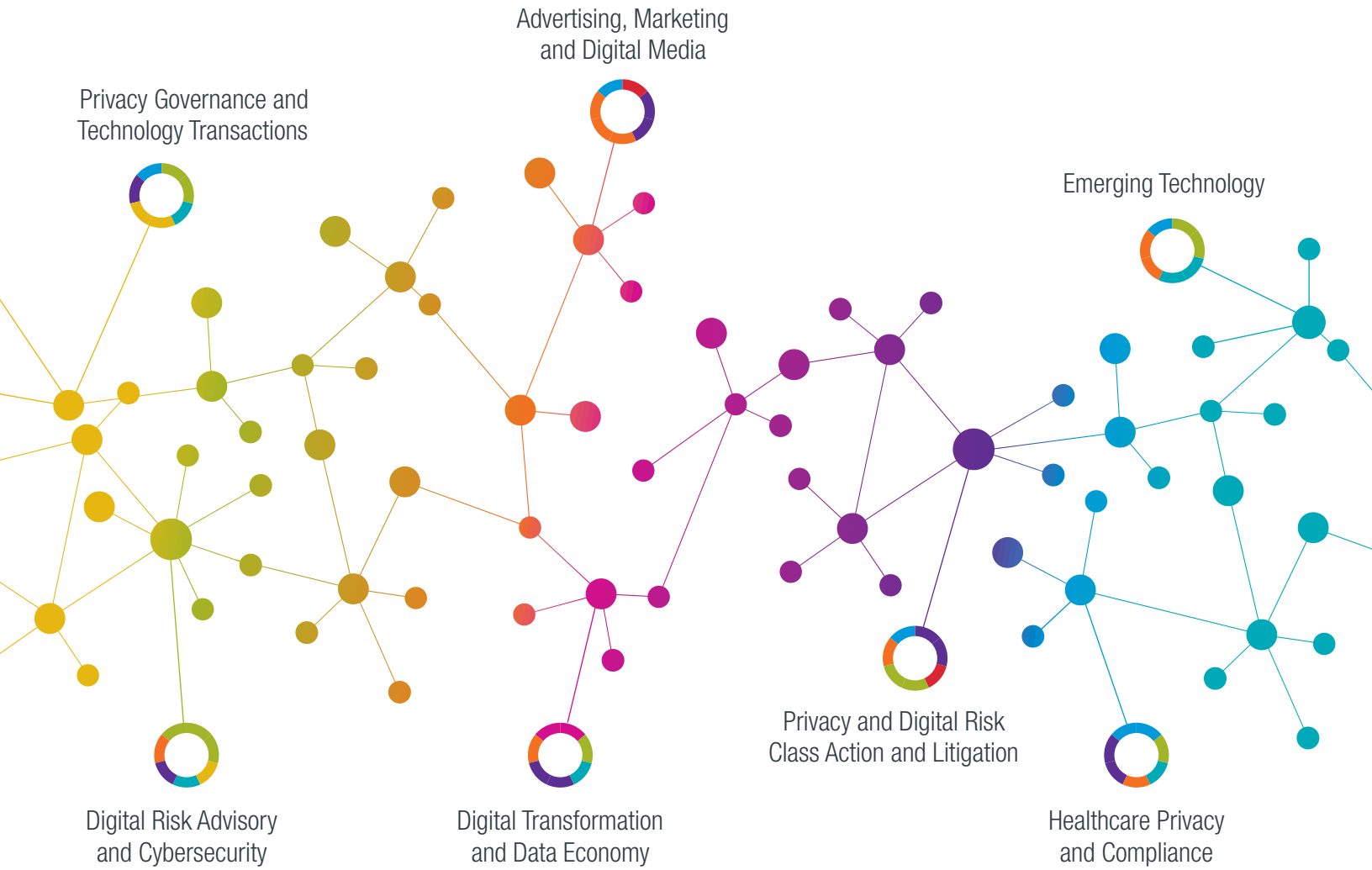
BakerHostetler

2020 DATA SECURITY INCIDENT RESPONSE REPORT

Digital Assets and Data Management – Managing Enterprise Risks and Leveraging Data in a Digital World



Key Findings

Enable MFA already!
Back at the top of our key findings again for many and obvious reasons.

Phishing remains the root of all evil. Training and awareness help. Technology solutions do, too. Both will fail, so you need detection capabilities and an effective triage response plan.

eCrime continues to pay.
Business email compromise schemes to divert wire transfers and ransomware deployments to extort ransom payments accounted for almost half the incidents we managed in 2019.

It's not all about stopping malware. Attacks increasingly involve use of stolen credentials or code executing in memory. Antivirus will not stop those. Defenses have to evolve.

Rise of metrics. Privacy and security are board-level issues. Boards like metrics, so providers and organizations increasingly use them to engage with decision makers on risk-based approaches to these issues.

How fast is as soon as reasonably possible?
Organizations are generally doing well at providing timely notification. Enforcement actions after incidents are rarely based only on notification timing.

Breach fatigue. It is real. But it is not a bad thing. Organizations should be more comfortable communicating quickly and directly with individuals about incidents.

Regulatory investigations.
Regulators do not have time or resources to investigate every incident. Investigations are more likely when there is a state-specific interest, in large matters, in healthcare matters involving more than 500 people, and in outlier incidents. Regulators are asking harder questions and their expectations are evolving.

