



11th Hour CLE

2018 Video Replay Series

Session 4

Friday, December 28, 2018





11th Hour CLE
2018 Video Replay Series

Session 4
December 28, 2018

- | | | |
|------------------|--|--------------|
| 1 p.m. | Data Privacy: What the Legal Professional Needs to Know
Julie Hein, Esq., <i>Baker & Hostetler, LLP</i> | TAB A |
| 2 p.m. | Ethical Red Flags
Matthew C. Blickensderfer, Esq., <i>Frost Brown Todd, LLC</i> | TAB B |
| 3 p.m. | Break | |
| 3:15 p.m. | What the Integration of Baseball Teaches Us About Diversity & Inclusion in the Law
John C. Greiner, Esq. and Brian C. Thomas, Esq.,
<i>Graydon Head & Ritchey LLP</i> | TAB C |
| 4:15 p.m. | Adjourn | |

TAB A



BakerHostetler

Julie A. Hein

Associate

Cincinnati

T +1 513.852.2602

F +1 513.929.0303

jhein@bakerlaw.com



Overview

Julie Hein focuses her practice on cybersecurity and on privacy and data protection, with a concentration on contracts. With a background in all aspects of litigation and having spent time developing a professional privacy and data protection law group, Julie has a wealth of knowledge regarding cybersecurity and client needs. She takes a personal interest in her clients' positions, and represents clients with the most effective and efficient approaches.

Experience

- Represented a client in an employment contract case. Proved fraud and tampering with documents, resulted in a favorable outcome for the client. The judge required all parties to return post-trial to issue sanctions against the other party, but a post-trial settlement was achieved before sanctions were issued.
- Second chair in a construction contract and injury trial. Prepared and took witnesses; resulted in favor of the client.
- Counsel at trial in a contract dispute over two intertwined contracts concerning the sale of medical records software. The matter lasted four years; took client witness and cross witness; resulted in a favorable outcome for the client, including pre- and post-judgment interest.

Recognitions and Memberships

Memberships

- Ohio Bar Association
- Cincinnati Bar Association: Trustee (2015 to 2017)
 - Young Lawyers Section, Executive Committee: Chair (2016 to 2017)
- Cincinnati Bar Foundation (2013 to 2015)
- American Inns of Court: Young Lawyer Liaison (2014 to 2016)

Press Releases

- 6/28/2017
BakerHostetler's Cincinnati Office Grows with Addition of 13 Attorneys

Community

- Summit Country Day School: Mock Trial Advisor (2012 to 2017)
- Greater Cincinnati Foundation, Summertime Kids Committee

Pro Bono

- Successfully tried a tenant/landlord eviction matter in Hamilton County, Cincinnati.

Services

- Privacy and Data Protection

Prior Positions

- Progressive Insurance Company: Law Clerk (2008 to 2009)

Admissions

- Ohio

Education

- J.D., Case Western Reserve University School of Law, 2009; Diane Ethics Award; Outstanding Woman Law Graduate Award; Student Bar Association, President
- B.A., College of Mount St. Joseph, 2004



G d v l # \$ u y d f | = #

Z k w @ h j o k \$ u r i w i r o d o @ h n g # # N o r z

Julie Hein, Esq.
 Privacy & Data Protection Team
 Baker & Hostetler LLP
 513.852.2602
 jhein@bakerlaw.com

BakerHostetler
 BAKERHOSTETLER

1

"I'm Not Tech Savvy"

- "State-of-the-art-security"
 - Something you probably do not have and should not ever say you have.
- Firewall & AV
 - Two security tools that give people a false sense of security
- Remote Access
 - A method of connecting to a network remotely (e.g., LogMeIn, TeamViewer, Citrix). Otherwise known as a breach waiting to happen if only single-factor authentication is required.
- Network Diagram
 - Something your forensic firm will ask for on the first call that your IT team will have to create or update before sending.
- Exfiltration
 - Something you are not likely to find actual evidence of but will not be able to disprove (unless you have good logging). See also "no actual evidence of exfiltration," which often means the company has insufficient logs or the attacker cleared them.

BakerHostetler

2

"I'm Not Tech Savvy" (cont.)

IRT

- "Incident response team," or the group that does not do their day job during the day for months or longer after a significant incident.

DDoS

- Not a data breach. Rather, it is an attempt to disrupt or shut down operation of a web server by flooding a website with a high volume of traffic.

Bitcoin Wallet

- What you will need to establish and fund to pay the operator of ransomware if you are affected and do not have available backups.

Logs

- Network and host-based records of actions that occurred. Many companies find they do not have sufficient logs to facilitate forensic analysis (length of time & verbosity).

"Data breach" or "Leak"

- The text of the subject line of countless emails sent by panicked incident responders when they learn of the first signs of an issue.

BakerHostetler

3

Ethics





Rule 1

Competence

Understand changes in law practice, including the benefits and risks of relevant technology



