BakerHostetler

2021 DATA SECURITY INCIDENT RESPONSE REPORT

Digital Assets and Data Management – Disruption and Transformation

Key Findings

Did we say, "Enable MFA"? It bears repeating. And not just for email—add a second authentication factor where sign-in gives access to sensitive data, source code, or critical operational services.

IAM/PAM (identity access management and privileged access management). Are these on your road map?

C-SCRM? Cybersecurity – supply chain risk management. Read the events in the news and layer in technology usage trends, and it's obvious why this long-standing challenge is even more important to address.

Attorney-client and work product. Establishing and preserving these for forensic investigations of security incidents remains a challenge. Focus on separating underlying facts from communications regarding advice.

Zero-trust: strategic priority or fad? If you define it as assume a breach and implement a defense-in-depth approach, it should be a priority.

Old data. Get rid of it. Old data on a file server is the most common source of notice obligations in ransomware matters.

Phishing training. Phishing is still prevalent, so are awareness training and measures like marking emails as from an "external sender" making a difference?

Endpoint detection and response (EDR). It is hard to argue against the need for an endpoint threat detection and response tool.

eCrime continues. From wire transfer schemes (the first 48 hours is the critical time for seeking recovery) to W2 phishing to fraudulent unemployment claims to payment card data theft (with a rise in e-commerce and slowing of card present theft).

What are meaningful cybersecurity metrics for boards? Boards need to know more than the patched vulnerability counts and number of pings dropped by a firewall to properly oversee the management of a cybersecurity program.

Disruption. Pandemic- and technology-driven changes occurred.

CCPA. The Biometric Information Privacy Act (BIPA)-like flood of California Consumer Privacy Act (CCPA) lawsuits that was widely expected has not yet materialized.

Ransomware scourge. Entities are still being victimized and paying ransoms for decryption keys and to avoid the publication of exfiltrated information.

Small actions. The trend of filing lawsuits over small incidents continued, especially in notifications to current and former employees involving theft of Social Security numbers (SSNs).

CONTENTS

02 At A Glance
04 Why Incidents Occur
06 Incident Response Life Cycle
07 Forensics
08 Litigation
10 Work From Home/ Information Governance
11 Vendor Incidents
12 CCPA
13 EU Regulatory Update
14 Healthcare
15 Advertising, Marketing and Digital Media
16 Security

Welcome to our seventh Data Security Incident Response Report (DSIR). It has been quite a year from many perspectives. Thank you to everyone we have continued to partner and work with to create this report.

We are excited to soon launch a new digital platform version, and we intend to update this version throughout the year with real-time data. The DSIR will continue to share data and insights about security incidents, regulatory enforcement actions, class actions, transactions, digital innovation, compliance projects, data governance, and advisory matters to help organizations develop solutions to address the issues that data and technology create.

We kicked off 2020 with the formation of a practice group focused on "everything data"—the Digital Assets and Data Management (DADM) Practice Group. At that time, no other law firm had prioritized these issues on the practice group level. We had big plans associated with the launch of DADM, and like those of everyone else, our plans for 2020 were disrupted. Fortunately, however, the members of our group quickly pivoted to meet the evolving needs of our clients. Also, the timing of our launch was fortuitous. Before the pandemic, it was already a cliché to say that every company is in some way a technology company. This is definitely the case after COVID-19 due to remote working and the temporary closure of brick-and-mortar businesses.

The DSIR we published in April 2020 anticipated some of the work-from-home challenges due to the pandemic. Our teams went from spending a significant amount of time on-site with clients to learning how to engage, advise, and train through videoconferencing. We scrapped a six-month effort to have a vendor build us a custom data security incident case management solution and, instead, had our IncuBaker legal technology team build it using existing resources. We saw some (but not many) incidents occur due to the rush to support remote work. In the summer and fall, we faced a surge of ransomware matters. Then, we definitely experienced an impact from the pandemic (in practical ways, such as dependence on technology that was not available heightening the need to pay a ransom and challenges in collecting evidence to do an investigation). Collaboration, teamwork, and resilience, helped us face these pandemic-driven obstacles and solve problems.

It would not be appropriate to discuss the past year without also addressing systemic racism and inequities seen across underrepresented minority groups. Diversity, equity, and inclusion are priorities for our practice, and significant time has been spent by leaders in our group to address these issues as part of our strategic planning. Law firms generally still have a lot of work to do in this regard; however, it is worth noting that: over 50% of our practice group is composed of female lawyers, nearly 30% of our lawyers are persons of color or LGBTQ+, and women and persons of color hold over 70% of our group's leadership positions. We will continue our commitment to not only hiring lawyers and staff from underrepresented groups but also integrating them into our group once they are hired so that they have a successful path forward.

We hope you enjoy this edition of the DSIR, and we welcome you to contact our DADM group members with questions or suggestions.