Business continuity.
The ransomware epidemic brought this previously overlooked cyber risk to the forefront, forcing organizations to align recovery and continuity plans with security incident response plans. Some notification laws include unavailability in the definition of a breach, so understanding what data would truly be unavailable if not accessible is important.

New targets. Ransomware is forcing manufacturing, schools, municipalities, professional services and other industries that were not targets in the past (because they did not have data worth stealing) to prioritize and fund enhancements to their cybersecurity measures.

Small targets. Lawsuits are being filed where the potential class size is smaller – classes of thousands or tens of thousands instead of only millions. Laws with private rights of action like the CCPA will continue this trend.

Big fines generally do not immediately follow new laws.
The threat of large fines drives compliance. But regulators appear to be taking time to observe compliance trends and then going after outliers or targets of opportunity.

Leveraging "compromise threat intelligence" works.
As old causes like lost unencrypted devices dwindle, new risks emerge. Each year there are new tactics, techniques, and procedures (TTPs). Watch for what is happening and adapt.

Detection has improved.
As organizations discover more incidents internally and faster, they are realizing the need to dedicate internal resources to manage incidents.

Reasonable security.
There is still no definitive list. If you do the basics, identify risks specific to your organization and prioritize implementation of measures to address those, and create a governance approach that incorporates security into your operations, you will have a good story to tell.

CONTENTS

We are excited to present our sixth Data Security Incident Response Report (DSIR). We hope this issue finds you safe and healthy while working from home (WFH). Each year, we talk about last year's trends and where we think the current year is taking us. Ransomware was, and continues to be, a big issue. We expect ransomware to continue full speed ahead. We are hopeful, however, that businesses are taking extra care with WFH rules to keep their data secure so that we do not see an increase in breaches due to simple mistakes.

This year, we are reporting on statistics from 950 of the 1,000+ incidents we helped manage in 2019. The incidents we worked on cover all industries and sizes of organizations. Although threats are always changing, we are hopeful that the information we are sharing in the Report will help you and your organization be better equipped to be "compromise ready."

Some of our lawyers have been helping clients manage breaches for more than 15 years. We spend a lot of time onsite with clients and we have grown to understand their operations and the enterprise risks data issues present. Because of that, in January, we elevated our highly regarded privacy, data protection, advertising, and IncuBaker practices and created a practice group dedicated to "everything data" – the Digital Assets and Data Management (DADM) Practice Group. The DADM Group marshals the strength of seven service delivery teams of attorneys with technologists and support professionals to help clients navigate the intersection of digital business, emerging technologies and the law.

Although the DSIR primarily focuses on security incidents, we have also included relevant contributions from all of our DADM teams. Data is everywhere, and every organization is – in some form – a technology company. The DADM Group brings preeminent teams together to provide comprehensive counsel on the full range of complex and evolving issues associated with data and technology, including digital innovation, e-commerce, fintech, cybersecurity, consumer privacy, transactions, governance, risk management, antitrust, and more.

These issues are central to the operations of all organizations, and they are increasingly more regulated. Just like our DADM Group is a one-stop enterprise risk solutions option, this year's Report provides insights on the spectrum of issues in this area. We hope you enjoy the Report and we welcome you to reach out to any one of the DADM Group's members with questions or suggestions.

Sincerely,

Ted Kobus
Chair, Digital Assets and Data Management Group

1,000+

Incidents in 2019

U.S. Breach Notification Law Interactive Map

bakerlaw.com/BreachNotificationLawMap

EU GDPR Data Breach Notification Resource Map

bakerlaw.com/EUGDPRResourceMap

For the latest, visit our blog

dataprivacymonitor.com

Security Considerations for Working Remotely

bakerlaw.com/alerts/security-considerations-for-working-remotely

Incident Response Trends

Top 5 Causes

1. **38%** Phishing
2. **32%** Network Intrusion
3. **12%** Inadvertent Disclosure
4. **8%** Stolen/Lost Device or Records
5. **5%** System Misconfiguration

What Happens Next After Phishing

- **31%** Office 365 Account Takeover
- **24%** Ransomware
- **13%** Installation of Malware
- **13%** Network Intrusion
- **8%** Wire Transfer
- **7%** Theft of Data
- **1%** Cryptomining
- **1%** Espionage

Incident Response Timeline (median)

Occurrence to Discovery	Discovery to Containment	Time to Complete Forensic Investigation	Discovery to Notification
12 Days	**3** Days	**34** Days	**38** Days

Industries Affected

- **23%** Healthcare (including Biotech & Pharma)
- **15%** Education
- **3%** Government
- **17%** Business & Professional Services (including Engineering & Transportation)
- **12%** Retail, Restaurant & Hospitality (including Media & Entertainment)
- **2%** Nonprofit
- **16%** Finance & Insurance
- **11%** Manufacturing
- **1%** Energy

Entity Size by Revenue

> $5B	7%
$1B–$5B	23%
$501M–$1B	11%
$101M–$500M	21%
$10M–$100M	27%
$1M–$10M	10%

Average Forensic Investigation Costs

- **$58,034** All Incidents
- **$65,227** Average Network Intrusion
- **$350,576** Average of 20 Largest Network Intrusions Investigations

Incidents Involving International Reporting

Encryption Key Received and Data Restored After Ransom Paid

Notifications vs. Lawsuits Filed

438 Notifications

14 Lawsuits Filed

Regulatory Inquiries Following Notification

The Ransomware Epidemic

Ransomware surged in 2019, and there is no foreseeable slowdown. All industry segments were impacted. Manufacturing and professional services were particularly hard hit, followed closely by healthcare, education, and government entities. The amount of ransom demanded and actually paid dramatically increased compared to 2018. Toward the end of the year, the epidemic worsened as a new threat actor group (Maze) upped the ante. They started stealing data before deploying ransomware and leaving a ransom note that pointed the victim to a website where Maze published a sample of the stolen data and threatened to release more unless the ransom was paid.