Rule 1.6

Confidentiality

Use "reasonable efforts" to prevent any unauthorized access



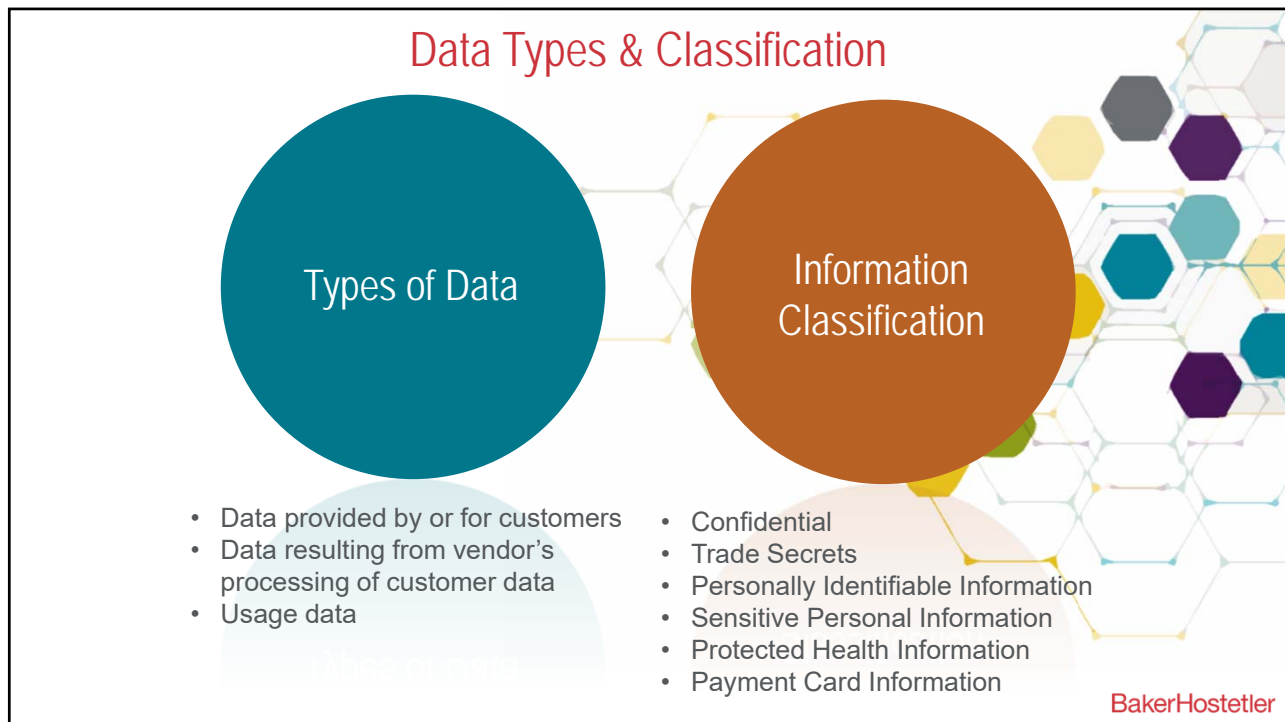
Rule 5

Supervision

Other lawyers, Non-lawyer Staff, and Vendors

BakerHostetler

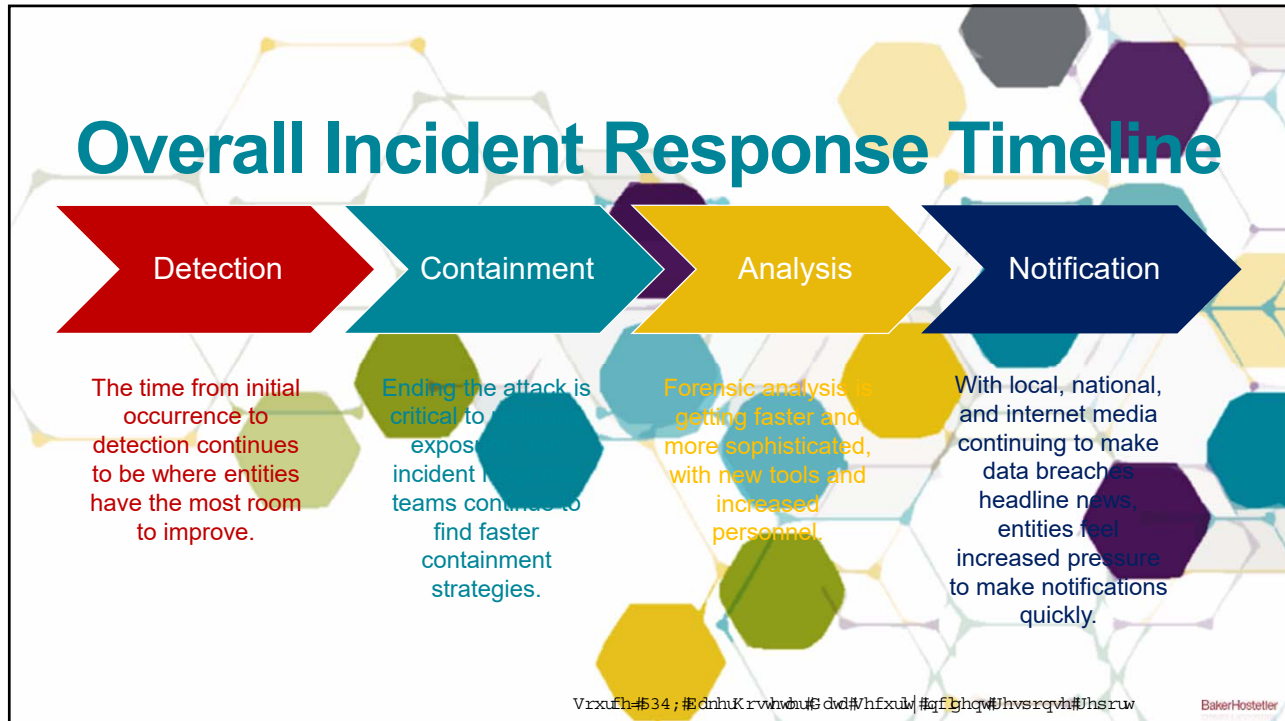
4



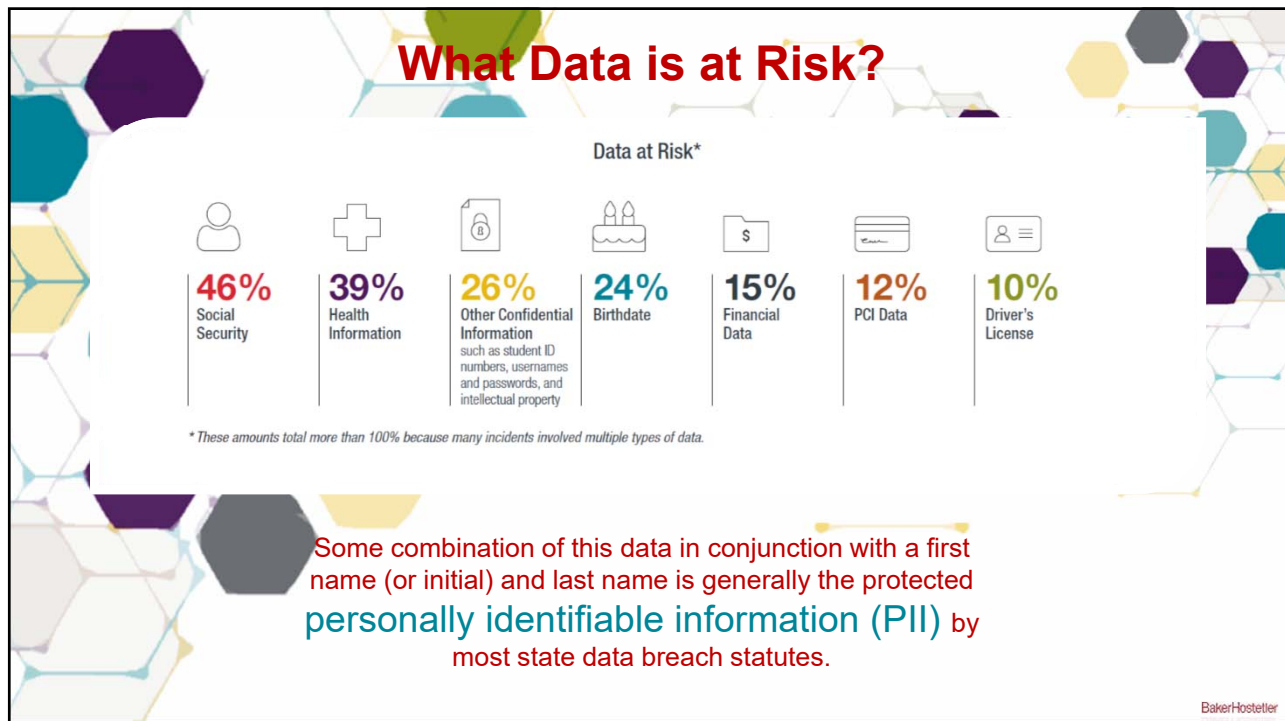
5



6



7



8



9

State Laws

- ▼ 50 States, D.C., & U.S. territories
- ▼ Laws vary between jurisdictions
- ▼ Varying levels of enforcement by state attorneys general
- ▼ Limited precedent
 - ▼ What does “access” mean?
 - ▼ What is a reasonable notice time?

EdinhKrvhwbnu

10

OHIO DATA BREACH STATUTE

[EXCERPT]

Breach of the security of the system means unauthorized access to and acquisition of computerized data that compromises the security or confidentiality of personal information owned or licensed by a person and that causes, reasonably is believed to have caused, or reasonably is believed will cause a material risk of identity theft or other fraud to the person or property of a resident of this state.

Personal Information means an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable:

- (i) Social security number;
- (ii) Driver's license number or state identification card number;
- (iii) Account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account.

Notification must be made "in the most expedient time possible but not later than forty-five days" following discovery or notification of the incident.

BakerHostetler

11

CALIFORNIA DATA BREACH STATUTE

[EXCERPT]

Breach of system security is unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. The statute applies where the information is either: (1) not encrypted or (2) encrypted, if an encryption key or security credential that allows an unauthorized party to render the data readable or usable is also compromised.

Personal Information means

- An individual's first name or first initial and his or her last name in combination with:
 - Social security number.
 - Driver's license number or California identification card number.
 - Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
 - Medical information.
 - Health insurance information.
 - Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.
- A username or email address in combination with a password or security question and answer that would permit access to an online account.

Notification must be made using a California-specific format.

Attorney General notification required if over 500 California residents are affected.

Private cause of action permitted for violation of statute.

Notice made in the most expedient time possible and without unreasonable delay.

BakerHostetler

12

NEW YORK DATA BREACH STATUTE

[EXCERPT]

Breach of the security of the system is unauthorized acquisition or acquisition without valid authorization of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business.

In determining whether information has been acquired without authorization, entities may consider the following factors, among others:

1. indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information;
2. indications that the information has been downloaded or copied; or
3. indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

“Personal information” is any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person. “Private information” is “personal information” in combination with the following, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired: (1) Social Security number; (2) driver’s license number or non-driver identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

Notice should be provided in the **most expedient time possible** and **without unreasonably delay**.

Notify Attorney General (portal), **NY Department of State, State Police** (online form)

If **over 5,000 NY residents** affected, notify **consumer reporting agencies**.

Attorney General may bring a civil suit for damages or an injunction.

BakerHostetler

13

FLORIDA DATA BREACH STATUTE

[EXCERPT]

Breach of the security of the system is unauthorized access of data in electronic form containing personal information.

Personal information means either of the following:

- (a) An individual’s first name or first initial and last name in combination with any one or more of the following data elements for that individual: (I) A social security number; (II) A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity; (III) A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual’s financial account;

A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

Notice should be provided as expeditiously as practicable and without unreasonable delay, but **no later than 30 days after determination of a breach**

If over **500 or more residents** are notified, then notification to the **Department of Legal Affairs (Attorney General)**, **no later than 30 days after determination of the breach**.

No private cause of action.

A violation is **an unfair or deceptive trade practice** and **AG may bring action**

BakerHostetler

14

INDIANA DATA BREACH STATUTE

[EXCERPT]

“Breach of the security of data” means “unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a person. The term includes the unauthorized acquisition of computerized data that have been transferred to another medium, including paper, microfilm, or a similar medium, even if the transferred data are no longer in a computerized format.”

Personal information means:

- (1) a Social Security number that is not encrypted or redacted; or
- (2) an individual's first and last names, or first initial and last name, and one or more of the following data elements that are not encrypted or redacted:

A driver's license number.

A state identification card number.

A credit card number.

A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account.

Notification should be made without unreasonable delay.

Notification to credit reporting agencies if more than 1,000 consumers are being notified.

Notification to AG's office required.

BakerHostetler

15

International Breach Notification

- ✦ Several Non-U.S. jurisdictions have security breach notification requirements
 - ✦ Some are specific to certain industries.
 - ✦ Some only require notification to a regulator.
- ✦ In certain countries, authorities have issued “guidance” for providing breach notification.
- ✦ GDPR will impose a 72-hour notification requirement. Effective May 25, 2018.



BakerHostetler

16

GDPR Breach Notification

“Personal data breach”: incident in security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed

Data controller must notify the competent Supervising Authority without undue delay and, where feasible, not later than 72 hours after discovery

If more than 72 hours later, must give reason for delay

Content: (1) Description of incident (number affected, categories of data subjects and data records); (2) DPO contact information; (3) likely consequences of incident, including mitigation efforts

Individual notification required if there’s a high risk (with exceptions)

Data processor must notify data controller “without undue delay” but no strict deadline

Entities operating in the EU should prepare a GDPR-compliant data security incident response plan

BakerHostetler

17

Is California the Next GDPR?

California Consumer Privacy Act of
June 28, 2018


- Takes effect June 2020
- Stated Purpose:
 - to give consumers more control and transparency regarding use of private information.

BakerHostetler

18

Rise of the Regulators

- Vvdw#Dwrugh|#hghudov#DJ v,
- R iifh#r#F ly#Ujkw#R FU,
- R vku#Uhx@wru



64 (Inquiries Following Notification

Djhqf#lv#vxh#F ly#qyhw#j dwyh#
G hp dggv#F IG v, wkdw#htxhw#


- ✓ Igirp dwrq#hfxu|#s@q
- ✓ Uhp hg#dwrq#wsv
- ✓ G lj l@#qylrqp hqw#hwd#bqg#lw#Ek|v#fdo#
Wnfkq#fdo#bqg#Dgp h#lwdw#h#F rquro

BakerHostetler

19

Regulators Expect:

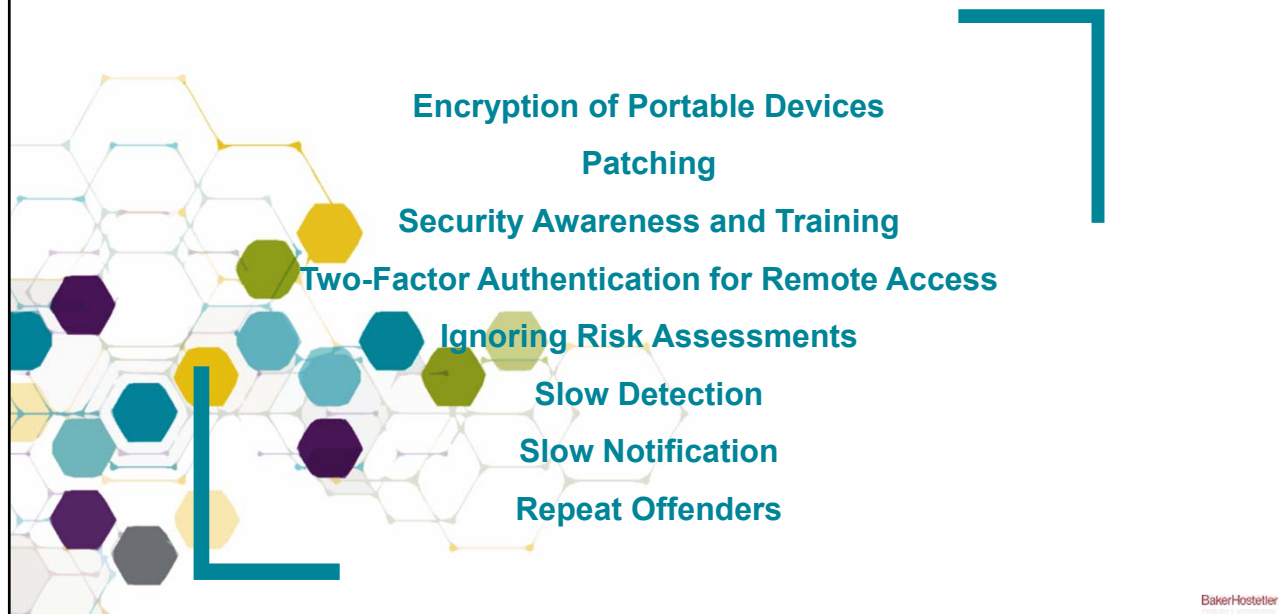
- Transparency: No Cover Ups.
- A prompt and thorough investigation.
- Good attitude and cooperation (commitment to compliance and safeguarding PII).
- Appropriate and prompt notification.
- Corrective action (know the root cause and address it; staff training; awareness program; technical safeguards; new policies/procedures/physical safeguards).
- Remediation and mitigation.