Sincerely,

Ted Kobus
(He | Him | His)
Chair, Digital Assets and Data Management Group

1,250+

Incidents in 2020

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

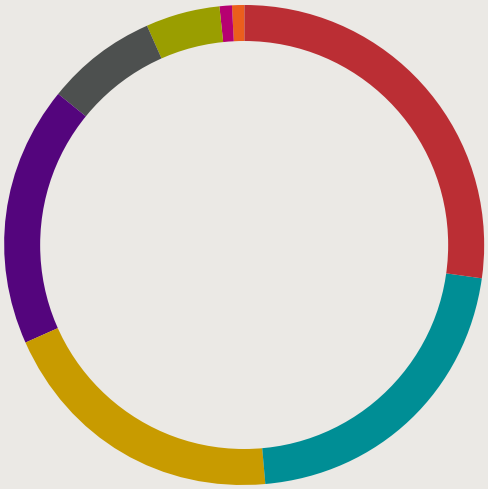
bakerdatacounsel.com

Incident Response Trends

Top 5 Causes

1. **58%** Network Intrusion
2. **24%** Phishing
3. **6%** Inadvertent Disclosure
4. **6%** Stolen/Lost Devices or Records
5. **4%** Access to Cloud Asset

What Happens Next After Phishing

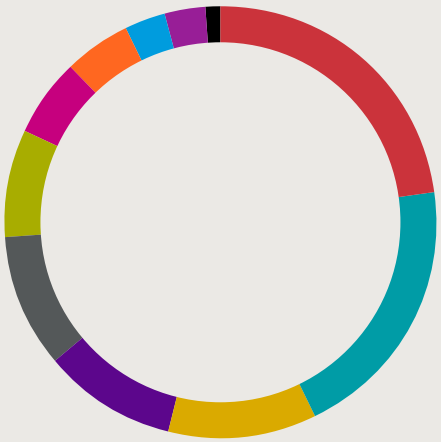


- **33%** Network Intrusion
- **26%** Ransomware
- **24%** Theft of Data
- **21%** Office 365 Account Takeover
- **9%** Installation of Malware
- **6%** Wire Transfer
- **1%** Cryptomining
- **1%** Espionage

Incident Response Timeline (median)

12	0	36	66
Days	Days	Days	Days
Occurrence to Discovery	Discovery to Containment	Time to Complete Forensic Investigation	Discovery to Notification

Industries Affected



23% Education

10% Business Services

3% Professional Services

20% Healthcare (including Biotech & Pharma)

8% Retail, Restaurant, & Hospitality

3% Technology

11% Manufacturing

6% Nonprofit

1% Energy

10% Finance & Insurance

5% Government

Entity Size by Revenue

> $5B	5%
$1B–$5B	15%
$501M–$1B	16%
$101M–$500M	17%
$11M–$100M	23%
$1M–$10M	25%

Average Forensic Investigation Costs

$55,960 All Incidents

$75,289 Network Intrusion Incidents

$464,234 20 Largest Network Intrusion Incidents

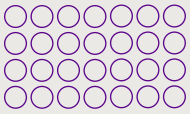
Incidents Involving International Reporting

Average Ransom Paid

$794,620

Notifications vs. Lawsuits Filed

543 Notifications



20 Lawsuits Filed

Regulatory Inquiries Following Notification

The Scourge of Ransomware

Ransomware matters surged in 2019, with the primary tactic being to encrypt as many devices in the network as possible simultaneously. Then the Maze group changed tactics in late 2019 – it began stealing data before encrypting data. This gave the group two pressure points and caused companies to pay ransoms, even when they restored using backups, in order to prevent disclosure of stolen data. It did not take long for dozens of other threat actors to adopt this tactic. And like a gambler using a large stack of chips to buy the pot, these groups were emboldened by their wins to increase their initial demands, sometimes by tens of millions of dollars.

In October 2020, the Department of the Treasury issued an alert reminding companies to address sanctions obligations before making ransom payments. The alert caused confusion and added more hurdles (e.g., subjective requirements demanded by a company's bank before it would wire money to the payment facilitator).

75
threat actor groups/variants (15 in 2019)

Clop Netwalker Conti Ryuk Pysa

$65+ million Largest ransom demand in 2020 (2019 was $18 million)

$15+ million Largest ransom paid in 2020 (2019 was $5+ million)

$794,620 Average ransom payment amount (2019 average was $303,539)

98% encryption key received after payment made

99% payment made by third party for the affected organization

67% of the time an organization was able to partially or fully restore from backup without paying ransom

70% of ransom notes contained claim of theft of data before encryption

90% found evidence of data exfiltration when there was a claim of data theft in the ransom note

25% involved theft of data resulting in notice to individuals

20% of matters involved a payment to a threat actor group even though the organization had fully restored from backup

8 Days
From demand to payment (median: 5)

9.2 Days
From demand to payment for payments over $1 million

7.4 Days
From demand to payment for payments $200,000–$1 million

13 Days
From encryption to restoration (median: 10)

Industries Affected

	AVERAGE INITIAL RANSOM DEMAND	AVERAGE RANSOM PAID	DAYS TO ACCEPTABLE RESTORATION	FORENSIC INVESTIGATION COST	INDIVIDUALS NOTIFIED
Healthcare	$4,583,090 (median: $1.6 million)	$910,335 (median: $332,230)	4.1 (median: 0)	$58,963 (median: $25,000)	39,180 (median: 1,270)
Manufacturing	$4,375,287 (median: $800,000)	$1,403,876 (median: $246,997)	5.7 (median: 0)	$51,957 (median: $29,463)	1,257 (median: 148)
Financial Services	$1,360,833 (median: $435,000)	$1,146,170 (median: $432,500)	2.7 (median: 0)	$32,951 (median: $19,500)	8,048 (median: 109)
Hospitality	$1,006,391 (median: $675,000)	$642,588 (median: $416,500)	4.9 (median: 0)	$68,513 (median: $35,750)	308,205 (median: 250)

Take Action

- **Focus on the basics with defense in depth.** One or more of these three circumstances was present in every ransomware event of impact: no EDR, ineffective backup solution/implementation, open remote desktop protocol (RDP).
- **Use compromise threat intelligence to identify tactics.** Some groups use one entry point as their go-to attack method (e.g., an unpatched firewall appliance).
- **Pay attention to your backup plans.** Know where they are stored, what they back up, and what it takes to use them to restore.
- **Address other pressure points.** Use data governance and hygiene practices to limit easily available sources of data (e.g., find file servers and clean up historical data that is no longer needed or that was inadvertently stored).