Whether the organization restores from backups or pays to obtain the encryption key, oftentimes it takes organizations weeks, if not months, to return to normal operations.

$18.8 million Largest ransom demand in 2019

$5.6 million Largest ransom paid in 2019 (2018 largest was $250,000)

$302,539 Average ransom payment amount (2018 average was $28,920)

encryption key received after payment made

payment made by third party for the affected organization

73% of the time organization restored from backup or managed without paying ransom

6% of incidents involved unauthorized access or acquisition of data resulting in notification to individuals

Take Action: Address Ransomware Risk

- **Guard against phishing, address security gaps caused by limited utility of antivirus against banking trojans like Trickbot and Emotet, and secure remote access (e.g., open RDP ports).**
- **Enable MFA for the organization and any service providers with remote access.**
- **Evaluate your business continuity and disaster recovery plans and how they integrate with your incident response plan.**
- **Look at your strategy for backups. Current backups, segmented from production systems and easily accessed, can help you avoid business interruption without paying a ransom.**
- **Understand your insurance resources. Think through the hourly impact of downtime in the event you have to decide whether, when, and how much ransom to pay.**
- **Ransomware attacks can also involve access to data that triggers notification obligations – contractual and legal. In the rush to restore systems, some organizations wipe and reimage devices without preserving evidence, which complicates the ability to determine what occurred after the attacker gained access to the network before ransomware was deployed.**

Ransomware Variants

Dharma Ryuk Zeppelin Buran RaaS Bitpaymer Roger Sodinokibi GandCrab SamSam IEncrypt Rapid Mamba Robinhood

Business Email Compromise Is Not Going Away

The FBI began tracking business email compromise (BEC) crime in 2013. Despite increased awareness, security tools, and preventative protocols, BEC incidents continue. Human error remains the leading reason the criminals behind the attacks continue to succeed – employees continue to be tricked by phishing emails into entering their email account credentials or by spoofed emails into changing wiring instructions.

In addition to the potential loss of funds wired to the criminal, the potential liability for being part of the chain that led to a fraudulent wire transfer, and the internal disruption such incidents cause, an organization whose email account was accessed must evaluate whether access to the account triggered contractual or legal notice obligations.

Over 70 %

of the email account access incidents in 2019 resulted in notification to individuals and regulators

of notifications involved a population of under 10,000

had more than one incident in 2019

30+ days longer

to notify than median time to notification for all incidents due to "e-discovery process" to find personal information and match to a mailing address

Take Action: Prevent Account Access and Wire Transfers

- **Properly implemented MFA significantly reduces risk.**
- **Pair MFA with a properly configured Office 365 tenant or G Suite, which includes disabling legacy protocols (e.g., IMAP and POP3) that do not support modern authentication, adjusting SPF/DKIM/DMAR, IP blacklisting where possible, setting alerts for "impossible logins" and creation of forwarding rules, and enabling appropriate logging.**
- **If it is not there it cannot be taken. Use good governance and retention practices to limit what is sent by email and how long emails are retained.**
- **Employee training and awareness – not just training on phishing and social engineering but also the proper use of MFA (if you are not attempting to log in, do not hit "Accept").**
- **Use good out-of-band verification protocols for changing wire instructions.**

Response Timeline – Setting Expectations and Identifying Where to Improve

Organizations feel the pressure to notify individuals and regulators as quickly as possible. They want to be transparent. They also have beliefs about "misses" by other organizations that faced prior incidents. And some are hearing metrics from security teams that measure dwell time, triage, investigation, and remediation in seconds and minutes using security automation tools. Add in other organizational pressures, and you have scenarios where the group responsible for making decisions can feel paralyzed by competing considerations and uncertainty.

Until you have worked through the investigation of an incident, it is hard to appreciate the practical challenges organizations face in quickly and accurately determining what occurred so notification obligation decisions can be made and appropriate communications prepared. Over and over we have leveraged these response timeline metrics to guide clients on setting appropriately aggressive response plans, context for how peers performed, and after the incident is over, to identify opportunities for improvement.

This year we are presenting the mean and median timeline numbers for several reasons. The mean can be misleading due to unusual incidents and the impact of the "e-discovery" process in determining whether email accounts contain personal information. Security firm annual reports also use median values, so this enables our metrics to be paired with theirs more easily. The metrics below are median values.

Detection

Occurrence to Discovery

The network intrusion mean has been around 90 days for years. The network intrusion median of 13 days closely matches the all incident median.