BakerHostetler

20

Regulatory “Hot Buttons”



21

Adobe Fined \$1M in Multistate Suit Over 2013 Breach

Nov. 11, 2016 – Adobe will pay \$1 million to settle a lawsuit filed by 15 state attorneys general over its 2013 data breach that exposed payment records on approximately 38 million people.

- ❖ In September 2013, Adobe learned of an attempt to steal customer payment card numbers maintained on one of its servers. The attacker ultimately stole encrypted payment card numbers and expiration dates, names, addresses, telephone numbers, e-mail addresses, and usernames as well as other data.
- ❖ Adobe discovered that one or more unauthorized intruder(s) had compromised a public-facing web server and used it to access other servers on Adobe’s network, including areas where Adobe stored consumer data.

22



23




BakerHostetler, 2017 Data Security Incident Response Report

24

Costs of a Security Breach

- Business interruption and income loss
- Forensic investigation expenses
- Notification-related expenses
 - Mailing, call center
 - Credit monitoring services
 - Crisis communication services
- Card network fines, fees, assessments
- Intellectual property theft
- Legal expenses (notification obligations, class actions, settlements)
- Regulatory fines
- Reputational damage
- Remediation of systems/networks

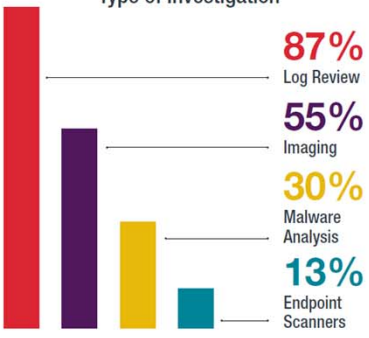


BakerHostetler

25


Forensic Investigations

Type of Investigation




Type of Investigation	Percentage
Log Review	87%
Imaging	55%
Malware Analysis	30%
Endpoint Scanners	13%

Use of Outside Forensics




65%
of Network Intrusion Incidents



41.5%
of Data Breach Incidents


Forensic Investigation Costs

Category	Cost
for All Incidents	\$84,417
for Network Intrusion Incidents	\$86,751
for 20 Largest Investigations	\$436,938



36
Days

Average Completion Time for Forensic Investigation



24%

Evidence of Data Exfiltration in Network Intrusion Incidents

BakerHostetler

26

Costs of a Cyberattack

- 2016: FedEx acquires TNT Express for \$4.8 billion.
- June 28, 2017: FedEx announces that the worldwide operations of TNT were significantly affected by the cyber-attack known as Petya.
- July 17, 2017: FedEx states that it expects the Petya outbreak to have a material financial impact.
- Citigroup analyst predicts the incident could reduce FedEx earnings by \$.50 - \$1 a share over the next year.
- FedEx does not have cyber insurance to cover financial losses related to the outbreak.

FedEx Struggles to Bounce Back From Cyberattack
Company's TNT Express business using manual processes in a significant portion of its operations

FedEx delivery truck trailers are parked outside the new Chicago Loop FedEx Ground Station on July 14. PHOTO: KAREN KRZACZYNSKI/REUTERS

By [Imani Moise](#)
Updated July 17, 2017 3:46 p.m. ET

Customers waiting for packages abroad are experiencing significant delays as FedEx Corp. [FDX -2.05%](#) continues to reel from the effects of a June 27 cyberattack.

The delivery giant said Monday in a securities filing that the global cyberattack known as Petya significantly affected the operations of its TNT Express business, which has delivery operations in the Middle East and Africa, Asia-Pacific, Europe and South

BakerHostetter

27

Threats Don't Stop After You've Been Compromised:

47%
of customers with at least one significant attack were successfully attacked again within one year.

Source: Mandiant, a FireEye Company, *M-Trends 2018*, (2018)

BakerHostetter

28

Insurance

- General liability insurance typically does not cover data breach or professional services liability.
- Errors and Omissions/Professional Liability
 - damages due to errors, acts, omissions or negligence in providing professional services.
- Cyber-risk
 - costs of a cyber-attack and/or data breach



BakerHostetler

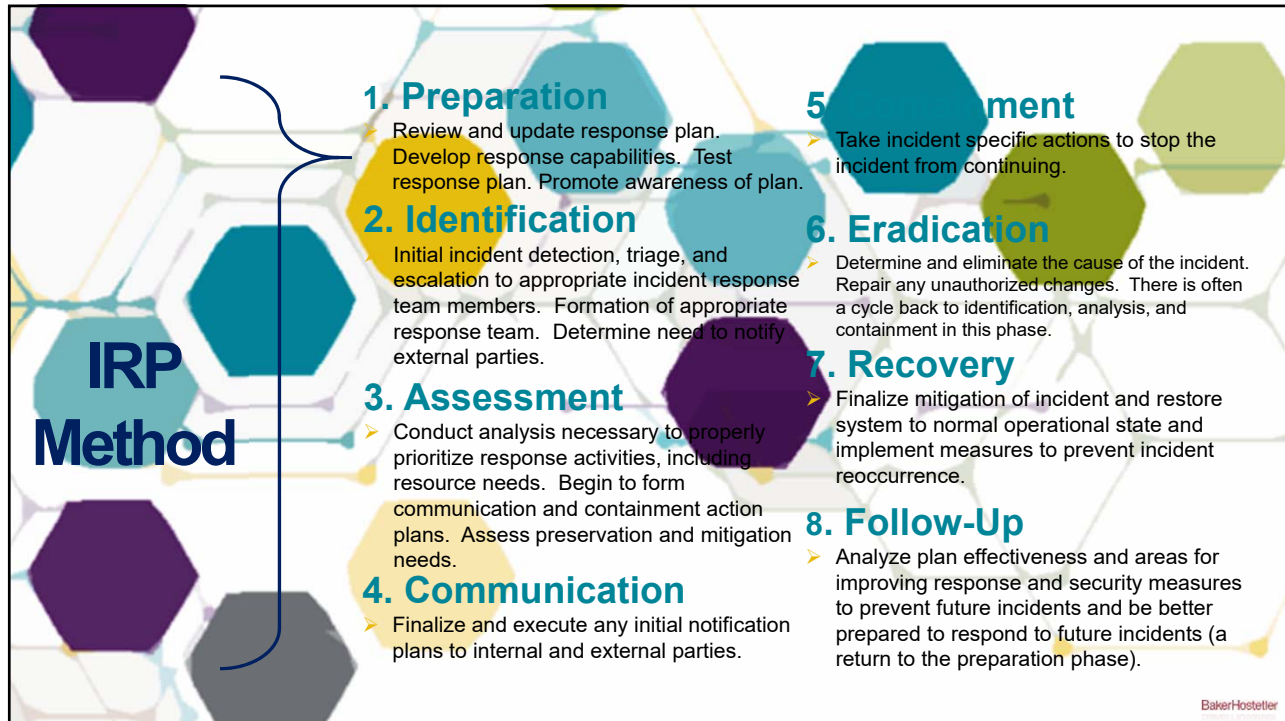
29

Cyber Insurance Coverage

Coverage type	Coverage
Privacy Liability	Liability coverage for claims resulting from failure to maintain the privacy of information. (e.g. PHI; PII; or a 3d Party's Confidential Information)
Network Security Liability	3d Party damages resulting from denial of service, costs related to data on third-party suppliers and costs related to the theft of data on third-party systems
Cyber-Extortion	The cost of investigation and the extortion demand (limited cover for ransom & crisis consultant expenses)
Regulatory Defense	The costs of complying with the various breach notification laws and regulations including legal expense, call centers, credit monitoring and forensic investigation
Data Property	The value of data stolen, destroyed, or corrupted by a computer attack
Business Interruption	Business income that is interrupted by a computer attack or a failure of technology including the extra expense
Crisis Management	Expenses for managing public relations

BakerHostetler

30



31



32

Building Cyber Resilience

Compromise Response Intelligence in Action



Key Findings



MFA is the gold standard.

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



It's not the cloud, it's you.

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



Rise of the regulator.

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



New year, same issues.

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



Everyone's involved.

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



No one is "too small."

Any entity, of any size, may become the victim of a cyber-attack. Hackers are happy to hit "singles" and take advantage of the lax security practices of small and medium-sized entities, and attacker techniques and tools simplify the process of finding even obscure targets of opportunity.



GDPR countdown drives uncertainty.

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



Reading the litigation tea leaves is an inexact science.

The line determining cognizable damages continues to blur. In addition, recent cases show that privilege may not apply to all incident-related communications, and that some entities choose to waive privilege.

CONTENTS

- 02 Incident Response Trends
- 04 Why Incidents Occur
- 06 Timeline Provides Context for Response Expectations
- 08 Forensics Drive Key Decisions
- 10 Regulators More Involved
- 12 Prepare for Privilege Challenges
- 14 Use Compromise Response Intelligence to Minimize Risk

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

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

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

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

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

Sincerely,



Ted Kobus

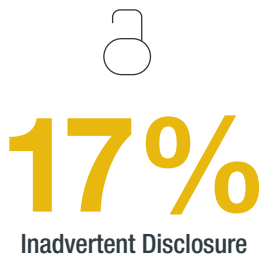
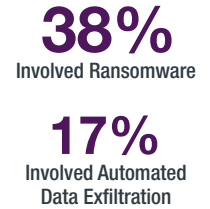
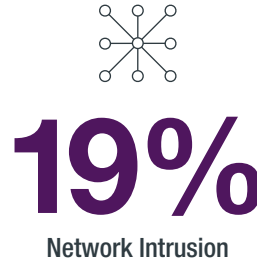
Leader, Privacy and Data Protection Team

560+

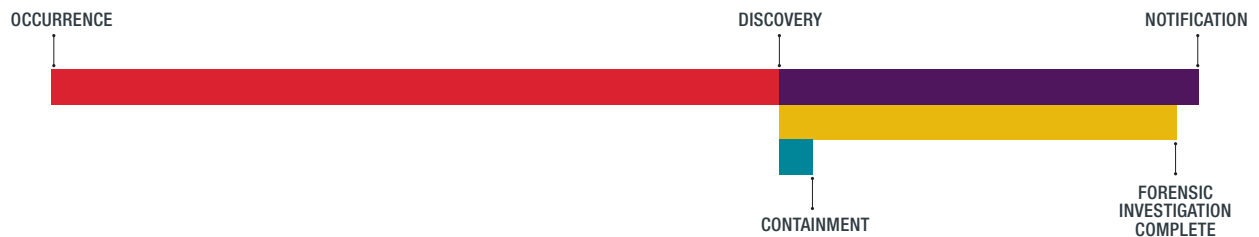
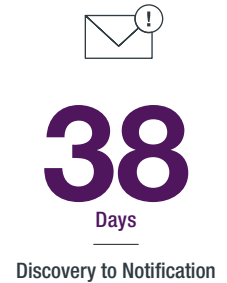
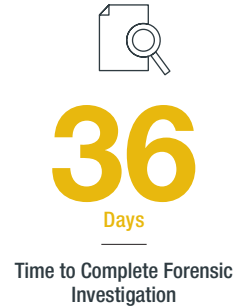
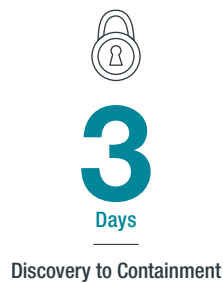
Incidents in 2017