Email account compromises to facilitate wire transfer fraud (BECs) are still happening

$26 million	$453,468	$6 million	$758,365	28%
In wire transfers resulting from a BEC	Average wire transfer	Largest wire transfer	Average recovery	Matters that had recovered funds totaling over $12 million

One area where we definitely saw the impact of the pandemic and working from home (WFH) was the response timeline.

Detection

Occurrence to Discovery

12 Days

The mean was 92 days for network intrusions compared to 70 in 2019 and a prior three-year mean of 87 days.

Containment

Discovery to Containment

0 Days

The mean was 6 days for network intrusions compared to 10 days in 2019 and a prior three-year mean of 5 days.

Analysis

Engagement of Forensics to Completion

36 Days

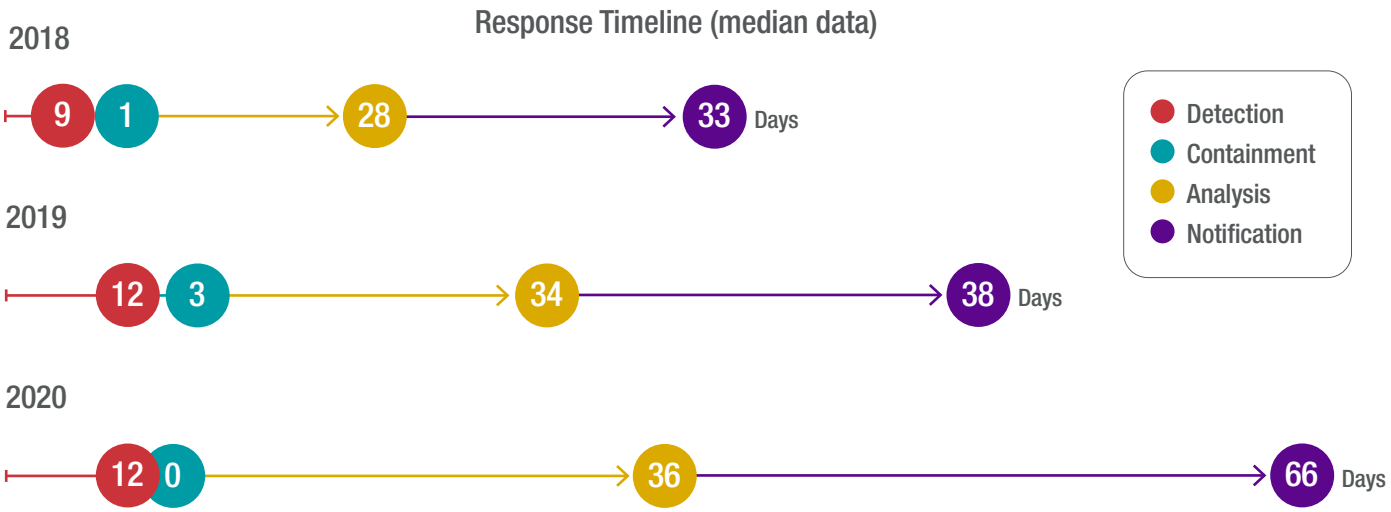
The mean was 42 days for network intrusions compared to 44 in 2019 and a prior three-year mean of 36 days.

Notification

Discovery to Notification

66 Days

The mean was 90 days for network intrusions compared to 60 days in 2019 and a prior three-year mean of 49 days.

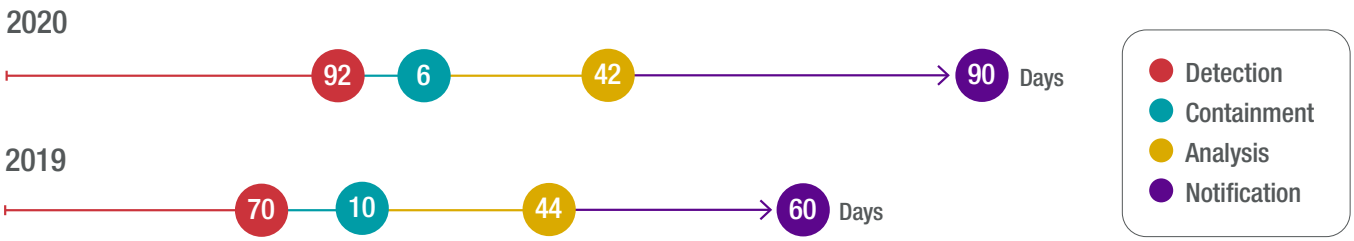


The pandemic disrupted the way organizations operate, and responding to data security incidents was no exception. With the continued surge of ransomware matters and the impact of large supply chain matters, the capacity of the incident response industry was stretched thin. Organizations worked to quickly contain incidents (despite challenges in simply getting passwords changed and EDR tools deployed to remote workers). Organizations with international operations contended with cross-border and regional restrictions on personnel movement. Getting access to facilities to obtain forensic images was a challenge. Necessity drove creative solutions.

Average Forensic Investigation Costs

$55,960	All Incidents
$75,289	Network Intrusion Incidents
$464,234	20 Largest Network Intrusion Incidents

Network Intrusion Timeline (median data)



EDR tool use growing but not yet widespread

An EDR tool can help detect and contain the initial foothold established on a device through phishing, social engineering, or exploitation of a vulnerability. Multiple investigations in 2020 involved quick analysis of incidents identified by an EDR tool at a phase that was right before theft of data and deployment of ransomware. EDR tools include FireEye's endpoint agent, CrowdStrike Falcon, Carbon Black, and Microsoft Defender ATP. Only approximately 10% of clients that faced a network intrusion in 2020 had a fully deployed EDR tool at the time of the incident. However, many of the related investigations used an EDR tool, and those clients often continued using the tool (or a different EDR solution) after the incident.