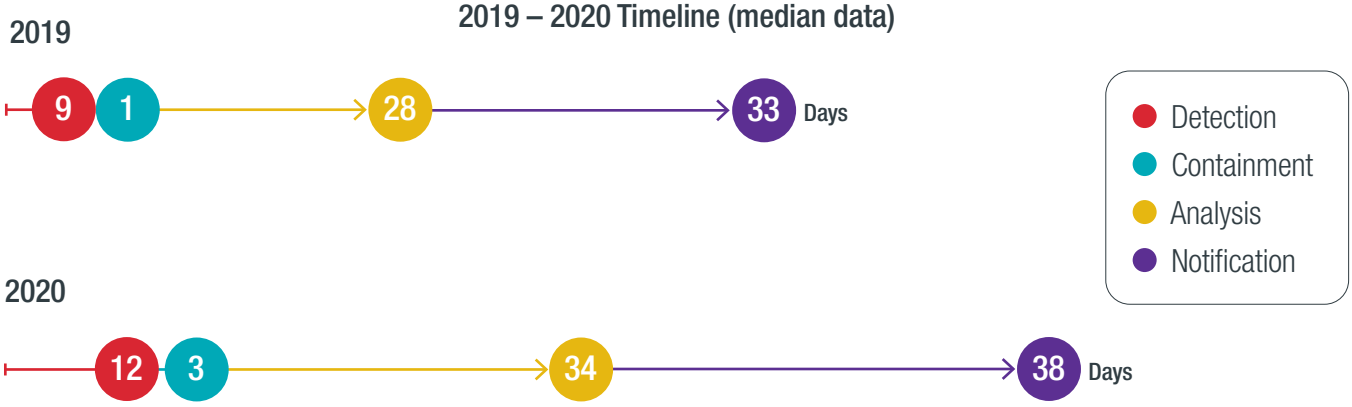
Containment

Discovery to Containment

Although 62% of network intrusion incidents were contained in 7 days or less, the mean slid to 14 days compared to 5 days in 2017 and 10 days in 2018.

2015 – 2018 Lookback (mean data)

2019 – 2020 Timeline (median data)



Analysis

Engagement of Forensics to Completion

34
Days

The mean and median are pretty close here for all incidents and network intrusions. The network intrusion mean was 40 days.

Notification

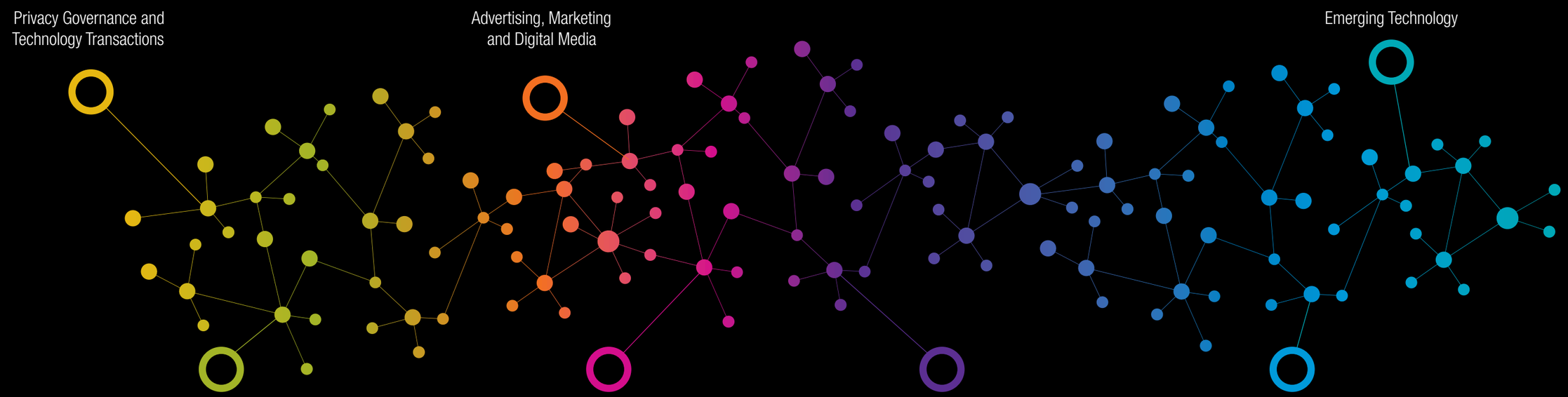
Discovery to Notification

38
Days

The network intrusion median (53 days) and mean (56 days) are a function of how long it takes to identify what occurred and whose information was involved.

The Lifecycle of Data

Transformed legal services for the information and technology ecosystem



Privacy Governance and Technology Transactions

- Assisting clients in capitalizing on the value of data in technology and commercial transactions.
- Working with companies in navigating their digital transformation and data strategies to maximize the commercial opportunities that data provides.
- Establishing rigorous data protection governance programs that leverage privacy compliance as a strategic advantage.

Digital Risk Advisory and Cybersecurity

- Helping clients assess and implement robust and defensible security programs.
- Leading organizations through the response to security incidents and post-notice regulatory investigations.
- Advising and training response teams, executives, and board members on cybersecurity, risk and responsibilities, and incident response.

Advertising, Marketing and Digital Media

- Providing counseling and litigation services in high stakes competitive advertising challenges.
- Defending companies in bet the company enforcement by the FTC and state attorneys general.
- Developing best practices for compliant marketing and promotional strategies across all major commerce and media platforms.