Incident Response Trends

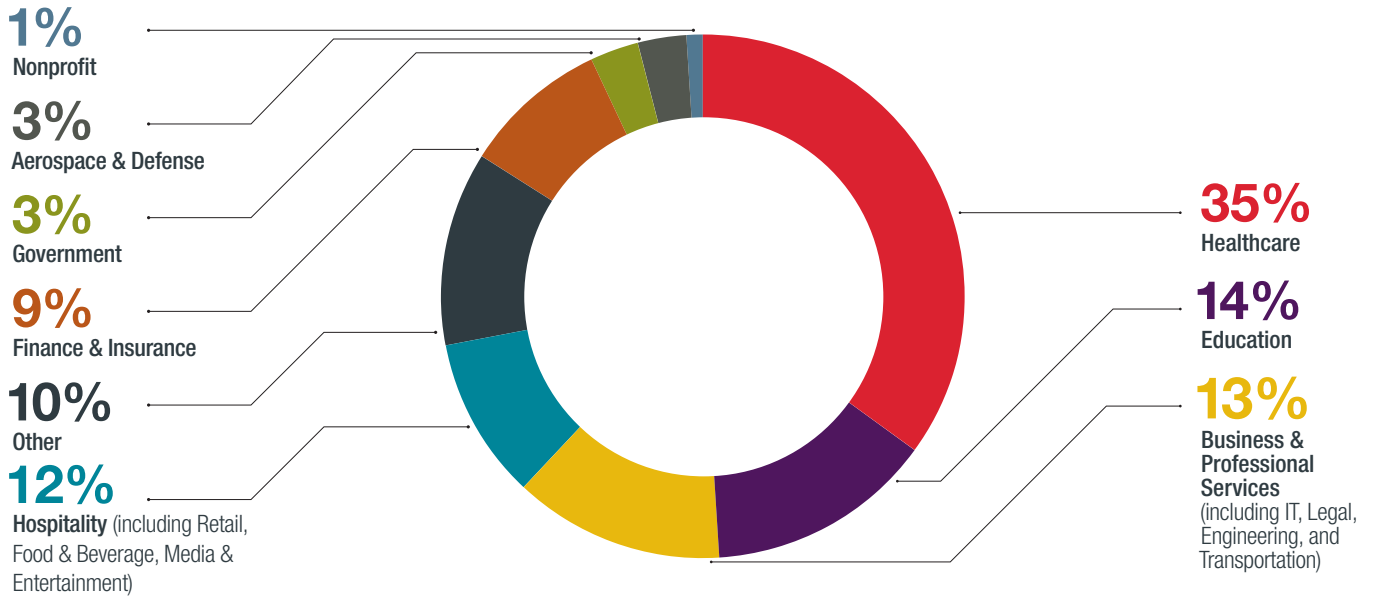
Top 5 Causes



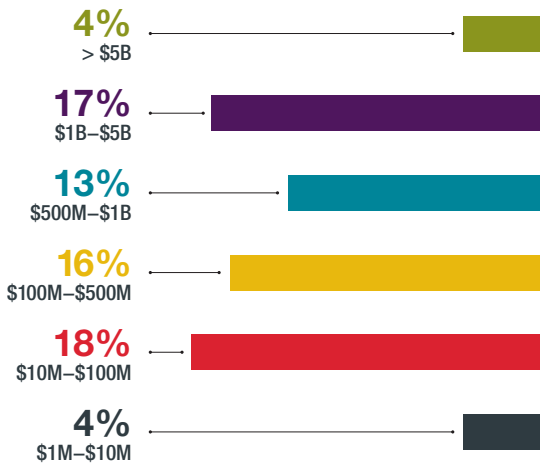
Incident Response Timeline



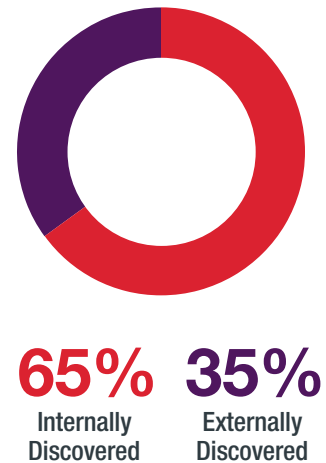
Industries Affected



Entity Size by Revenue



Breach Discovery



Average Forensic Investigation Costs

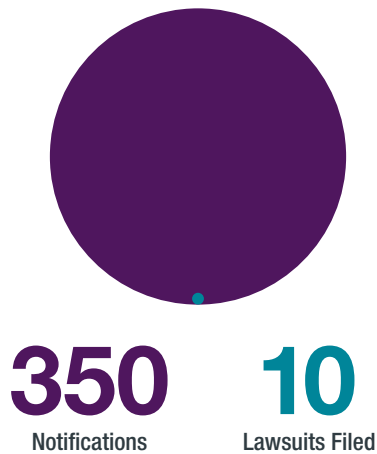


\$84,417
All Incidents

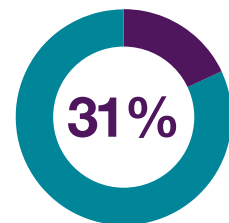
\$436,938
20 Largest Investigations

100%
Increase Over Last Year

Notifications vs. Lawsuits Filed



AG Inquiries Following Notification



Non-AG Inquiries

Year	Count
2016	29
2017	43

Why Incidents Occur

Phishing and Exploitation of Vulnerable Systems Top the List

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

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

Ransomware Attacks Continue

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

Cloud Misconfigurations: A Growing Trend

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



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

Phishing for Mail Access

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

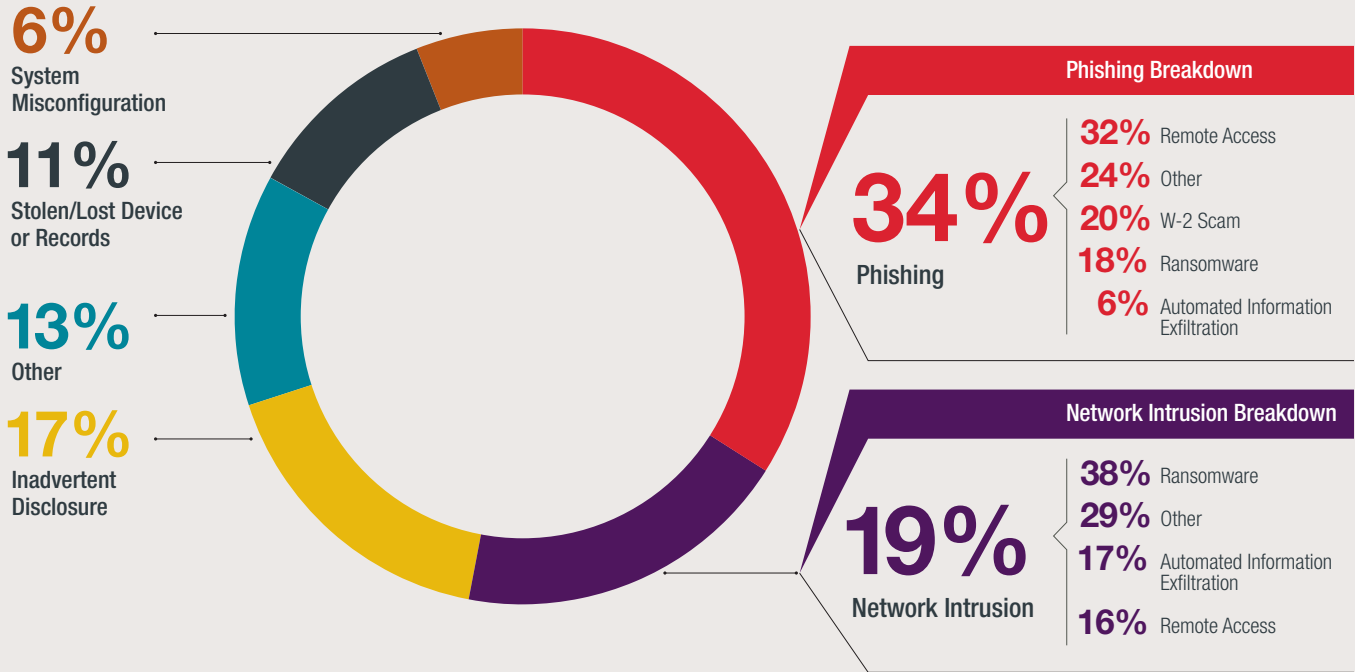
One tactic used by attackers to avoid detection was so common that it is worth a special note. After compromising a user’s mail account and using the target’s account to send fraudulent emails (in furtherance of a wire fraud scam, W-2 theft or some other fraud), an attacker will typically add mailbox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

Take Action: Close the Employee Loophole

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

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

Overall



Responsible Party



53%

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



31%

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



16%

Vendors/Service Providers

Breach Discovery



65%

of Breaches Internally Discovered

35%

of Breaches Externally Discovered

Ransomware



\$40,000

Average Payment

100% relied on vendor when payment in bitcoins requested

Timeline Provides Context for Response Expectations

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

Network Intrusion Timeline

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

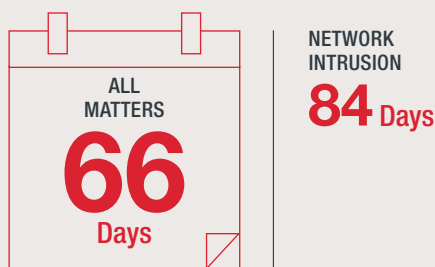
Overall Incident Response Time



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

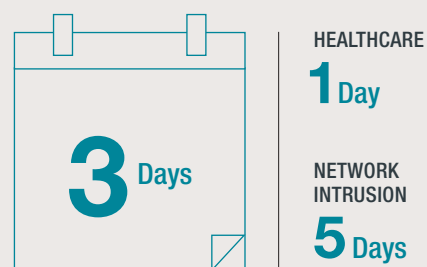
Entities are more aware than ever of the importance of constant vigilance. Of the data breaches in this year's survey, 65% were detected internally. Only 8% remained undetected for more than six months, and only 4% for more than a year.