Take Action: Adapt to Survive

- **Consider an EDR tool.** Threat actors know how to evade traditional antivirus programs. EDR tools use behavior-based detection models to identify unauthorized activity that traditional antivirus does not detect.
- **Protect your backups.** Backups ideally should be stored off your network, should be accessible only through unique credentials that aren't used to access anything else, and should be given a name that hides what they are. The "backup" server is a sure target for threat actors.
- **Make sure you can remotely manage your devices.** We're in a WFH world. If you have an incident, there's a good chance you'll need to deploy an EDR tool to all of your endpoints to aid in containment and investigation. You may also have to execute an enterprisewide password reset. If you can't remotely manage your devices, the time to complete these tasks increases significantly.
- **Don't go it alone.** Internal IT teams can be overwhelmed in the early days of an incident. There are firms that specialize in providing emergency "helping hands" support to companies in these situations. From resetting passwords to building segmented networks for restoration purposes and executing tasks to support containment, they can relieve internal resource constraints, shorten the time to recovery, and minimize the demand on your IT team.

Smaller Data Breach Class Actions Proliferate

A trend we saw in 2019 continued in 2020 – lawsuits being filed over small incidents (where 100,000 or fewer individuals were notified). Most were filed by a handful of plaintiff firms. These cases often have a regional population, so they are often brought in state courts and pled in a way that prevents removal to federal court.

These plaintiff firms are filing more cases and then seeking early settlements. To defendants, the math often makes sense when comparing litigation costs to an early class settlement (especially on a claims-made basis). The litigation costs part of the equation is not always more expensive, as defendants are still winning early motions to dismiss, even in state courts. Often, this is because the lawsuits are hastily brought after the announcement of a breach and the named plaintiffs can point to no actual fraud or other harm. The operational impact of ransomware is being used in healthcare cases to identify a new idea of perceived harm (disruption of patient care), even if the data itself was not stolen or misused. This theory has met with mixed results in the courts.

Standing and Dismissal Challenges Continue to Bring Highs and Lows

Forecasting litigation costs and likely outcomes is challenging because decisions by courts remain inconsistent. In some cases, threshold standing and damages arguments found the same type of success as they have in the past, even in circuits that generally are more plaintiff-friendly. In other cases, claims survived motions to dismiss under (1) traditional data breach injury arguments like time and effort and credit monitoring and (2) novel theories based on the alleged lost value of personal information and claimed loss of the benefit of the bargain due to the defendant's allegedly inadequate data security. Although case law continues to be sparse on the class certification front, a New York federal court denied certification of any damages class in the case against Excellus Health Plan over the 2013-14 cyberattack on Excellus's computer network systems, while allowing a class for injunctive relief to go forward. It remains to be seen how the United States Supreme Court will rule in *TransUnion LLC v. Ramirez*, Case No. 20-297, where the Court could weigh in on the threshold question of whether or not every putative class member must have standing to proceed forward as a class. A decision in the *Ramirez* case is expected in June 2021.

20 lawsuits filed related to incidents disclosed in 2020 (compared with 14 in 2019)

- **3** lawsuits arose from incidents that started with unauthorized access to Office 365 inboxes
- **2** lawsuits involved payment card data
- **9** lawsuits involved SSNs
- **9** lawsuits involved medical/health information
- **7** lawsuits involved ransomware
- **3** lawsuits were vendor related

Number of Lawsuits by Individuals Notified

2	6	4
over 2 million	under 1,000	under 10,000

Without clear guidance, some federal judges have gotten creative when dismissing particularly specious data breach class actions for lack of standing by using unconventional means to prevent their reemergence. Because dismissals for lack of standing normally are not merit-based, plaintiffs can refile their cases in other courts, usually in state courts. Recently, a few federal courts have dismissed data breach class actions for lack of standing but have done so with prejudice to the plaintiff's rights to refile. On their face, these dismissals may appear to be technically improper. But they pose a dilemma for plaintiffs: refile in state court, which may uphold the federal court's dismissal with prejudice, or appeal the dismissal in federal court, which may affirm an erroneous dismissal with prejudice if the claims are clearly meritless. It is notable that in these standing-based dismissals with prejudice, the trial courts telegraph their view of the merits of the plaintiff's claims, while not formally reaching the merits. Whether this represents an emerging trend or simply a few outlier cases, it is an interesting and creative approach to maintaining the standing bar while trying to stem repetitive litigation and forum shopping.

New Substantive Areas Have Emerged

While lawsuits following incidents arising from phishing, network intrusions, and ransomware still dominate class action filings, there has been a rise in the following areas:

- Supply-chain cases – business-to-business indemnity claims over the impact of a vendor's data breach. We predict that these lawsuits will not only continue but will also have an impact on how indemnity, limitation of liability, and other contract provisions will be drafted in vendor and other business contracts going forward.
- Claims under California's automatic license plate recognition (ALPR) (tracking license plates) statute are also on the rise. Enacted in 2016, California's ALPR law mandates that an "ALPR end-user," which it defines as a person that accesses or uses an ALPR system, must maintain "reasonable security procedures and practices" and "implement a usage and privacy policy in order to ensure that the access, use, sharing, and dissemination of ALPR information is consistent with respect for individuals' privacy and civil liberties."
- Internet tracking cases. New filings against hospitals have decreased, probably while the plaintiffs await the outcome of key motions in cases that were filed in 2019 and 2020. The new filings involve claims being filed in states that have an anti-wiretapping law, most notably in Florida.
- BIPA cases (perhaps not a new trend but a trend that continues). In addition to cases against employers that use biometric timekeeping technologies, we have seen cases against companies that use facial recognition technologies but do not have direct customer interaction and attempt to bring in affiliated entities or franchisors.