Digital Transformation and Data Economy

- Accelerate: counsel new market entrants when launching products and services by providing IP, transactional, and corporate formation guidance.
- Pivot: maximize the unique value proposition of the existing data assets and find new uses and alternative revenue streams by assessing regulatory restrictions on the use of the data and providing strategic guidance on supply chain and workforce issues.
- Exit: advise on regulatory compliance requirements, data broker and competition law restrictions, and restructuring guidance for sale of data.

Privacy and Digital Risk Class Action and Litigation

- Leveraging extensive experience (procedural and substantive) for early case assessment, modeling, and implementing strategic plans.
- Numerous wins include defeating novel legal theories and avoiding large exposures through orders granting motions to dismiss and denying class certification, as well as through appeals.
- Negotiating creative settlement structures and other cost-effective resolution of matters.

Healthcare Privacy and Compliance

- Advising healthcare entities and business associates on incident response and defending the state and federal regulatory investigations that follow.
- Building HIPAA compliance strategies, training programs, and data strategies for appropriate use of research and other data collected by a covered entity or business associate.
- Advising on international regulations addressing health information, including GDPR for academic medical centers.

Emerging Technology

- Assisting organizations with information governance models generally and their application in support of artificial intelligence.
- Advising organizations on the use of blockchain and related digital ledger technologies.
- Applying emerging technologies to the practice of law on behalf of clients and their counsel, including assistance with building data lakes, conducting data analytics, and using artificial intelligence to support legal processes.

Forensics Drive Key Decisions

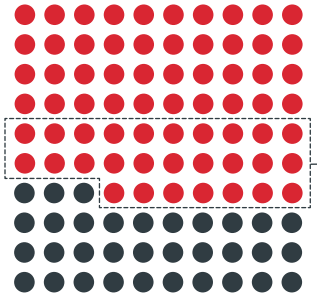
Regulatory obligations and perceived expectations continue to drive increasingly faster security incident disclosure (sometimes within 72 hours). So an effectively scoped and well-executed forensic investigation can help you bring an end to an attack, determine appropriate notifications, and stave off or support the defense of regulatory investigations and lawsuits.

In 2019, organizations used digital forensic investigation firms in 72% of overall incidents, a 7% decrease from 2018. This drop may be attributable to:

- more ransomware incidents affecting organizations with insufficient resources to recover forensic data;
- less availability of Microsoft Office 365 extended activity logging in the context of business email compromise investigations; and
- greater use of advanced endpoint monitoring solutions and security incident and event management (SIEM) tools in the SME and upper-middle markets.

However, most organizations lack the capacity, skillsets, advanced tools and/or experience to conduct an adequate forensic investigation without third-party assistance. Boards of directors and executives continue to engage leading forensic firms to satisfy scrutiny from regulators and external auditors.

The average cost of all investigations dropped from $63,001 to $58,034; the average cost of network intrusion investigations dropped from $120,732 to $65,277 – possibly because forensic firms have started using less expensive solutions like automated triage scripts and endpoint detection and response solutions for post-ransomware investigations in lieu of costly imaging, log, and malware analyses.



642 of 950
investigations used forensics

259 of 642
resulted in notification to individuals

78% of the data breaches in this year's survey were discovered internally (4% more than last year).

Take Action: Help Forensics Work for You

- **Don't wait to engage with a forensic firm. Contract negotiations can drastically reduce response time, so identify and engage a firm before an incident occurs. A retainer agreement with a guaranteed response time is an option, but even just pre-negotiating the MSA will save valuable time.**
- **Update data maps and system inventory. If you don't know where data is stored and how it flows across your network, it's harder for a forensic firm to help you. In addition, an updated data map and system inventory are necessary components of GDPR and CCPA compliance.**
- **Evaluate log retention periods. 50% of forensic investigations involve log review. Average dwell time is months, not days. So if your network logs only go back days or a few months, you could be missing critical data.**
- **Conduct a full backup and restoration test. Available backups are still your best weapon against ransomware. However, backups must be tested to ensure all necessary data is being fully backed up. Restoration testing will reveal how long it will take to fully recover from a ransomware infection.**

Litigation Continues to Evolve

Showing Harm Still Key Issue

Demonstrating harm and damages remains the key issue. To avoid it, some plaintiffs rely on laws providing statutory damages, like the CCPA. Otherwise, plaintiffs have concentrated on three claimed injuries to demonstrate classwide harm: (1) the inherent value of personal information; (2) overpayment based on an alleged failure to deliver data security or privacy as part of the service or product; and (3) the cost of future credit monitoring and identity theft protection.

These alleged injuries continue to receive varied treatment by federal and state courts. A March 2019 ruling allowed for federal standing based on an alleged increase of future identity fraud, denied federal standing based on an alleged overpayment or the claimed inherent value of personal information, and left questions regarding the viability of plaintiffs' claims under state law to be decided at a later time. In June 2019 the D.C. Circuit allowed for Article III standing based on an alleged increased risk of identity fraud in the litigation over the Office of Personnel Management data breach.