Occurrence to Discovery



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

Discovery to Containment



Number of Individuals Notified



AVERAGE:

87,952

Notifications by Industry

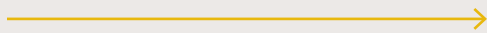
Hospitality (Food/Beverage, Retail)	627,723
Education	46,783
Business & Professional Services	8,284
Healthcare	6,470
Finance & Insurance	3,572
Other	2,729
Nonprofit	957
Government	927
Aerospace & Defense	275

Take Action: Keys to Shortening the Timeline

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



Analysis



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

Engagement of Forensics to Completion



HEALTHCARE
29 Days

NETWORK
INTRUSION
36 Days



Notification

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

Discovery to Notification



HEALTHCARE
43 Days

NETWORK
INTRUSION
45 Days

Forensics Drive Key Decisions

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

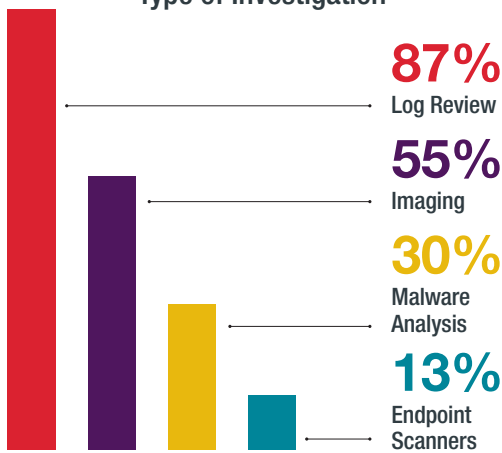
In 2017, forensics were used in 41% of intrusion incidents overall, compared with 34% in 2016, showing that entities are realizing the value of hiring outside investigators with broad experience and resources. Forensics were used in 65% of network intrusion incidents, probably due to the inherent complexity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

Forensic investigators use a variety of tools to determine the scope of information affected and the extent of the incident. Depending on the situation, they may analyze information from an entire network, a specific application, or a particular computer, mobile device, or other endpoint. In 2017, the most frequently used tool was log review, which enables the investigator to reconstruct how data was accessed and to determine whether it was exfiltrated. It can tell you who clicked on a phishing link, and how effective your defenses are. Log

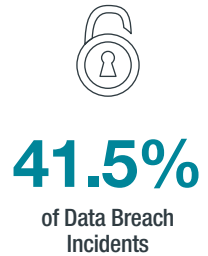
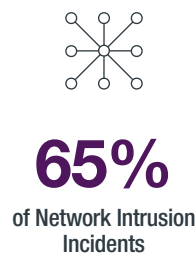
review was used in 87% of forensics investigations this year, probably due to the increase in Office 365 incidents involving attackers gaining access to different accounts. This trend further demonstrates how critical it is for entities to collect and retain robust logs in both on-premises and cloud environments.

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

Type of Investigation



Use of Outside Forensics



Forensic Investigation Costs

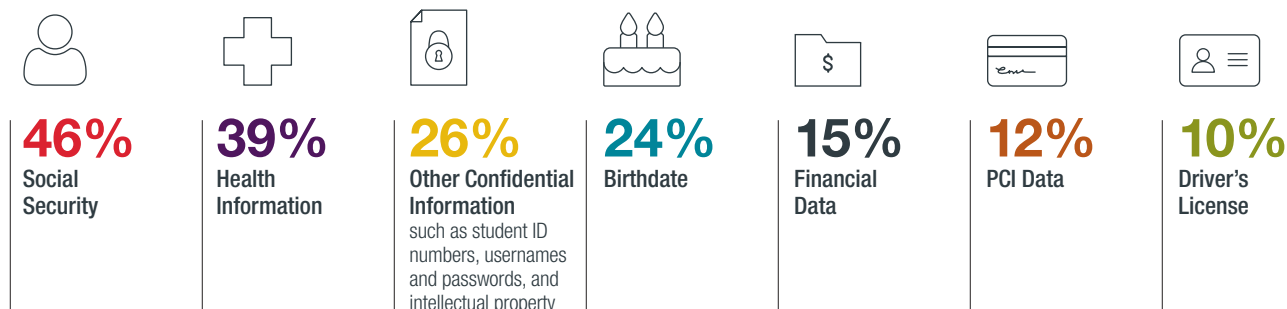


Average Completion Time for Forensic Investigation



24%
Evidence of Data Exfiltration in Network Intrusion Incidents

Data at Risk*



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

Latest Trends in Forensics

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

Investigating in the Cloud

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

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

Take Action: Choose the Right Forensic Firm

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

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

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

Regulators More Involved

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

Higher Budgets, Higher Stakes

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

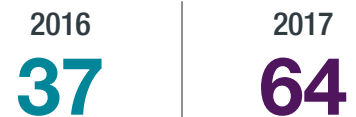
State AGs and other regulators, well-funded by large multistate settlements, are combining their power to compel testimony and documents with more experts to help them dive deeper into your operations than ever before. CIDs and informal letters now request not only your entity's information security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

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

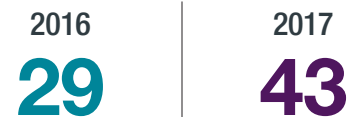
Size Doesn't Matter

AGs are looking beyond the number of affected residents to explore an entity's "systemic issues." Those that are slow to investigate, are slow to notify and experience repeat data incidents may be especially vulnerable.

AG Inquiries Following Notifications



Non-AG Inquiries



OCR Inquiries Where Notice in a Healthcare Incident Exceeded 500



What an AG Wants

					
Incident Response Plan	Employee Training Manual	Policies and Procedures	Forensic Reports	Information on Specific Data Loss Prevention	Information on Use of MFAs

Technology Helps Protect Payment Cards

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

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

EU Update: Preparing for GDPR Notification Requirements



The EU's General Data Protection Regulation (GDPR), effective May 25, 2018, addresses personal data breach notification in Article 33 (notifying authorities) and Article 34 (notifying individuals). The harm threshold for notifying regulators is lower than the threshold for notifying individuals – notification to authorities should occur within 72 hours after the entity has “become

aware” of a personal data breach that is likely to result in a “risk to the rights and freedoms of natural persons.” By contrast, notification to individual data subjects must occur when the breach is likely to result in a high risk to the rights and freedoms of natural persons. In both cases, the risk analysis must broadly consider the confidentiality, integrity, and availability of data.

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

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

2017 Per Card Assessment Range for Operating Expense and Fraud

\$4-\$20

Credit Monitoring Offered When Notification Occurred

60%

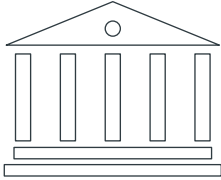
Average Redemption

35%

Take Action: Manage Regulatory Risk

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

Prepare for Privilege Challenges



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

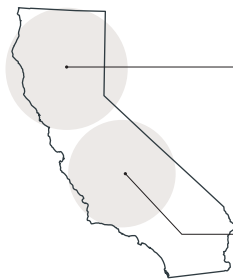
Data breach litigation is surviving motions to dismiss and proceeding to discovery, where plaintiffs seek breach investigation records and challenge defendants' assertions that the investigations are protected by various legal privileges. In 2017, three courts ruled on these challenges, with different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

California Protects Forensics Documents

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

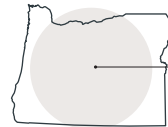
The United States District Court for the Central District of California reached a similar conclusion in a case involving a major consumer credit reporting agency. The plaintiffs argued that the forensic report and related documents were not protected by the attorney work-product doctrine because the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

Are Forensic Documents Protected From Discovery?



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

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



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

Oregon Limits the Privilege

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

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

Take Action: Build the Paper Trail

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

Use Compromise Response Intelligence to Minimize Risk

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

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

PREVIOUS RECOMMENDATIONS ARE STILL CRITICAL

1 Increase awareness of cybersecurity issues.

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

2 Identify and implement basic security measures.

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

- Retain logs for at least one year, preferably longer.
- Prohibit access to personal email accounts from the entity's network.

3 Create a forensics plan.

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

4 Build business continuity into your incident response plan.

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

5 Manage your vendors.

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

6 Combat ransomware.

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

7 Purchase the right cyber insurance policy.

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

NEW RECOMMENDATIONS KEEP YOUR RISK POSTURE CURRENT

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

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

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

Authentication by username and password alone can no longer protect sensitive information or secure remote access to network resources and third-party providers. This is true for several reasons. First, outdated guidance on password complexity and rotation (now updated) has inadvertently trained users to create bad passwords and share them across sites and services. Second, attackers have breached so many large stores of username and password combinations

that billions of breached password records are now in the public domain. Third, attackers use simple tools to automate so-called credential-stuffing attacks, in which attackers use these stolen password databases to brute-force their way into poorly protected services and sites.

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

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

Consider implementing these controls in any scenario involving (1) remote access to email (on-premises or in the cloud); (2) remote access to network resources through VPN; (3) remote

access to cloud resources, including third-party SaaS providers that handle sensitive information like HR or payroll data; and (4) login pages to customer-facing web applications containing sensitive data or processes.

10 Keep data secure in the cloud.

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

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

11 Prepare for more regulatory inquiries.

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

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

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

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

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

Risk Assessments: An Essential Guide

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

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

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

About BakerHostetler

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

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

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

Editor in Chief

Craig Hoffman

Cincinnati
T +1.513.929.3491
cahoffman@bakerlaw.com

Janine Anthony Bowen

Atlanta
T +1.404.946.9816
jbowen@bakerlaw.com

David A. Carney

Cleveland
T +1.216.861.7634
dcarney@bakerlaw.com

Teresa C. Chow

Los Angeles
T +1.310.979.8458
tchow@bakerlaw.com

Casie D. Collignon

Denver
T +1.303.764.4037
ccollignon@bakerlaw.com

William R. Daugherty

Houston
T +1.713.646.1321
wdaugherty@bakerlaw.com

Gerald J. Ferguson

New York
T +1.212.589.4238
gferguson@bakerlaw.com

Amy E. Fouts

Atlanta
T +1.404.256.8434
afouts@bakerlaw.com

Alan L. Friel

Los Angeles
T +1.310.442.8860
afriel@bakerlaw.com

Randal L. Gainer

Seattle
T +1.206.332.1381
rgainer@bakerlaw.com

Lisa M. Ghannoum

Cleveland
T +1.216.861.7872
lghannoum@bakerlaw.com

Linda A. Goldstein

New York
T +1.212.589.4206
lgoldstein@bakerlaw.com

Patrick H. Haggerty

Cincinnati
T +1.513.929.3412
phaggerty@bakerlaw.com

John P. Hutchins

Atlanta
T +1.404.946.9812
jhutchins@bakerlaw.com

Edward Jacobs

New York
T +1.212.589.4674
ejacobs@bakerlaw.com

Laura E. Jehl

Washington, D.C.
T +1.202.861.1588
ljehl@bakerlaw.com

Andreas T. Kaltsounis

Seattle
T +1.206.566.7080
akaltsounis@bakerlaw.com

Paul G. Karlsgodt

Denver
T +1.303.764.4013
pkarlsgodt@bakerlaw.com

David E. Kitchen

Cleveland
T +1.216.861.7060
dkitchen@bakerlaw.com

Theodore J. Kobus III

New York
T +1.212.271.1504
tkobus@bakerlaw.com

M. Scott Koller

Los Angeles
T +1.310.979.8427
mskoller@bakerlaw.com

Aaron R. Lancaster

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

Melinda L. McLellan

New York
T +1.212.589.4679
mmclellan@bakerlaw.com

Holly A. Melton

New York
T +1.212.589.4208
hmelton@bakerlaw.com

Eric A. Packel

Philadelphia
T +1.215.564.3031
epackel@bakerlaw.com

Lynn Sessions

Houston
T +1.713.646.1352
lsessions@bakerlaw.com

James A. Sherer

New York
T +1.212.589.4279
jsherer@bakerlaw.com

James A. Slater

Cleveland
T +1.216.861.7885
jslater@bakerlaw.com

Paulette M. Thomas

Cincinnati
T +1.513.929.3483
pmthomas@bakerlaw.com

Daniel R. Warren

Cleveland
T +1.216.861.7145
dwarren@bakerlaw.com

Christopher A. Wiech

Atlanta
T +1.404.946.9814
cwiech@bakerlaw.com

BakerHostetler

bakerlaw.com

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



TAB B



Matthew C. Blickensderfer



Member

mblickensderfer@fbtlaw.com

301 East Fourth Street
Great American Tower, Suite 3300
Cincinnati, Ohio 45202

T: 513.651.6162 | F: 513.651.6981

Assistant

Melissa Zahn
mzahn@fbtlaw.com
T 513.651.6770

PRACTICE AREAS

Antitrust Litigation and Counseling
Appellate
Business Litigation
Class Actions
Litigation

CONCENTRATIONS

Antitrust and Trade Regulation
Appellate Advocacy

INDUSTRIES

Automotive
Health Care

FIRM COMMITTEES

Ethics Committee, Member
Information Security Steering
Committee, Member

BAR MEMBERSHIPS

Illinois, 1995
Ohio, 2000

EDUCATION

Harvard Law School, J.D., 1995,
cum laude

Matt helps clients solve their challenges in two principal areas: (1) commercial litigation, with a focus on antitrust litigation and counseling, and (2) appellate litigation. Matt is a member in the litigation department.