Class Action Settlement Trends

When a decision to settle is made, there are creative and cost-effective ways to bring class actions to a close. Trends we see in class action settlement administration include:

- Claims-made settlements – the expectation of claims rates increasing during COVID-19 did not occur.
- Heightened administration costs due to mailing issues, confusion and interaction issues with the public (e.g., increased phone traffic), and dealing with fraudulent claims.
- Judges taking a much closer look at settlement, notice, and claim program terms than before. Ultimately, preliminary and final approval of settlements continue, but we are seeing the following issues get focus from judges:
  - Are claims really typical enough to satisfy a settlement class, and should plaintiffs submit a specific typicality affidavit?
  - After the 11th Circuit opinion on incentive fees, can settlements be approved with incentive fees at all?
  - Should claims/opt-out/objection periods be extended due to delays in providing notice (such as re-mailing)?
  - Should class members getting a re-mailed notice get automatically extended claims deadlines?
  - How does the class get notified of remote hearings?

WORK FROM HOME

Technology trends already had security professionals working on how to build defenses for an environment that was no longer inside a perimeter wall. The necessity of WFH has brought more attention to this need. Other consequences of WFH include:

- Unfortunate things happened in the haze of the initial move to WFH (e.g., plugging in unpatched appliances, fewer eyes on glass monitoring).
- Highlighted security gaps for mobile device management (MDM) (e.g., organizations had former employees with data stored on devices used as part of a BYOD program).
- Taking eyes off the ball – financial impact, personnel availability, new priorities, and other issues resulted in organizations making tough choices about what could be completed from its security road map.
- Things were not noticed – while organizations were closed or while people were not working on-site, security events were not noticed as quickly.
- Extended timeline for forensic investigations – there were numerous practical challenges, ranging from getting physical access to make an image of a device to installing an EDR tool on devices that were ofline.
- False unemployment claims – starting in spring 2020 and continuing throughout the year, many organizations identified fraudulent unemployment claims for current employees (sometimes a few and sometimes hundreds, often including executives).
- Ransomware impact – the combination of the WFH distraction from security, practical challenges of investigating an incident and restoring systems led to threat actors receiving payments, which led to a surge in ransomware events and higher ransom demands in the summer and fall of 2020.

INFORMATION GOVERNANCE

Take Action

Avoid organizational information governance practices that don't work in the "real world." Real-world problems include:

- **Storing sensitive information longer than necessary and in locations not protected or managed by IT security (including external devices, file shares, and cloud services) – increasing an attack surface and creating opportunities for access to information that should not exist in the first place.**
- **Inability to monitor and detect accidental exposure or theft by insiders of sensitive data.**
- **Confounding employee use of information – necessary diagrams go missing, or multiple versions of the same document lead to confusion and inefficiency (or worse!).**
- **Presenting inconsistent or nonexistent reportable practices during internal or third-party audits.**
- **Multiplying costs during eDiscovery responses to litigation and regulatory investigation.**

Consider taking discrete steps that offer outsize effects:

- **Execute a brief, focused information governance policy (e.g., "Manage Information Responsibly").**
- **Confirm a records retention schedule with defensible practices.**
- **Automate the application of the records retention schedule against file locations according to information type and retention period.**
- **Responsibly delete; move to storage; delete; concatenate and remediate; and delete again.**

VENDOR INCIDENTS

of total incidents involved vendor-causes

of vendor-caused incidents had notice requirements

of notices had regulatory inquiries

Third-Party Service Providers

Shopify Tablet SolarWinds Radial Accellion Citrix Blackbaud Finastra Mimecast

High-profile compromises of third-party service providers including SolarWinds, Blackbaud, finastra, and Shopify as well as compromises due to exploiting vulnerabilities in vendor software (Accellion in 2020 and Microsoft Exchange in 2021) have put C-SCRM front and center. Incident responders continue to work through the impact of those incidents, while using lessons learned to help organizations improve (e.g., defense in depth). Like collaborations between drug manufacturers on COVID-19 vaccines, the efforts and information shared by firms that have investigated third-party incidents (e.g., information provided by FireEye regarding SolarWinds) benefited many and showed a path for more effective responses.

C-SCRM and vendor compromises will only become more challenging as organizations rely more on third parties and threat actors see how effective these attacks can be. Below is a list of vendor-caused incident challenges and lessons learned.

Timeline from Discovery to Client Notification It often takes longer for individuals to be notified when a vendor discovers an incident than when the principal organization does. The difference starts with the amount of time it takes vendors to notify their customers of an incident. In addition, the vendor's initial notice may be incomplete or inaccurate.

Only the Vendor Can Investigate Because the incident occurred in the vendor's network, the vendor has to conduct the investigation, leaving the client waiting for results. These investigations are often frustrating for customers, as vendors may be reluctant to share full details or are overwhelmed by inquiries from multiple customers.

Vendor Vetting Is More Important than Ever (But Read the Section on Zero-Trust) Before engaging a new vendor that will receive access to their environment or data, companies must vet the vendor to make sure it has the proper safeguards in place.

Contractual Terms and Conditions Matter When a vendor experiences an incident involving thousands of clients, the customers' rights and remedies start with the language of the vendor contract. The efficacy and appropriateness of terms vary significantly in different scenarios.

Understand and Limit What You Provide to a Vendor It is not uncommon for clients to be surprised by what data the vendor had.