14 lawsuits filed related to incidents disclosed in 2019 (compared with 4 in 2018)

- **4** lawsuits arose from incidents that started with unauthorized access to Office 365 inboxes
- **2** lawsuits involved payment card data
- **9** lawsuits involved SSNs
- **8** lawsuits involved classes of 100,000 or fewer of individuals notified who had data meeting the definition of personal information under state notice laws or PHI under HIPAA (6 were less than 10,000)

Plaintiffs Unable to Certify Classes

We are aware of three class certification decisions in 2019, all favorable to defendants:

- The Middle District of Alabama denied certification of a putative issuer bank class following an alleged payment card security incident at retail store Fred's. The court held that individualized issues of causation and damages as well as choice of law predominated over common questions.
- A Georgia state court denied class certification based on lack of commonality in a case against Piedmont Athens Regional Hospital. The court held that the likelihood of individualized damages inquiries and the effect on individual patients precluded classwide adjudication.
- The Northern District of California held that neither the request for the remedy of future credit monitoring nor the reduced value of stolen personal information was a cognizable injury in a case against Facebook over a September 2018 data breach. The ruling certified an injunctive relief class, allowing consumers to sue as a group to require Facebook to employ more robust data security and privacy precautions.

Settlement Trends

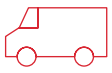
Most cases that survive motions to dismiss settle before the court rules on the plaintiffs' motion for class certification. A data security settlement described as "the largest and most comprehensive recovery in a data breach in U.S. history by several orders of magnitude" has been appealed by noted objectors, including one whose appeal from a cy pres settlement with Google recently reached the Supreme Court.

State Privacy Laws

The California Consumer Privacy Act (CCPA) contains a well-publicized private right of action that lets California residents seek statutory damages from companies that have suffered a data security incident as a result of failing to implement "reasonable security procedures and practices." So far, we have not seen the predicted deluge of new putative class actions brought under the CCPA, as most commentators predicted. At least 16 states have also introduced legislation similar to the CCPA. This increased activity in state legislation will be a critical area to watch for new developments in data privacy law in 2020 and beyond, that will continue to impact data security and privacy litigation as well.

Using Compromise Threat Intelligence to Be Prioritized, Agile, and Resilient

If your threat intelligence efforts only focus on what is next, you may overlook well-known, constant threats. Effective use of compromise threat intelligence (looking at what is actually causing incidents at other organizations) means identifying what allows the known to continue to be successful in addition to trying to see around corners. Doing both is part of having an agile, resilient security posture. Encryption mostly stopped notifications about lost/stolen unencrypted devices, and awareness slowed the scourge of W-2 phishing. While the methods of initial compromise (e.g., phishing) have remained constant, the TTPs of what happens next (privilege escalation, reconnaissance, lateral movement, outcome) continue to evolve. What knowns will continue and what will threat actors do next?



"Supply chain attacks" By gaining access to a managed service provider, a threat actor can access a single client environment or impact most of the MSP's client base, by either taking data or deploying ransomware.

Payment card attacks have occurred for over 15 years. Wider deployment of P2PE has slowed the pace of successful card present attacks, and EMV has made it harder to use counterfeit cards. As predicted, theft of card data from online transactions has increased. Tokenization and iframe solutions help, but there are still potential attack surfaces (e.g., code injection).

Bypassing MFA Whether it is because legacy protocols that do not support modern authentication are not disabled or a distracted employee hits "Approve" when the threat actor attempts to log in, enabling MFA is not a cure-all.

Ransomware Of course, this will increase. Why? It is working. The average ransom paid by our clients increased from $28,920 in 2018 to $302,539 in 2019. Expect more threat actors to take data before deploying ransomware and then pair the ransom demand with an extortion threat. Expect demands to increase, too.

Phishing A leading security firm reported in its 2020 trends report that phishing was the most common method for gaining access to an organization – just as it has been reporting since 2010.

Business email compromise Whether by accessing an email account or using a spoofed email domain, business email compromise will continue. Email accounts that can be accessed online with just a password and banking trojans like Trickbot and Emotet are contributing factors. So are employees who continue to be tricked.

Insider threats? Incidents attributed to malicious insiders remains a very small percentage of all reported incidents. Will security automation detect more incidents by insiders?

Rise of e-crime threats The availability of botnets and effective open-source toolkits will continue the increase in "crimeware" fueled incidents such as credential stuffing, theft of payment card data, credential harvesting to sell access, selling stolen personal information, and deployment of ransomware. Organizations need a plan for addressing phishing leading to installation of banking trojans and post-exploit use of programs like Mimikatz and PowerShell (hint: antivirus is not the plan).

Account takeovers followed by monetization of assets (e.g., loyalty point redemption, use of stored payment methods) will continue.

Take Action: Stop Account Takeovers

Hundreds of millions of username and password combinations have been taken and are available online. A threat actor can use a botnet to script out rapid-fire testing of credentials against online accounts and mobile apps. Because people re-use passwords, some of the attempts work. The threat actor then attempts to use the access for financial gain, often by using a stored payment card to make a purchase or by redeeming accumulated loyalty points. This should not be considered a "breach." And organizations are motivated to stop them because of the fraud loss impact. But it can be a frustrating game of whack-a-mole. These options can help stop ATOs:

- **Risk assessment/threat modeling – evaluate the data collected, processes a threat actor may exploit, and design appropriate controls. But account for customer friction (e.g., not all users want or can use MFA).**
- **Privacy by design – use data minimization (e.g., just collect month and day of birth not the year) and do not store or truncate data elements covered by breach notification laws.**
- **Strong security measures – use a web application firewall to prevent bot traffic. Use secure coding practices and assess the app using standards like the OWASP Top 10.**
- **Account creation measures – consider email validation before opening a new account.**
- **Baseline detection and prevention measures – (1) rule-based prevention measures, such as velocity checks; (2) a strong password policy approach; (3) requiring a unique username instead of an email address; and (4) use of a reCAPTCHA.**
- **Digital identity-based authentication – device/user recognition solutions that may include behavioral analytics to facilitate risk-based authentication.**
- **Authentication options – offer MFA as an option for user to enable, a second passcode feature option for user to enable to enter after log-in, integration with SSO options like Sign in with Apple, hardened password reset process, or stepped-up authentication options based on risk.**
- **Fraud analytics – build a dedicated team to monitor account authentication and fraud patterns, spot trends, and develop mitigation tactics to address changing threat tactics.**
- **Monetization incentive reduction – identify what threat actors are targeting and change program features to reduce ease of monetization (e.g., impose a delay on redemption or shipping of reward, offer internal redemption instead of a prepaid gift card or require presentation of actual gift cards in person for redemption).**
- **Customer awareness – notify users of important changes to accounts (e.g., when a password or shipping address is changed or a new payment method is added) and develop a protocol for notifying customers of ATOs (e.g., prepare template notification emails).**
- **Threat intelligence – develop internal options (e.g., check credentials against haveibeenpwned.com site) or use a vendor to monitor the dark web for availability of credentials and monetization efforts.**

OCR Investigates Often, but Collects Lower Amounts in Settlements

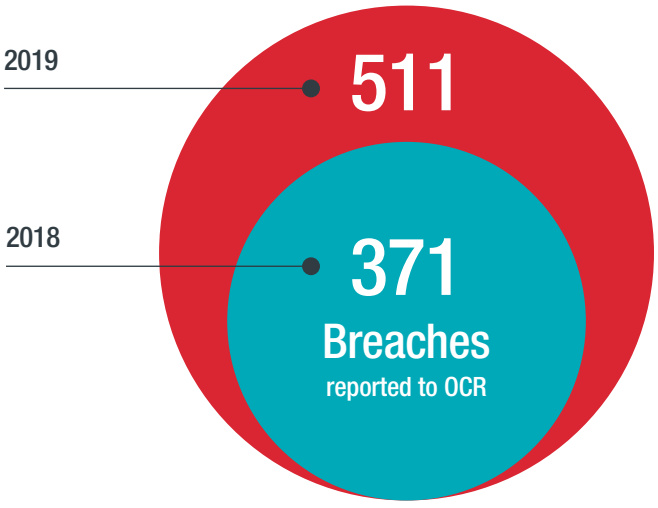
HIPAA-covered entity breaches continued to draw attention from the Office for Civil Rights (OCR) and other regulators in 2019. Any HIPAA breach that involves 500 or more individuals will certainly bring an OCR data request. While these investigations can be burdensome and costly for organizations to respond to, few of them actually result in a penalty to the entity. Of 511 breaches of 500 or more individuals reported in 2019, the OCR assessed penalties in only 11.

The amount of total penalties also decreased significantly in 2019, likely due to the OCR's April 2019 discretionary enforcement decision lowering the cap on dollar amounts it could obtain as a penalty for a particular HIPAA violation in a calendar year. The OCR now bases amounts on the level of culpability, with four levels from least culpable (no knowledge of the violation) to most culpable (willful neglect/not corrected), and the annual limits are $25,000, $100,000, $250,000 or $1.5 million, respectively.

Based on current investigations, we expect that the OCR will end up "gaming" the system to push more incidents to the highest culpability tier and/or stack more HIPAA violations per incident. The OCR may also push more investigations to state attorneys general (AGs), who continued to bring HIPAA enforcement actions in 2019. More state AGs are initiating investigations, often starting before an OCR data request arrives.

Most OCR investigations continue to focus on HIPAA Security Rule compliance with deep dives into security risk analyses and risk management plans. The OCR has publicly stated that it expects there is a lot of low-hanging fruit with HIPAA compliance, which is borne out in our experience. For example, recent OCR guidance takes a more aggressive stance on what was thought to be a well-settled interpretation of the Four Factor Risk Assessment for covered entities. We expect to see more investigations, more enforcement actions, and aggressive positions taken by the OCR in this area.

Breaches of 500 or more individuals



11 incidents
where the OCR penalized entities in 2019

$15.27 million
in total penalties in 2019 (ranging from $10,000 to $3 million)

10 incidents
where the OCR penalized entities in 2018

$28.7 million
in total penalties in 2018

Source: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Create a Compelling Security Story

Organizations heard a lot about "reasonable security" in 2019. But many feel no closer to answering these key questions: What exactly is it, and when have they done "enough"? There is no single answer to these questions – the requirements have to work for organizations of different sizes and circumstances – but there is a common process that any organization can use to create a compelling story for regulators and litigants about how it approaches and implements data protection.

The roots of reasonable security obligations are: (1) years of Federal Trade Commission (FTC) enforcement actions alleging unfair or deceptive practices tied to alleged unreasonable security practices; (2) Article 32 of the EU's GDPR mandate of "appropriate technical and organizational measures to ensure a level of security appropriate to the risk;" and (3) U.S. state laws. Against this background, organizations must develop a plan to define, implement, and maintain reasonable security. It may not be as simple as implementing the Center for Internet Security's Critical Security Controls (CSCs) (as many have suggested, pointing to a 2016 report from the California Attorney General). A robust security program – and one that allows an entity to articulate reasonable security to regulators and litigants – requires a combination of good governance, a proper risk assessment, and tailored controls.