Experience

Antitrust Litigation and Counseling

Matt has handled a wide variety of antitrust litigation, including cases alleging price-fixing and other conspiracies, monopolization, tying, and exclusive dealing. His antitrust work includes cases brought by government enforcers and private plaintiffs, including class actions. He frequently consults with clients outside the litigation context on all aspects of state and federal antitrust law including price discrimination. He frequently advises clients on their relationships with competitors, their relationships with suppliers and customers, and pricing issues.

His antitrust work spans many industries, including sports, manufacturing, petroleum, pharmaceuticals, automobile-related businesses, and payment services.

Highlights of Matt's recent antitrust work include these matters:

- *Commonwealth of Kentucky v. Marathon Petroleum Company LP* (W.D. Ky.) - Matt represents a petroleum refiner in the defense of a *parens patriae* action brought by the Attorney General of Kentucky. The lawsuit alleges that Marathon restrained trade in and monopolized the market for reformulated gasoline in the Louisville and Northern Kentucky metropolitan areas.

Matthew C. Blickensderfer

Northwestern University, B.A.,
1992, with highest distinction

- *Hyland v. Homeservices of America, et al.* (E.D. Ky.) - Matt currently represents a real estate brokerage firm accused of conspiring with other real estate brokers to fix the commissions on residential real estate in the Commonwealth of Kentucky. The district court certified a class of more than 70,000 sellers of residential real estate for the period 2001-2005. In July of 2012, less than two weeks before trial was set to begin, the district court granted summary judgment in favor of our client. The Sixth Circuit affirmed.
- *Midwest Agency Services et al. v. JPMorgan Chase Bank, N.A. et al.* (E.D. Ky.) - Matt represented the defendants in the successful defense of tying and state law claims. The plaintiffs alleged that Chase Bank refused to purchase automobile loans made by dealers unless the loans included a gap product issued by a Chase affiliate, and that this amounted to illegal tying under the federal antitrust laws and violations of Kentucky insurance statutes. The district court dismissed all claims, accepting all of the arguments advanced on behalf of the defendants: (1) the plaintiffs failed to plead injury to overall competition and thus had not established antitrust injury, (2) the conduct alleged was not a tying arrangement at all, but rather the defendants' legitimate choice as to what risks to accept, and (3) the conduct alleged did not violate the Kentucky insurance statutes.
- *Kentucky Speedway LLC v. NASCAR* (E.D. Ky.) - Matt represented NASCAR in the successful defense of a conspiracy and monopolization case brought by Kentucky Speedway in federal district court. The lawsuit alleged that NASCAR and various racetrack operators, including NASCAR's sister company, had conspired to exclude Kentucky Speedway and that NASCAR had illegally monopolized stock car racing. The district judge granted summary judgment for the defense. The Sixth Circuit affirmed.

Commercial Litigation

Matt's commercial litigation practice involves the prosecution and defense of claims for breach of contract (including UCC Article 2 litigation), tortious interference, fraud, and disparagement. Much of his work in these areas has involved Article 2 litigation for manufacturers, especially those in the automotive sector.

Matthew C. Blickensderfer

- *ClarkWestern Dietrich Building Systems, LLC v. Certified Steel Stud Association et alia* (Butler County Ohio) - Matt was part of the trial team that secured the largest verdict (in the longest jury trial) in the history of Butler County, Ohio. ClarkDietrich sued several competitors and their trade association for disparagement, defamation, violations of the Ohio Deceptive Trade Practices Act, and civil conspiracy. Matt led the damages aspects of the trial, including examination of both sides' experts and relevant fact witnesses. He also handled settlement discussions. During the two-and-one-half month trial, three of the four defendants settled. The jury awarded \$49.5 million in damages against the remaining defendant. The Ohio Court of Appeals affirmed the judgment.

Appellate Litigation

Matt also represents clients in federal and state appellate courts. He served as a law clerk to the Honorable David A. Nelson, United States Court of Appeals for the Sixth Circuit. He was the editor-in-chief of the third edition of the *Sixth Circuit Practice Manual* (LexisNexis 2006) and the author of its chapters on appellate jurisdiction, stays pending appeal, and briefing requirements. He was also a co-author of *Kentucky Appellate Practice* (Thompson/West 2006) with his colleagues Sheryl Snyder and Griffin Terry Sumner.

Matt's appellate work includes these matters:

- *State ex rel. Doner v. Zebringer*, 139 Ohio St.3d 314, 2014-Ohio-2102, 11 N.E.3d 1152 (Ohio 2014) - Matt represented the Ohio Department of Natural Resources and its Director in this contempt proceeding involving underlying eminent domain actions that the Supreme Court of Ohio had previously ordered the Department to file. Before Frost Brown Todd's representation began, the Supreme Court of Ohio had held the Department and its Director in contempt for delays in initiating the eminent domain actions. Subsequently, after Frost Brown Todd began representing the Department and its Director, the property owners filed a second contempt motion based on events in the underlying actions. The Supreme Court unanimously rejected the property owners' second contempt motion.
- *Huffman v. Hilltop Companies, LLC*, 747 F.3d 391 (6th Cir. 2014) - Matt represented Hilltop Companies in the successful appeal of a federal district court's refusal to compel arbitration of cases brought under the Fair Labor Standards Act. The district court had denied a motion to compel arbitration despite the existence of arbitration clauses in the plaintiffs' independent contractor agreements with Hilltop, because those agreements contained survival clauses that did not include the arbitration provision as a term that survived the expiration of the agreements. In a case of first impression at the federal appellate level, the Sixth Circuit reversed and compelled arbitration. The court of appeals held that the absence of the arbitration clause from the list of surviving provisions was insufficient to overcome the presumption that an agreement to arbitrate disputes survives the expiration of a contract.

Matthew C. Blickensderfer

- *Lipker v. AK Steel Corporation*, 698 F.3d 923 (6th Cir. 2012) - The plaintiff filed this ERISA benefits action against AK Steel for alleged miscalculation of surviving spouse benefits under the company's pension plan. The district court granted summary judgment in favor of the plaintiff. We secured a reversal in the Court of Appeals, which held that the company had correctly interpreted its plan and correctly calculated benefits. The decision effectively cut off a potential flood of other lawsuits and liabilities, including a simultaneously pending class action.
- *Welsh Development Company v. Warren County Regional Planning Commission*, 128 Ohio St.3d 471, 2011-Ohio-1604, 946 N.E.2d 215 (Ohio 2011) - The court of appeals had held that Welsh Development failed to perfect its administrative appeal based on its interpretation of the statutes governing appeals in Ohio state courts. The Ohio Supreme Court accepted our discretionary appeal to establish clear standards for Ohio administrative appeals. In a unanimous decision, the Supreme Court held that Welsh Development's appeal had been properly filed, and it articulated clear standards for filing such appeals.
- *Alliance Health Group LLC v. Bridging Health Options, LLC*, 553 F.3d 397 (5th Cir. 2008) - This case of first impression in the Fifth Circuit involved an issue of interpretation of forum selection clauses on which three other circuits had split. The Fifth Circuit accepted our client's position that a clause requiring litigation "in" a particular county permitted litigation in federal court, and not just the state court for that county, so long as the federal courthouse was physically located in the county in question.
- *Ignazio v. Clear Channel Communications*, 113 Ohio St.3d 276, 865 N.E.2d 18 (Ohio 2007) - The court of appeals had held that Clear Channel's employment arbitration agreement was unenforceable because of an objectionable provision. The Ohio Supreme Court accepted our discretionary appeal in order to set standards for severability of contract provisions. The Supreme Court held 6-1 in our client's favor that the unlawful provision of the arbitration agreement was severable and the remainder of the agreement enforceable.
- *Scovill v. WSYX/ABC*, 425 F.3d 1012 (6th Cir. 2005) - In this employment discrimination lawsuit, the Sixth Circuit accepted our client's arguments and reversed the district court's severance of certain aspects of an arbitration agreement while affirming the district court's findings that the dispute was arbitrable and the arbitration clause lawful.

Highlights & Recognitions

The Best Lawyers in America® Cincinnati "Lawyer of the Year," Litigation - Antitrust, 2013 and 2018

The Best Lawyers in America®, 2013 - 2019 (Litigation-Antitrust; Commercial Litigation)

Super Lawyers®, 2018 (Appellate Litigation)

Cincy Leading Lawyers, Antitrust and Appellate Litigation, 2006-2018

AV® Pre-Eminent Rated, *Martindale-Hubbell*®

Acritas Stars®

FBT Publications

July 9, 2018

Matthew C. Blickensderfer

AT&T / Time Warner Ruling Offers Insights into Antitrust Landscape

Legal Update

March 27, 2014

Sixth Circuit Dismisses Misclassification Class Action

Legal Update

July 9, 2009

U.S. Department of Justice Ramps Up Antitrust Enforcement

April 14, 2009

Antitrust Developments: Legislative Changes on the Horizon?