Oversight After Engagement Is Critical Easy to say, hard to do.

Beware of Fourth-Party Risk Vendors have vendors too.

The CCPA dominated much of the conversation in the privacy and product counseling space in 2020. Organizations spent the bulk of 2019 working to implement the CCPA's statutory requirements and addressing the first round of regulations issued by the Office of the Attorney General (OAG). For the first half of 2020, companies awaited the OAG's final regulations as the CCPA's July 1 enforcement date approached. The OAG kept everyone on their toes, issuing multiple rounds of modifications to the regulations before the final version was adopted on August 14, 2020.

On Election Day 2020, California voters approved the California Privacy Rights Act (CPRA) ballot referendum. Sometimes referred to as "CCPA 2.0," the CPRA will add to and amend organizations' CCPA compliance obligations. Although the majority of the CPRA's amendments will not become effective until January 1, 2023, the CPRA immediately extended the CCPA's exemptions for personal information obtained in the HR and business-to-business contexts. Below are some facts and statistics regarding our CCPA compliance efforts with clients in 2020.

CCPA Compliance Statistics and Facts

- In 2020, we assisted more than 100 companies from a broad range of industries – including big tech, retail, advertising technology, telecommunications, and others – in developing and implementing CCPA compliance programs.
- BakerHostetler assisted the Interactive Advertising Bureau (IAB) in the development of its CCPA Compliance Framework for Publishers and Technology Companies, a technical and legal framework aimed at addressing the vexing issues arising from the CCPA's novel "Do Not Sell" right in digital advertising use cases.

Consumer Request Statistics and Facts

- The overwhelming majority of organizations we counseled received at least some CCPA consumer requests, though the numbers varied widely, from a handful of requests to thousands. In general, the volume was higher at the start of 2020, then leveled off or significantly decreased for most companies by the middle of the year.
- Deletion and Do Not Sell requests were the most common type of requests received.
- Placement of a Do Not Sell link on company websites was less common prior to the OAG's July 1 enforcement date; thereafter, DNS link adoption increased significantly.
- In addition to requests submitted directly by individual consumers, a majority of companies received requests from automated request services.

Enforcement actions from European Union (EU) data protection authorities (DPAs) in 2020 underscored how DPAs are implementing the GDPR and member state policies in determining breach-related fines. Although DPAs began actions in response to data breach notifications, in some instances investigations resulted in GDPR non-compliance fines unrelated to the data breaches themselves, demonstrating that a breach may expose an organization to a DPA's examination of its entire GDPR compliance program.

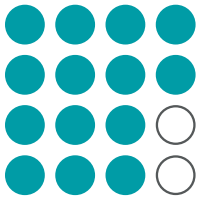
EU Regulatory 2020 Trends

- **Timing Is (Still) Everything** Much of the focus on GDPR's notice obligations has been on the 72-hour deadline for notifying a DPA. While some DPAs accept delays accompanied by explanations, others take a much narrower view of the permissible bases for extending the deadline. In particular, the Dutch DPA has taken a hard stance that the need to further investigate the incident and its effects is not a sufficient reason for delayed notice. Several other DPAs, including in Ireland and Sweden, fined companies for failing to notify within the 72-hour deadline. Companies subject to the GDPR should be prepared to move quickly to make an initial, timely notification that may require follow-up once a more complete analysis is ready.
- **Gentle (Yet Firm) Suggestions** Some DPAs prefer to suggest a course of action or have a phone call about a notice rather than open an inquiry or issue an order. While these suggestions are generally understood to be unofficial orders, they save clients the time and expense of responding to a more formal process and reduce the chance of a broader examination of GDPR compliance. Noncompliance with a DPA during an investigation has been cited in enforcement actions as a reason for fining a company.
- **Learning to Collaborate** Some DPAs are asking to review and comment on individual notices before they are mailed. In countries where this practice is common, such as Italy, companies may benefit from giving the DPA a chance to provide input up front or to comment on the need for individual notice. This helps minimize the risk that the DPA will take issue with the content of a communication or assess harm after the fact.
- **Data Controller Responsibility** DPAs tend to have the greatest interest and assess the largest fines in incidents where the DPA finds fault with the company's responsibility for EU personal data, particularly where there are repeat data breaches. In particular, DPAs have assessed how companies:
  - identify and respond to data breaches
  - implement and maintain organizational and technical measures to safeguard personal data
  - assess third-party vendors
  - conduct data protection-related risk assessments
  - document data breaches
- **Limited Resources, Limited Reaction** DPAs are receiving more notices than they can fully investigate, even where they involve issues with a notice timeline, security measures, or an organization's broader compliance program. Incidents with small numbers of individuals or less-sensitive personal data and those involving companies without a significant EU footprint have continued to garner relatively little follow-up after notification. In general, DPAs have not shown interest so far in testing the full extraterritorial scope of the GDPR.

DPA enforcement actions in 2020 drew particular attention to a number of mitigating factors in determining fines, and we expect these to be of continuing relevance this year:

- financial hardship, including the impact of the COVID-19 pandemic on the industry;
- actions taken by the organization to minimize potential harm to individuals;
- full cooperation with the DPA during investigation (although not all DPAs view cooperation as a mitigating factor);
- appropriate notice to the regulator and individuals;
- other fines already imposed and costs incurred in relation to the same incident; and
- an absence of prior violations.

As more countries implement mandatory breach notification procedures, we anticipate that regulatory enforcement will expand throughout 2021.