- You can't protect something if you don't know what it is and where it is. Data protection efforts must begin by understanding what data the organization has, how it's processed, what third parties it's shared with, and the regulatory obligations it triggers.
- Conduct and then base your controls on a proper risk assessment. No organization can implement every conceivable control. Use a risk-based selection process to select controls. This is different than a gap or maturity assessment (neither show how controls were prioritized by risk). The framework must also be broad enough to cover all applicable technical, administrative, and physical controls (this is why the CSCs alone may not be enough). Combining the CSCs and the NIST Cyber Security Framework is a good starting point.
- Maintain your controls through good governance. A reasonable data protection program is more than a point-in-time exercise. It requires ongoing evaluation and review by a dedicated committee tailored to the organization's size and complexity. The committee should review assessment results to evaluate how identified risks were addressed, identify new risks based on emerging threats and new initiatives (e.g., moving data to the cloud), and document data protection actions to support a defense (if needed). Ideally, this work will evaluate privacy and security risks together.
- Address security requirements across all applicable regulations. With proper planning and oversight, an organization can articulate its definition of "reasonable security" and prepare a compelling story to defend against the state, federal, and international regulatory inquiries or litigation.

2019: What Changed?

The requirement to maintain reasonable security is not new. But 2019 saw an increased risk of penalties and litigation tied to unreasonable security practices:

California
The CCPA's private right of action allows an individual whose information was involved in a data breach to sue a data owner for statutory damages if the breach resulted from a failure to maintain reasonable security.

EU
After a year of relative calm, supervisory authorities began penalizing companies in earnest for deficient security measures following GDPR breaches and audits.

United States
Across the United States, state legislatures enacted laws requiring reasonable security and giving regulators more enforcement authority.

FTC
The agency formulated a new framework for enforcing reasonable security in its consent orders, promising aggressive future enforcement.

Blockchain and Self-Sovereign Identity

Blockchain supports the emerging field of self-sovereign identity (SSI), an Internet-based credential transfer and storage. Here the majority of identity verification uses peer-to-peer decentralized identifiers (DIDs) containing no personal data. DIDs use private blockchains that underpin authenticity and validity, but personal data is stored separately in another type of decentralized database. SSI therefore offers a potential path to replace centralized databases with methods that are much more difficult to attack.

Research & Development, IncuBaker, and New Client Demands

Recent client demands have focused on data analytics, machine learning, natural language processing, and smart legal contracts associated with the following interests:

Computational linguistics for drafting in litigation

Contract analytics for due diligence review and lease abstraction

Intelligent automation for agreements (such as NDAs) **and customized workflows**

Automated patent drafting for attorneys and agents

Westlaw Edge, Bloomberg Law, Docket Navigator, and other sources of judicial analytics

Robotic process automation for business transformation (such as onboarding, augmented research, and workflow efficiency)

Chatbots

We've also seen an increase in the following:

Introductions to legal technology designed to educate practitioners and illuminate the right technologies for bespoke use cases in a crowded legal technology marketplace

Current state assessments with specific questions to guide discussions and process mapping

Facilitation of process vision sprints to guide clients to define and gain their desired end states

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

BakerHostetler is a leading law firm recognized for client service that helps organizations around the world address their most complex and critical business and regulatory issues. Our Digital Assets and Data Management Practice Group (DADM) is a multidisciplinary team of highly regarded attorneys advising clients on all things related to data and technology. We have united key service offerings and technologists to address all the risks associated with an entity's digital assets. Our clients are collecting data and then utilizing advanced technology to transform their products and services. Doing this creates enterprise risk. We work with our clients through the life cycle of data – privacy, security, marketing and advertising, transactions, and emerging technology.

Chair, DADM Practice Group
Theodore J. Kobus III
New York
T +1.212.271.1504
tkobus@bakerlaw.com

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

DADM Practice Group Teams

Digital Risk Advisory and Cybersecurity

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

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

Advertising, Marketing and Digital Media

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

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

Privacy Governance and Technology Transactions

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

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

Digital Transformation and Data Economy

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

Chad A. Rutkowski
Philadelphia
T +1.215.564.8910
crutkowski@bakerlaw.com

Jeewon Kim Serrato
San Francisco
T +1.415.659.2620
jserrato@bakerlaw.com

Healthcare Privacy and Compliance

Lynn Sessions
Houston
T +1.713.646.1352
lsessions@bakerlaw.com

Privacy and Digital Risk Class Action and Litigation

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

Emerging Technology

Katherine Lowry
Cincinnati
T +1.513.852.2631
klowry@bakerlaw.com

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

Office Practice Coordinators

Atlanta and Orlando

Janine Anthony Bowen
T +1.404.946.9816
jbowen@bakerlaw.com

California

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

Chicago

Aleksandra Vold
T +1.312.416.6249
avold@bakerlaw.com

Denver

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

Houston

Lynn Sessions
T +1.713.646.1352
lsessions@bakerlaw.com

New York

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

Ohio

Craig A. Hoffman
T +1.513.929.3491
cahoffman@bakerlaw.com

Philadelphia

Daniel A. Pepper
T +1.215.564.2456
dpepper@bakerlaw.com

Seattle

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

Washington, D.C.

Eulonda G. Skyles
T +1.202.861.1555
eskyles@bakerlaw.com

BakerHostetler

bakerlaw.com