September 2008

Whole Foods and its Wild Oats: Antitrust scrutiny of mergers and acquisitions doesn't end when the deal closes

January 22, 2008

NASCAR Wins Summary Judgment in Antitrust Case brought by Kentucky Speedway

July 2007

U.S. Supreme Court Gives Manufacturers Greater Leeway in Controlling Distributors' Prices

News

November 24, 2014

Sixth Circuit won't pierce corporate veil in class action against real estate companies

Legal Newsline

FBT Events

May 24, 2012

Classless Actions Revisited: Fallout from the Supreme Court's Recent Class Action Decisions

August 25, 2011

Classless Actions: Practical Impacts of Recent Supreme Court Decisions

Press Releases

August 15, 2018

163 Frost Brown Todd Attorneys Listed in The Best Lawyers in America© 2019

December 6, 2017

34 Frost Brown Todd Attorneys Recognized by Ohio Super Lawyers® and 20 Recognized by Ohio Rising Stars® for 2018

August 15, 2017

161 Frost Brown Todd Attorneys Listed in The Best Lawyers in America© 2018

August 15, 2016

Matthew C. Blickensderfer

168 Frost Brown Todd Attorneys Listed in The Best Lawyers in America© 2017

August 17, 2015

175 Frost Brown Todd Attorneys Listed in The Best Lawyers in America© 2016

August 20, 2014

175 Frost Brown Todd Attorneys Listed in The Best Lawyers in America© 2015

August 15, 2013

172 Frost Brown Todd Attorneys Recognized in 2014 Best Lawyers®

February 12, 2013

Nine Frost Brown Todd Attorneys Recognized as Leading Lawyers in Cincinnati

September 13, 2012

17 Frost Brown Todd Attorneys Named 2013 “Lawyers of the Year”

August 27, 2012

167 Frost Brown Todd Attorneys Recognized in 2013 Best Lawyers®

Civic & Charitable Organizations

Springer School and Center (primary school for children with learning disabilities), Trustee, 2009-2017; President, 2014-2017

Non-FBT Publications And Events

Editor-in-chief and contributing author: "Sixth Circuit Practice Manual" (LexisNexis 3d ed. 2006)

"Kentucky Appellate Practice" (Thompson/West 2006)

Snyder, Sumner and Blickensderfer



Ethics and Risk Management in Law Firms – The Role of the Law Firm General Counsel





Matt Blickensderfer
Member
Frost Brown Todd LLC

1

Duties of the Law Firm General Counsel

- New engagements
- Conflicts and waivers
- General ethics consultation
- Discovery from the firm
- Risk management / loss prevention / claims
- Ethics / risk management policies
- Training
- Attorney arrivals and departures
- Information security
- Contract review



2

New Engagements

- The law firm general counsel oversees aspects of the new engagement / business intake process
 - Engagement agreements
 - Law firm-drafted
 - Critical components: definition of client; scope of work; resolution of any conflicts / conflict waiver
 - Client-drafted / outside counsel guidelines
 - Increasingly common
 - Frequently these contain provisions that are problematic for the law firm and even for the client that drafted them
 - Confidentiality provisions – consistent with ethical obligations?
 - Indemnification provisions – expansion of liability? consistent with insurance coverage?
 - Conflicts searching and resolution



3

Conflicts and Waivers

- Several types of conflicts considered – for example:
 - Current client
 - Cannot be adverse to a current client
 - Does not matter whether the matter is related or unrelated to work for the client
 - Former client
 - Can be adverse on unrelated matters
 - Joint representation
 - E.g., representation of employer and supervisor in an employment lawsuit
 - Will interests of jointly represented clients diverge?
 - What happens if they do?
 - How to treat one client's confidential information?



4

Conflicts and Waivers

- Several types of conflicts considered – for example:
 - Prior work
 - Dispute may involve the firm's prior work
 - E.g., litigating a patent the firm prosecuted
 - Is the client's interest aligned with the firm's interest in protecting its work?
 - Emerging
 - New parties enter the matter after engagement
 - E.g., new lender in a transaction, third-party defendant in a lawsuit
 - Thrust upon
 - Conflict created by events beyond the control of the law firm
 - E.g., merger or acquisition



Frost
Brown Todd
ATTORNEYS

5

Conflicts and Waivers

- Several types of conflicts considered – for example:
 - Confidential information / material limitation
 - Law firm may know something critical to one client that it cannot reveal due to confidentiality obligations to another client
 - Law firm may owe a duty to one client that is inconsistent with its duties to another client
 - Personal interest
 - Lawyer in the firm has a personal or “extracurricular” interest in the matter
 - E.g., lawyer serves on a board that is adverse to a firm client
 - E.g., a family member of a firm lawyer is adverse to a firm client



Frost
Brown Todd
ATTORNEYS

6

Conflicts and Waivers

- Conflict waivers
 - Basic rule – must be knowing and confirmed in writing
 - “Knowing” – depends on the sophistication of the client
 - Generally requires disclosure of the particulars of the conflict
 - Best practice is to explain the considerations the client should consider
 - “Confirmed in writing” can be a formal letter that is counter-signed, or it could be a letter or e-mail documenting a verbal conversation
 - Nonconsentable conflicts
 - Most conflicts can be waived
 - Some cannot – for example:
 - Plaintiff and defendant in the same litigation
 - Confidential information conflicts may not be consentable because the firm cannot explain why there is a conflict due to confidentiality obligations



Frost
Brown Todd
ATTORNEYS

7

General Ethics Consultation

- Privilege and confidentiality issues
- Fee, retainer, trust account issues
- Advertising and solicitation issues
- Disengagements
- Relations with adverse parties and opposing counsel
- Transfer of client files to or from another lawyer/firm
- Unauthorized practice / multijurisdictional practice
- Ancillary businesses



Frost
Brown Todd
ATTORNEYS

8

Discovery from the Law Firm

- Subpoenas / affidavits / depositions – for example:
 - Discovery in connection with a dispute over a transaction that firm handled
 - Commercial disputes between the law firm and a vendor
 - Personal matters for firm lawyers



Frost
Brown Todd
ATTORNEYS

9

Risk Management / Loss Prevention Claims

- Investigation of actual or potential claims
 - How they come to the general counsel's attention:
 - Reporting (usually self-reporting) by lawyers
 - Demand letter or complaint
 - Request for tolling agreement
 - Legal hold
 - Gathering facts
- Interaction with malpractice carrier
- Retention and supervision of outside counsel
- Negotiation of settlements



Frost
Brown Todd
ATTORNEYS

10

Reporting actual or potential claims to the law firm general counsel

- In-firm privilege – Does the attorney-client privilege apply to a firm lawyer’s communications about a loss prevention issue with the firm’s general counsel?
 - Trend is favorable, but bad precedents remain
 - The argument against the privilege is that lawyers and firms owes fiduciary duties and loyalty to clients, and secret discussions adverse to a client violate those obligations
 - Most recent authority rejects this view and recognizes the right of lawyers in a law firm to receive legal advice and that clients frequently benefit from that advice
 - Good law in the Southern District of Ohio – *Tattle Tale Alarm Sys., Inc. v. Calfee, Halter & Griswold, LLP*, 2011 WL 382627 (S.D. Ohio Feb. 11, 2011) (Kemp, M.J.)
- Best practice is to assume in-firm communications will be discoverable



11

Ethics / Risk Management Policies

- The law firm general counsel may be responsible for the creation, implementation, and enforcement of ethics and risk management policies – examples:
 - Insider trading
 - Social media
 - Officer / director positions
 - Business relationships with clients
 - Use of firm facilities
 - Confidentiality / information security



12

Training

- Orientation for new hires
- Ongoing ethics and risk management training for lawyers and staff
 - Partner / associate meetings
 - Practice group meetings
 - Staff meetings
 - Periodic e-mail tips



13

Attorney Arrivals and Departures

- Arrivals
 - Review of lateral hires when necessary
 - Conflicts
 - Background checks, prior discipline, prior claims
 - Orientation
- Departures
 - Client relationships
 - Departing attorney may have duties to the firm imposed by common law or partnership/LLC agreement
 - Departing lawyers are frequently
 - General rule in Ohio is that, prior to actual departure, a lawyer may only tell clients (1) that she is departing, (2) new contact information, and (3) whether she would be interested in continuing to work for the client
 - Client files

14

Information Security

- Financial scams
- Social engineering / spear fishing schemes
- HIPAA compliance
- Client auditing of information security policies and protocols/systems



15

Contract review

- Law firms enter a variety of contracts just like any other business
 - E.g., software vendors, copying/courier services
- The law firm general counsel frequently is involved in reviewing and approving these contracts



16

Questions?



TAB C





Brian C. Thomas

CONTACT

513-629-2859 (office)

bthomas@graydon.law

Downtown Cincinnati

312 Walnut Street, Suite 1800
Cincinnati, OH 45202

EDUCATION

Georgia Institute of Technology, B.S., with honors, Management, 1998 - Georgia Tech Track Team, Co-Captain 1996-97, 1997-98

LAW SCHOOL

University of Dayton School of Law, J.D., cum laude, 2001 - Law Review, Editor in Chief, 2000-01 - Moot Court Team Member, 2000-01

BAR ADMISSIONS

State of Ohio
U.S. District Court of Appeals - Sixth Circuit
U.S. District Court - Southern District of Ohio
U.S. District Court - Northern District of Ohio

AREAS OF PRACTICE

Business Litigation
Education
Employment - Labor & Employment
Employment (Construction)
Health Care
Hospitals & Health Systems
Labor & Employment
Start-Ups
Workplace Health & Safety

COMMUNITY OUTREACH

Black Lawyers Association of Cincinnati - Immediate Past President
People Working Cooperatively - Board of Trustees & Loan Committee Chairman
Greater Cincinnati Minority Counsel Program - Steering Committee Member
Leadership Cincinnati - Class 41
St. Vincent de Paul Society - Board
Cincinnati Academy of Leadership for Lawyers - Class XV; Board

Brian is a partner at Graydon and chairs the firm's Workers' Compensation Practice Group. He has 15 years of experience representing employers in a wide range of employment matters, including workplace health and safety. Brian takes pride in seeing both the forest and the trees. He lives by Einstein's saying that "any fool can know. The point is to understand." Brian recognizes that every client has unique challenges and opportunities. He knows that he must first listen and genuinely understand an employer's business before he can provide effective representation.

Brian learned these life lessons early. He started playing football in the second grade and saw how good teams are always greater than the sum of their parts. His parents also taught him that hard work pays off. Brian worked hard in high school to become a national champion hurdler. He continued his track and field career at Georgia Tech, where he was a four year letterman for the Yellow Jackets and served as the team's co-captain his junior and senior years. But Brian didn't limit his hard work to athletics.

Brian graduated from the University of Dayton School of Law, cum laude. While at UD, Brian served as the Editor-in-Chief of the University of Dayton Law Review and was an active participant on the school's Moot Court team. Brian believes success involves more than just individual achievements. Giving back is very important. Brian currently serves on several civic and non-profit boards including People Working Cooperatively, St. Vincent de Paul, the Greater Cincinnati Minority Counsel Program and the Cincinnati Academy of Leadership for Lawyers. Brian also mentors new lawyers as part of the Ohio Supreme Court's Lawyer to Lawyer Mentor Program.

Brian is still a sports fanatic, but his family is his greatest joy. You can find him at Paul Brown Stadium on Sunday with his mom, watching the Cleveland Cavaliers with his wife, or watching his two daughters train for gymnastics gold in the 2028 Olympics.