16 notices to 8 different EU DPAs

2 investigations remain open

Privacy and Compliance Highlights

Novel COVID-19 Issues
The pandemic raised numerous novel healthcare privacy and compliance issues. As continuous monitoring and surveillance and contact tracing became key pillars of the fight against COVID-19, complex issues related to data sharing, consent and data privacy quickly came to the fore. We helped clients across a wide variety of industries — from employers to universities to retailers to healthcare organizations to governmental agencies — put solutions in place that enabled the client to ensure health and safety while also complying with federal and state regulations.

Telehealth
The pandemic accelerated the adoption of telemedicine throughout the country, as providers were forced to adopt telehealth solutions almost overnight. The significant reliance on telehealth, particularly early on, greatly normalized telehealth as a healthcare delivery model. Most states eliminated existing regulatory barriers to widespread adoption of telehealth virtually overnight to combat the pandemic. While there will likely be some retraction after the national health emergency ends we anticipate that telehealth is here to stay and many regulatory restrictions will be permanently loosened.

Information Blocking
The Office of the National Coordinator (ONC) was tasked with implementing information blocking regulations in the 21st Century Cures Act. The regulations are heralded as having the potential to revolutionize the healthcare industry and increase transparency by arming patients with significantly more data, which carries its own healthcare privacy and compliance concerns.

OCR Shifts Focus

The Office for Civil Rights (OCR), as the enforcement arm of the Department of Health and Human Services, continues to open investigations in all matters involving 500 or more patients affected in a HIPAA breach incident. However, it is still relatively rare for any one of those investigations to move toward enforcement via a settlement or imposition of penalties.

Although the OCR entered into 20 resolution agreements in 2020, more than half did not involve data security incidents. Rather, the bulk of settlements related to the OCR's Right of Access Initiative, which seeks to enforce patient complaints relating to timely access to medical records. To date, the OCR has entered into 16 settlements under this initiative, 11 of which were in 2020.

The settlement amounts in resolution agreements involving HIPAA breaches ranged from a high of $6.85 million to $100,000 on the low end. The higher multimillion-dollar settlements tended to involve incidents affecting millions of patients. The smaller settlements involved smaller providers and smaller incidents.

In general, the 2020 resolution agreements showed little evidence of a particular pattern or focus. While a few enforcement actions were based on the failure to perform a risk analysis or to maintain appropriate HIPAA policies and procedures, others involved lack of encryption or lack of access controls. The OCR may be looking for low-hanging fruit at this point rather than focusing on a specific aspect of HIPAA.

Looking ahead, it may be more challenging for the OCR to significantly ramp up enforcement or penalty amounts in light of the recent M.D. Anderson Cancer Center decision. In January 2021, the 5th Circuit vacated the OCR's $4.3 million penalty against MD Anderson for three separate incidents involving lost thumb drives and a stolen laptop – all unencrypted. The 5th Circuit Court of Appeals held that the simple loss of unencrypted protected health information did not amount to an affirmative "disclosure" under HIPAA and that the OCR's penalty lacked support under the regulations.

Significantly, the 5th Circuit also found it arbitrary and capricious that the OCR enforced the rules against some covered entities but not others. MD Anderson was able to point to instances where other HIPAA-covered entities lost unencrypted laptops but were not penalized.

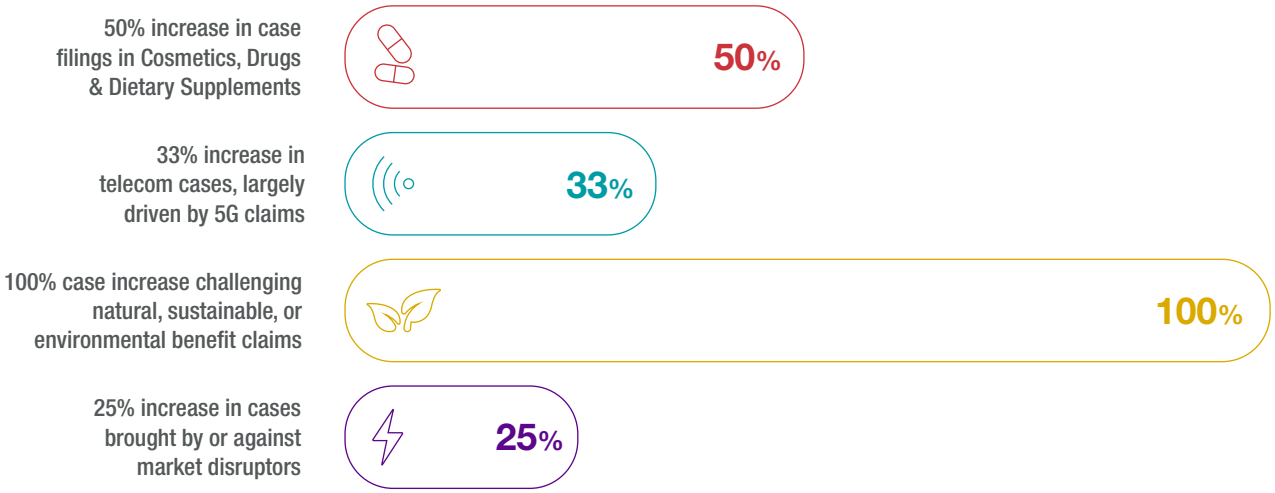
It is unclear how the OCR will navigate these new post-MD Anderson waters – whether inside or outside the jurisdiction of the 5th Circuit. But MD Anderson will certainly provide some additional arguments for covered entities to consider when responding to OCR investigations.

