following Notifications

135

OCR Investigations

2017	2018
22	34

Percent of Incidents That Triggered an Investigation

2017	2018
54	27

California Alters U.S. Privacy Law

Companies need to start preparing to comply with the forthcoming California Consumer Privacy Act (CCPA), a paradigm-shifting approach to data privacy that borrows heavily from European law. The CCPA will affect all but the smallest businesses with data on California residents. Those with existing compliance programs for the EU's GDPR will have a head start. The CCPA is effective January 1, 2020, but companies will need to have begun detailed data mapping and tracking of data practices as of January 1, 2019 in order to comply in 2020 with notice and consumer request requirements that are subject to a 12-month lookback.

The CCPA gives California residents the right to learn categories of personal information that businesses collect or otherwise receive, sell, or disclose about them; the purposes thereof; and the categories of third parties with whom businesses disclose PI. It also grants California residents the rights to (1) obtain more detailed information about their own personal information; (2) access and obtain transportable copies of their personal information; (3) prevent businesses from selling their personal information; and (4) subject to certain exceptions, to request that a business and its service providers delete their PI.

The CCPA prohibits businesses from discriminating against consumers who exercise these rights, subject to some exceptions. The CCPA will require detailed disclosures as well as multiple methods for exercising data subject rights.

Further, the CCPA requires that contracts with service providers include certain terms, including a requirement to delete personal information.

The California Department of Justice has stated that it will need to secure more than $57.5 million annually in civil penalties to cover its cost, suggesting the potential for robust enforcement. There is also a limited private right of action for security incidents. Plaintiffs' class action attorneys may also attempt to bring claims under California's Unfair Competition Law for CCPA violations, notwithstanding language in the CCPA that should preclude such actions.

Although bringing your company into compliance with the CCPA will require an investment of time and resources, it also provides an opportunity to identify inefficiencies, upgrade outdated processes, and proactively tackle privacy and data security concerns. And with at least 15 other states drafting similar laws, a wait-and-see approach to beginning compliance efforts is likely to leave you scrambling and at risk.

> "The California AG may bring actions for civil penalties of $2,500 per violation, or up to $7,500 per violation if intentional."

EU Update: GDPR a Game-Changer for Data Breach Notification

When the EU GDPR took effect on May 25, 2018, it dramatically changed the way multinationals manage the reporting of personal data breaches. It also substantially raised the stakes: entities found to have violated the GDPR's data security and breach reporting obligations may face much steeper regulatory fines under the new regime, far greater than penalties typically experienced by companies in the U.S.

Among the challenges in responding to a personal data breach in the EU are the scope of what constitutes a notifiable breach and the tight time frame for providing notification. The GDPR defines "personal data" more broadly than the definition of "personally identifiable information" under most U.S. laws. And its definition of a "personal data breach" includes any incident that affects the confidentiality, availability, or integrity of personal data – even incidents caused by accidents or natural events. This departs from some U.S. laws that define breaches more narrowly, with a focus on confidentiality breaches and breaches caused by malicious actors. An entity that experiences a data security incident must investigate and notify regulators within 72 hours of becoming aware that the incident is a personal data breach, unless it is "unlikely to result in a risk to the rights and freedoms of natural persons." In addition, entities must notify affected individuals where the incident is "likely to result in a high risk" to those rights and freedoms. Failure to implement appropriate data protection policies or to properly notify regulators or individuals is punishable by fines of up to 4% of a company's global annual turnover.

In advance of the GDPR's implementation date, our data privacy lawyers guided clients through more than 150 multifaceted GDPR compliance projects. Since late May 2018, we have helped clients investigate and respond to more than 20 incidents where notification was made to a data protection authority in the EU and other international jurisdictions. The incidents ranged from Office 365 account takeovers affecting only a few individuals with relatively low-risk data to complex network intrusions involving notification to individuals and data protection authorities across dozens of countries/territories.

Take Action: Address the Globalization of Incident Response

- **In advance of a breach implicating the GDPR, identify the regulators to whom you will report and the associated reporting requirements. There are substantial challenges to meeting the 72-hour GDPR deadline, beyond just the short time period. Many DPAs have created online reporting portals and allow preliminary reports to be supplemented once affected entities have more information about the incident. However, particularly for English-only speakers, navigating inconsistent, unclear, foreign language-only, or nonexistent reporting portals can consume valuable time while the clock is ticking.**

bakerlaw.com/EUGDPRResourceMap

This resource provides access to EU member state-specific notice forms, supervisory authority contact details, and state-specific guidance.