John C. Greiner

CONTACT

513-629-2734 (office)
513-484-2734 (mobile)
513-333-4316 (fax)

jgreiner@graydon.law

Downtown Cincinnati

312 Walnut Street, Suite 1800
Cincinnati,
OH <span
itemprop="postalCode">45202

EDUCATION

Miami University, B.A., cum laude, Political
Science/Economics, 1980

LAW SCHOOL

University of Notre Dame, J.D., cum laude,
1983 - Law Review

BAR ADMISSIONS

State of Ohio

AREAS OF PRACTICE

Appeals
Business Litigation
Cyber Security & Data Privacy
Intellectual Property
Intellectual Property Disputes
Litigation
Media & Marketing
Public Records

COMMUNITY OUTREACH

University of Cincinnati Law School - Adjunct
Instructor
ProKids Resource Team Leader
CBA Communications Committee - Chair
CBA Judicial Evaluations Research
Committee - Member
Ohio State Supreme Court Lawyers to
Lawyers Mentoring Program - Mentor
Ohio News Media Association Government
Relations Committee - Member
Beyond Civility Board - Member
Public Media Connect - CET/Think TV - Board
Member

AFFILIATIONS

Cincinnati Bar Association - Member -
Communications Committee - Chair

Jack is a commercial litigator with an emphasis on communications and media law. He is one of the region's leading advocates for governmental transparency, having argued numerous cases in the Supreme Courts of Ohio and Kentucky and in appellate courts in the tri-state area. His clients have included The Cincinnati Enquirer, ESPN, Vogue Magazine, and television stations in 16 markets.

Jack serves on the firm's Appellate Practice Group. Jack successfully argued a case before the United States Sixth Circuit Court of Appeals that prevented a title insurance company from denying coverage to a mortgage lender. Jack also argued a case in Ohio's Eighth Appellate District that protected the rights of mortgage lenders in foreclosure actions. Both cases are leading precedents in the field.

Jack is recognized with an AV Rating, the highest rating given to lawyers by Martindale-Hubbell. Jack has also been selected by his peers for inclusion in The Best Lawyers in America for his work in Commercial Litigation, Litigation-Banking and Finance, Litigation-First Amendment, and Litigation-Intellectual Property from 2005 to 2016. Jack has also been selected as The Best Lawyers in America "Lawyer of the Year" for his work in Litigation-Banking and Finance in 2012 and 2016; and The Best Lawyers in America "Lawyer of the Year" for his work in Litigation-First Amendment in 2015. In addition, from 2007 to present, Jack has been named an Ohio Super Lawyer for his work in Commercial Litigation and First Amendment Law. He was awarded the Ohio Society of Professional Journalist Award for Best Defense of the First Amendment for his contribution to "Lead's Dangerous Legacy."

Jack is a talented writer and in addition to having created the firm's e-newsletter, InfoLaw News, and his own blog - Jack Out of the Box. The blog received first place in the 2018 Ohio SPJ Awards for Best Blog in Ohio. He is the author of "Imagine When You're Feeling Better," a children's book written to benefit Josh Cares, a Cincinnati charity. He also enjoys Notre Dame football, Cincinnati Reds baseball and XU basketball. He has donated about eleven

Ohio State Bar Association - Member
Media Law Resources Center - Internet Law
Committee Chair
Ohio Coalition of Open Government -
Member
American Advertising Federation - Cincinnati
Chamber - Member

gallons of blood through Hoxworth, although not all at once. Guilty pleasures include LaRosa's pizza, Graeter's ice cream and Skyline Chili. (Did we mention Jack is a Native Cincinnati?) His real passion, however, is his family - his wife, Kathy, and four children, Katie, Joe, Ben, Ellie, granddaughters Lucy and Evelyn and grandson Jack - to whom he refers as his "greatest achievement."

Baseball and the Law

Brian C. Thomas, Esq.
Jack Greiner, Esq.

GRAYDON

1

CHRONOLOGY QUIZ

#1 What is the significance of the following dates?

GRAYDON

2

CHRONOLOGY QUIZ

YEAR

1899


GRAYDON

3

CHRONOLOGY QUIZ

ANSWER

Last black player in professional baseball until 1946



Bill Galloway

GRAYDON

4

CHRONOLOGY QUIZ

YEAR

1947


GRAYDON

5

CHRONOLOGY QUIZ

ANSWER

Jackie Robinson's
Rookie Year



GRAYDON

6

CHRONOLOGY QUIZ

YEAR

1949-1953






GRAYDON

7

CHRONOLOGY QUIZ

ANSWER

Rookie of the Year in NL

 Don Newcombe (1949)	 Sam Jethroe (1950)	 Willie Mays (1951)	 Joe Black (1952)	 Jim Gilliam (1953)
---	--	--	---	--

GRAYDON

8

CHRONOLOGY QUIZ

YEAR

1954

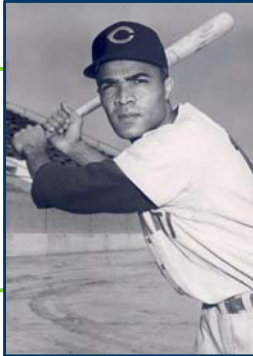
GRAYDON

9

CHRONOLOGY QUIZ

ANSWER

**Chuck Harmon -
First Black Red**



GRAYDON

10

CHRONOLOGY QUIZ

YEAR

1959

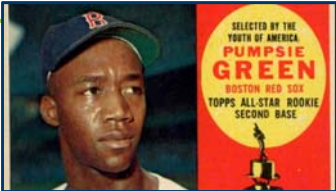
GRAYDON

11

CHRONOLOGY QUIZ

ANSWER

**Boston Red Sox –
Last MLB team to integrate**



Pumpsie Green

GRAYDON

12

CHRONOLOGY QUIZ

YEAR

1975


GRAYDON

13

CHRONOLOGY QUIZ

ANSWER

**Frank Robinson
is first Black Manager**



GRAYDON

14

#2 A Brief History of Baseball's Color Ban

1884:

Moses Fleetwood Walker played for Toledo of the then Major League American Association



GRAYDON

15

A Brief History of Baseball's Color Ban

1887:

Seven black players played in the International League (considered the most prestigious minor league at that time)

1887:

Newark of the International League doesn't play Walker and George Stovey at the insistence of their opponent, the Chicago White Stockings; on the same day, the IL votes 6-4 to prohibit signing additional black players; later that year, the Ohio League adopts the same rule.


GRAYDON

16

A Brief History of Baseball's Color Ban

1901: John McGraw, the manager of the Baltimore Orioles, signed Charles Grant, the second baseman of the Columbia Giants of Chicago, claiming he was a Native American name Tokohoma. Grant's black friends in Chicago, however, publicly honored him for signing a major league contract, which caused the deal to blow up

1942: Commissioner Kennesaw Mountain Landis: "[t]here is no rule, formal or informal, or any understanding – unwritten, subterranean, or sub-anything – against the hiring of Negro players by teams of organized ball."



17

#3 The Societal Landscape

LOUISIANA


Apartments could only rent to one race, but landlords could allow black custodians to live in the building;

FLORIDA

During summer vacation, books from black schools couldn't be stored in the same building as books from white schools;

OKLAHOMA

Fishing lakes and phone booths were segregated




18

#4 The Legal Landscape

1922

Federal Baseball Club v. National League,
295 U.S. 200 (1922) – grants baseball an anti
trust exemption.

GRAYDON

19

The Legal Landscape

1964

STATE CIVIL RIGHTS ACT -
typically address places of public
accommodation, not employment.

GRAYDON

20

The Legal Landscape

1866

Federal Civil Rights Act of 1866 –
“All persons within the jurisdiction of the United States shall have the same right in every state and territory to make and enforce contracts.”

GRAYDON

21

The Legal Landscape

1883

Civil Rights Cases of 1883 –
U.S. Supreme Court rules the statute applies only to state action, not private conduct. That interpretation upheld by the 8th Circuit in 1942 in *Love v. Chandler*, 124 F.2d 785.

GRAYDON

22

The Legal Landscape

1896

Plessy v. Ferguson, 163 U.S. 537 (1896)

"We consider the underlying fallacy of the plaintiff's argument to consist in the assumption that the enforced separation of the two races stamps the colored race with a badge of inferiority. If this be so, it is not by reason of anything found in the act, but solely because the colored race chooses to put that construction upon it.

GRAYDON 

23

Does the 14th Amendment permit private discrimination?

1945

Railway Mail Assn. v. Corsi,

326 U.S. 88 (1945)

Union argues that a New York statute prohibiting labor unions from discriminating on the basis of race offended the due process clause of the 14th Amendment. The Supreme Court unanimously rejected the argument.

GRAYDON 

24

The Legal Landscape

1945

Ives-Quinn Act,

The first fair employment practices act. It expressly prohibited discrimination on the basis of race. It applied to private employers with more than 6 employees. It created a State Commission Against Discrimination. Massachusetts adopted similar legislation. Isadore Muchnik, a Boston City Council Member, threatened to deny the Red Sox permission to play on Sundays unless the team considered hiring black players.

GRAYDON 

25

The Legal Landscape

SIGNIFICANT IMPACT

3 major league teams played in New York and two played in Boston. New York was also home for 13 minor league franchises.

GRAYDON 

26

The Legal Landscape

SIGNIFICANT IMPACT

Ives-Quinn provided political leverage. In October of 1945, a state panel investigating violations of the Ives-Quinn Act demanded that the three New York major league teams sign pledge promising not to discriminate in hiring. All three refused. And the pressure mounted.

GRAYDON 

27

The Legal Landscape

SIGNIFICANT IMPACT

Rickey signed Robinson on October 23, 1945. Some believed it was an effort to deflect the pressure. And some believed it slowed the process. Note the Giants and Yankees did not sign any black players until 1949. And the first black player to wear a Yankee uniform was Elston Howard in 1955.

GRAYDON 

28

5 The Societal IMPACT

1954 - Brown v. Board of Education of Topeka, 347 U.S. 483

1958 - Segregation prohibited in the U.S. Military

1964 - United States Civil Rights Act

1965 - Voting Rights Act

GRAYDON 

29

5 The Business IMPACT

The median Major League team gave up nearly \$2.2 million in 1950 dollars (more than \$19 million in 2010 dollars) during the period that they remained segregated. See ii. When only those teams that remained segregated beyond 1950 – when the returns to integration should have been obvious – are considered, the median teams lost profits are still more than \$1.2 million in 1950 dollars (over \$11 million in 2010 dollars). Id.

Decimation of the Negro Leagues

GRAYDON 

30

5 The **Baseball** IMPACT

- 1) 1947-1957 Yankees win 7 WS Titles
- 2) 1958-1967 Yankees win 3 WS Titles
- 3) 1947-1957 AL wins 8 WS Titles
- 4) 1958-1967 NL wins 6 WS Titles
- 5) 1939-1949 AL wins 8 All Star games
- 6) 1949-1959 NL wins 7 All Star games
- 7) 1960-1970 NL wins 12 of 14 All Star games

GRAYDON 

31

Lessons for Diversifying an Organization

GRAYDON 

32



Example of Branch Rickey



See beyond status quo



innovate



Think outside the box

GRAYDON

33

SOLICIT BUY IN



Example of Old line scout Clyde Sukeforth

GRAYDON

34

Jackie Robinson

Not “best” player in Negro leagues

1. Raised in CA – outside heavily segregated South
2. College UCLA
3. Multi Sport athlete
4. Military Service
5. Stable Family

35

Accomodation

- Wendell Smith hired to travel with Robinson during 1946 spring training and season.
- Robinson assigned to Montreal in 1946.
- 1947 Spring training in Havana

36



HELP AND SUPPORT from MANAGEMENT

Veterans traded
Petition shut down
Forfeit bluff called

GRAYDON

37



Thank You!

GRAYDON

38