Truth in Advertising Trends

At the NAD

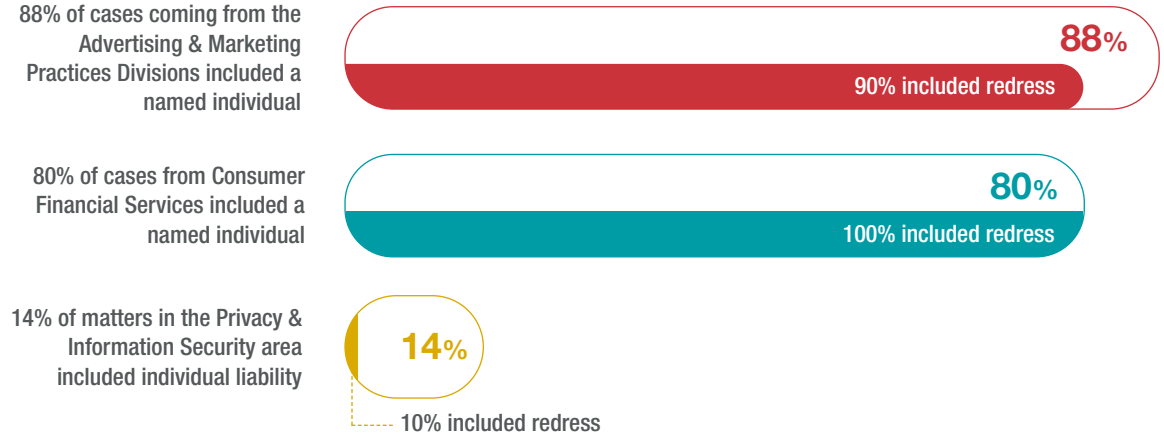
The National Advertising Division (NAD), the investigative unit of the advertising industry's system of self-regulation, monitors national advertising and resolves disputes to increase consumer confidence in the truth and accuracy of advertising claims and to support fair competition.

Overall, 2020 saw business as usual at the NAD, with no dip in the number of cases handled. What wasn't business as usual? The increase in certain types of claims that were the subject of an NAD dispute. Key trends included:



At the FTC

Two important trends emerged at the FTC: the push for monetary redress and the pursuit of individual liability when settling traditional advertising and marketing cases. We expect this enforcement focus to continue under the Biden administration. While our team members remember when injunction-only orders were the norm, in 2020 we saw:



Addressing Supply-Chain Attacks

Supply-chain attacks have increased sharply over the past decade, and that trend continued in 2020 and early 2021. Supply-chain attacks have obvious appeal to attackers and will keep happening. Organizations need a broader perspective and should assume that all software and devices are vulnerable. While a compromised supply chain gives an attacker initial access to your network, what they can do next depends on whether your organization has additional controls in place to prevent movement to other devices. So, you can – and should – defend against supply-chain attacks just as you defend against any other attack: Identify and implement reasonable controls to prevent, detect, and limit what an attacker can do in your network.

Vendor Management Is Not Enough

Good vendor management will help companies avoid suppliers that fall below a baseline and comply with regulations that mandate vendor oversight. Vendors involved in recent attacks serve major multinational corporations around the globe and have already been subjected to sophisticated vendor assessments—none of which detected the issues that led to these incidents. There's no reason to think that "better" vendor management would have prevented these incidents.

Start with Effective Risk Assessment

The starting point for strong controls against supply-chain attacks (or any other attack) is to answer three key questions:

Who is likely to target the organization?

What gaps exist in controls that may detect, prevent, or limit an attack?

Which of these threat/gap combinations is most likely to lead to a significant incident if not addressed?

That last question is the most important because it allows an organization to focus its limited resources on the most important areas. It is also hard to do without truly understanding how attacks occur and the real costs associated with those attacks.

Understanding and Using Zero-Trust Principles

As they are assessing and implementing new controls, maturing organizations should also look to implement zero-trust principles. Zero-trust is not new, but recent attacks and shifts in technology usage show the futility of defending a network with only a perimeter wall.

Zero-trust simply means you can't implicitly trust anything or anyone. That Exchange server might be good, or it might be saddled with vulnerabilities known only to an advanced threat actor. That might be Pat from accounting, or they might be an attacker using Pat's credentials to download the company's customer database before launching ransomware. Zero-trust principles constantly evaluate whether the activity makes sense based on contextual factors. This mindset helps protect against external attackers, supply-chain issues, and insider threats who may use their privileged access to harm the organization or steal data. Tools that support endpoint detection and response, identity and access management, and privileged account management are part of this approach—so are tools that aggregate and analyze data to identify unexpected or anomalous behavior.

No Easy Solutions

Knowing the solution doesn't mean these things are easily done. Practical obstacles—including limited resources and skill shortages—will limit how fast organizations can move. Cloud computing has helped somewhat, with zero-trust options available on major cloud platforms, but they still require skilled personnel to implement the solutions properly. Then there are architectural challenges. Most of today's networks developed organically over years or decades. Rapid turnover in technology jobs means those who built critical networks or applications may have left long ago. Significant architectural changes don't happen overnight—and when they do, that can lead to other problems.

These are long-term solutions that will take time to implement. But organizations should still develop plans and take deliberate actions to implement them. This will require investment and top-level support. While they are doing this, government action can help. Legislation should encourage organizations to investigate, document, and share information about incidents without fear that those results will be unreasonably used against the organization. This will improve information sharing, which will in turn improve assessments and collective defense. And federal legislation should provide a limited liability shield to organizations engaged in interstate commerce that have taken reasonable steps to implement security measures. This will incentivize organizations to take action while ensuring that those falling clearly below the bar may be held accountable.

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 convergence practice addressing enterprise risks, disputes, compliance, and opportunities through the life cycle of data, technology, advertising, and innovation, including marketing strategies and monetization.

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 K. 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

BakerHostetler

bakerlaw.com

© 2021 BakerHostetler®