- **Entities subject to the GDPR should identify their Lead Supervisory Authority (LSA) before a breach occurs. The benefit of an LSA designation is significant; it permits the entity to report a breach to a single DPA (the so-called "one-stop shop") rather than to authorities in each EU member state.**
- **Incident response plans should be revised to contemplate GDPR breaches. Consider the timing and complications associated with reporting a personal data breach in multiple countries, including inconsistent or conflicting legal and regulatory requirements, and unique risks that may arise in certain jurisdictions.**
- **Consider the role of the Data Protection Officer (DPO) or Article 27 Representative. Entities subject to the GDPR's requirement to designate a DPO or a Representative (for businesses not established in the EU) should consider the role of these individuals in the data breach response process, particularly for multinational incidents that might implicate legal privilege in the U.S.**
- **More than 25 jurisdictions around the world impose some sort of data breach notification obligation. That number is almost certain to grow. The variations in what information must be reported and to whom, as well as the circumstances, format, and language of such reports, are unpredictable. And there is often little guidance as to how authorities will enforce requirements or respond to notification. Multinationals holding personal data for individuals should make privacy and data protection a top priority, with proper planning for cross-border incident response a key component of their data security program.**

Litigation

Class actions involving a criminal attack on a network are on the rise.

No decisions on class certification in 2018

Increase in shareholder derivative actions

2018 saw new developments in the evolving law surrounding data privacy class actions. Over the past several years, there has been a shift in the types of cases filed. As entities have taken measures to reduce incidents involving loss or theft of unencrypted devices containing sensitive data, class actions filed over physical theft of data have decreased. Simultaneously, consistent with the increase in phishing and network intrusion incidents, there has been an increase in class actions involving a criminal attack on a network. This includes numerous high-profile attacks where hundreds of millions of individuals were notified.

Most circuits continue to reject attempts to end lawsuits at the outset through challenges to consumer standing. Although the circuits are split on Article III standing, decisions continued to trend toward finding standing in data breach class actions, even in the absence of actual financial loss suffered by the named plaintiffs. The Supreme Court has not yet addressed the issue head-on. Although many hoped that the Court would grant certiorari in the *Zappos.com, Inc. v. Stevens, et al.* case seeking review of the Ninth Circuit's decision finding standing in a data breach case, the Court passed on this opportunity in early 2019. Thus, the trend toward finding standing will likely continue.

Decisions on motions to dismiss data breach class actions for failure to state a claim continued to be inconsistent. The most common outcome is a decision that grants in part and denies in part motions to dismiss for failure to state a claim. The outcomes of these motions differ significantly based on the types of claims asserted, the state whose laws govern the complaint, and the individual predilections of the assigned judge. For example, the Northern District of Georgia in *In Re Equifax, Inc., Customer Data Security Breach Litigation* allowed a majority of the plaintiffs' claims to go forward, whereas the D.C. District Court recently dismissed all claims asserted in *Attias v. Carefirst, Inc.* (except for two claims asserted on behalf of only two of the plaintiffs). In some cases, courts dismissed contract-based claims but allowed tort claims to go forward. In other cases, tort claims were dismissed but contract-based claims survived. Many courts were also reluctant to dismiss state statutory claims at the pleading stages. We expect this trend to continue as more states enact breach notification statutes that allow for private rights of action.

On the class certification side, another year went by without a significant development. Case precedent on certification (outside of settlement certification) remains scarce. In recent years there have only been two contested cases where data breach classes were certified. In 2015, the District of Minnesota certified a class of financial institutions that had to reissue credit cards following a cyberattack on retailer Target. In 2017, the Middle District of Alabama certified a relatively small class – 1,208 patients of a hospital lab – whose information was compromised by an employee who stole patient files and then made at least 124 fraudulent tax returns with the stolen information. One common element is that members of both classes articulated actual

"Decisions on motions to dismiss data breach class actions for failure to state a claim continued to be inconsistent."

damages directly traceable to the incident. The few other courts that have addressed contested class certification motions in data breach actions have been unwilling to certify classes due to the individualized nature of causation and damages. Specifically, it has been unclear in those cases whether many class members actually suffered damages following the security incidents. Even if the class members did suffer damages, it was unclear whether such damages were actually caused by the particular security incident in question. This is a developing area of the law to watch in 2019.

Perhaps the most impactful development is in the area of shareholder derivative actions, arising from disclosures of security incidents and regulatory compliance. As more of these cases survive motions to dismiss and result in favorable settlements, the incentive to file them has increased.

BIPA Litigation

200 Pending Class Actions Involving Biometric Data

There are currently more than 200 class actions pending in Illinois state and federal courts involving claims under the Illinois Biometric Information Privacy Act (BIPA). Roughly half were filed in 2018. Most of the lawsuits challenge Illinois employers' use of timekeeping systems where employees use finger, hand, or facial scanning to clock in and out of work.

Slightly over 10% of the lawsuits involve the use of "biometric" technology in the consumer context. Plaintiffs assert that employers and technology providers failed to have BIPA-compliant policies in place regarding data retention and destruction, and failed to provide notice to employees that their scans were being collected and to obtain their written consent. While many of the cases were stayed in 2018 pending an Illinois Supreme Court opinion interpreting a portion of BIPA, there were some significant rulings. One such ruling was for an airline company where the case was dismissed when the court determined that the claims were pre-empted by federal labor law.

The most notable recent ruling occurred on January 25, 2019, when the Illinois Supreme Court issued a decision in *Rosenbach v. Six Flags Entertainment Corp.* The court held that the collection of a finger scan from a 14-year-old for an amusement park season pass without providing written notice of biometric collection or obtaining a parent's consent violated BIPA even though no harm such as improper use or a breach of data was alleged. Now that the *Rosenbach* decision has been issued, the stayed BIPA cases will be actively litigated, and a new surge of BIPA class action filings has begun.

Despite the *Rosenbach* decision, BIPA defendants still have a number of strong defenses available to defeat BIPA claims and to oppose class certification. We anticipate that BIPA litigants will focus on motion practice in 2019.

Leveraging Compromise Response Intelligence to Minimize Risk

Most incidents are preventable. And not all incidents are catastrophic – the most common often only affect a small number of people and have simple causes. Despite the scare tactics and other challenges, like capacity and budgets, there are basic steps that can be taken to drive incremental improvement in an entity's compliance and risk posture. You can look at the types of incidents other entities in your industry have faced, determine whether the same could happen to your entity, and then use projections of costs and impact to prioritize where to start.

BASELINE RECOMMENDATIONS

1. **Increase awareness.** Do training to show employees how they will be exploited (e.g., social engineering and phishing) and the simple mistakes they can work to prevent (e.g., sending an email with sensitive data to the wrong person or attaching the wrong file).

2. **Conduct risk assessments.** Identify gaps and risks, and then build a prioritized plan to incrementally improve your security posture and address any identified gaps.

3. **Implement basic security measures.** Securely configure devices and systems, use segmentation, deploy endpoint agents, funnel logs to a SIEM tool, address patch and vulnerability management, use access controls, address privileged credential management, and use multifactor authentication for remote access points.

4. **Improve detection capabilities.** Reducing the time from intrusion to detection remains one of the top areas in which companies can improve. Ensure your company is investing in the right mix of detection technology and personnel (whether internal or through managed security providers), and continually refine the tools to reduce false positives and adapt to the changing threat landscape.

5. **Prepare to respond when incidents occur.** Who are the key people at your entity that will triage reports of new potential incidents to make sure the right response plan and right third parties are brought in? Conduct tabletop exercises.

6. **Address and be realistic about business continuity.** Ransomware is a significant issue and, like home improvement, the time to restore from backups usually takes several times longer (if it works at all) than initial projections.

7. **Continue to address vendor risks.** Increase awareness of the need for all parts of an entity (e.g., marketing, HR, business) to work with security and legal to vet potential vendors, negotiate appropriate contract terms, and oversee vendors throughout their life cycle.

8. **Mitigate financial impact.** Build realistic assessments of financial impact in the event of an incident and purchase cyber insurance accordingly.

NEW RECOMMENDATION TO ADDRESS EMERGING RISKS

9 **Trust but verify.** Most CISOs inherit a network that has been built over time by different teams. When taking over an existing environment, don't just ask questions (e.g., Do we have good segmentation?). Take steps to verify that the key items your security measures and risk posture evaluations are built around have been implemented in the way you have been told. Threat actors who gain access to one device in a network are very effective at exploiting ineffective segmentation.

10 **MFA and access controls.** Regulators increasingly view MFA as an expected practice, not just a best practice. Some methods of MFA are more effective than others. And make sure to get the implementation right. For example, in Office 365 tenants, some forms of connections do not support modern authentication, so there are ways to authenticate without being prompted for a second factor, even if MFA is enabled for most connection types.

11 **Digital risk committee.** The next evolution in addressing the enterprise risk created by privacy compliance and network security issues (i.e., digital risk) is to form an enterprise digital risk committee that has budgetary funding.

12 **Secure your cloud resources.** It's time to embrace the continued move to cloud. Take advantage of the benefits of the move, but make sure to adjust your security approach to what works in the cloud. Pay attention to configurations. Given the effectiveness of phishing, cloud resources accessible by just a username and password will continue to be at risk.

13 **Adapt your detection methods and defense.** Threat actors have modified their tools, tactics, and procedures to avoid detection. They are using credential harvesting tools to gain legitimate admin credentials so they can "live off the land" as they move through networks. They are using legitimate system tools, like PowerShell, to broadly deploy their tools. They are injecting their malware into running processes instead of writing them to disk to avoid detection by antivirus programs.

14 **Prepare for increased ransom demands.** Towards the end of 2018, we saw changes in the ransomware threat that has continued into 2019. Instead of pushing out commodity malware broadly, threat actors are buying access to environments from other threat actors. When they get into the network, they may find and delete backups before deploying the ransomware to many devices. The threat actors are also paying more attention to identifying their victims and demanding a higher ransom.

Security Risk Assessment Guide

As we've noted before, properly conducted risk assessments will help an organization satisfy the dual goals of improving security and meeting regulatory requirements. But to achieve these goals, clients should address a few key points.

A gap assessment is not enough. A risk assessment must go beyond a mere gap analysis that identifies an organization's vulnerabilities or areas of noncompliance with a framework. To provide value and comply with regulatory requirements, ensure your assessment goes beyond a gap analysis to identify the organization's significant risk scenarios based on the real-world attacks likely to affect the organization and its data.

Define the assessment's methodology. Establish a clear understanding with your assessor of how the assessment will be conducted. Will the assessment be based on interview and document reviews only, or will it include a technical analysis component to validate interview responses? Technical analysis is not always required, but it may be, depending on the assessment's goals and what other recent technical testing the organization has completed.

Ensure the assessment will support prioritized planning. Based on the risk scenarios identified, the assessment should provide concrete recommendations for how the organization can mitigate each risk scenario identified. These recommendations should be prioritized to help drive decisions on information security improvements and spending. An organization can help ensure it gets the expected results by clearly defining deliverables and reviewing sample output before project engagement.

Consider protecting the assessment results. A risk assessment's primary purpose is to help an organization identify its most significant legal, operational, and regulatory risks tied to its information security practices. When an assessment is structured properly, counsel may help protect its results as a component of counsel's overall legal analysis and advice to the organization. There are, though, times when assessment results will not be protected by privilege, including assessments completed to satisfy a regulatory requirement (e.g., a HIPAA risk analysis); assessments deemed to have been completed primarily for a business purpose, not a legal one; and assessments completed for multinational organizations operating in countries that do not recognize a U.S.-style attorney-client privilege.

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

BakerHostetler has more than 970 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 3,500 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, security risk assessment, and class action defense.

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

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

Chair, Privacy and Data Protection Team
Theodore J. Kobus III
New York
T +1.212.271.1504
tkobus@bakerlaw.com

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

Joseph L. Bruemmer
Cincinnati
T +1.513.929.3410
jbruemmer@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 J. 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

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

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

Amy Ralph Mudge
Washington, D.C.
T +1.202.861.1519
amudge@bakerlaw.com

Robert A. Musiala, Jr.
Chicago
T +1.312.416.8192
rmusiala@bakerlaw.com

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

Jaime B. Petenko
Philadelphia
T +1.215.564.2409
jpetenko@bakerlaw.com

Lynn Sessions
Houston
T +1.713.646.1352
lsessions@bakerlaw.com

Randal M. Shaheen
Washington, D.C.
T +1.202.861.1521
rshaheen@bakerlaw.com

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

Eulonda G. Skyles
Washington, D.C.
T +1.202.861.1555
eskyles@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

Anthony P. Valach
Philadelphia
T +1.215.564.2588
avalach@bakerlaw.com

Aleksandra Vold
Chicago
T +1.312.416.6249
avold@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

Sarah (Xiaohua) Zhao
Washington, D.C.
T +1.202.861.1560
szhao@bakerlaw.com

BakerHostetler

bakerlaw.com