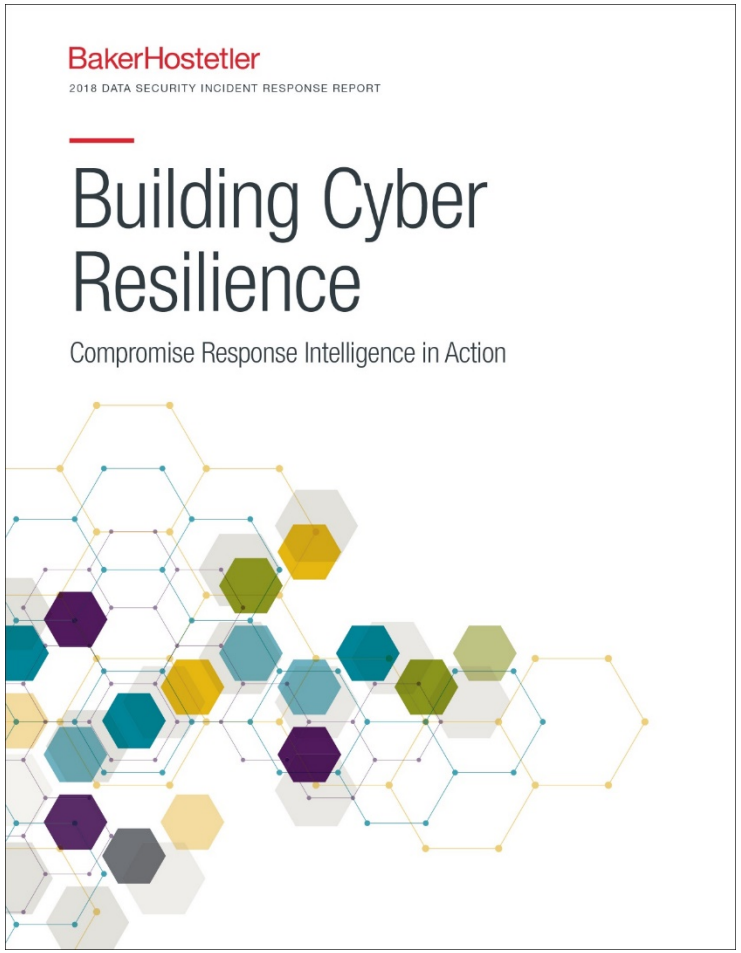
2018 Data Security Incident Response Report

Building Cyber Resilience: Compromise Response Intelligence in Action



BakerHostetler

April 11, 2018

Contact Information

Casie D. Collignon
Partner
Denver
303.764.4037
ccollignon@bakerlaw.com

Theodore J. Kobus, III
Leader, Privacy and Data Protection Practice
New York
212.271.1504
tkobus@bakerlaw.com

Craig A. Hoffman
Partner
Cincinnati
513.929.3491
cahoffman@bakerlaw.com

Lynn Sessions
Partner
Houston
713.646.1352
lsessions@bakerlaw.com

About the Team

- 50+ member team
- 15+ members for Incident Response
- Chambers Ranked
- Law360 Privacy Team of the Year (2013 - 2015)
- Law360 Privacy MVPs (2013 - 2016)
- Law360 Privacy “Rising Stars” (2013 - 2016)
- 2500+ incidents

The 2018 Report

- 560+ Incidents
- All industries represented
- Phishing and exploitation of vulnerable systems top the list of why incidents occur
- Regulators are getting more involved
- Companies of all sizes impacted
- Crypto-miner attacks on the rise
- Ransomware is not going away
- Forensics drive key decisions
- Privilege issues need to be considered early

Compromise Ready

- Contractual obligations & regulatory compliance
- Threat information gathering
- Technology – preventative & detective
- Personnel – awareness & training
- Security Assessments
  - Identify assets and sensitive data
  - Implement reasonable safeguards
  - Increase detection capabilities
- Vendor management
- Conduct tabletop exercises
- Cyber liability insurance
- Ongoing diligence and oversight (leverage cyber response intelligence to prioritize)

Compromise Response Intelligence

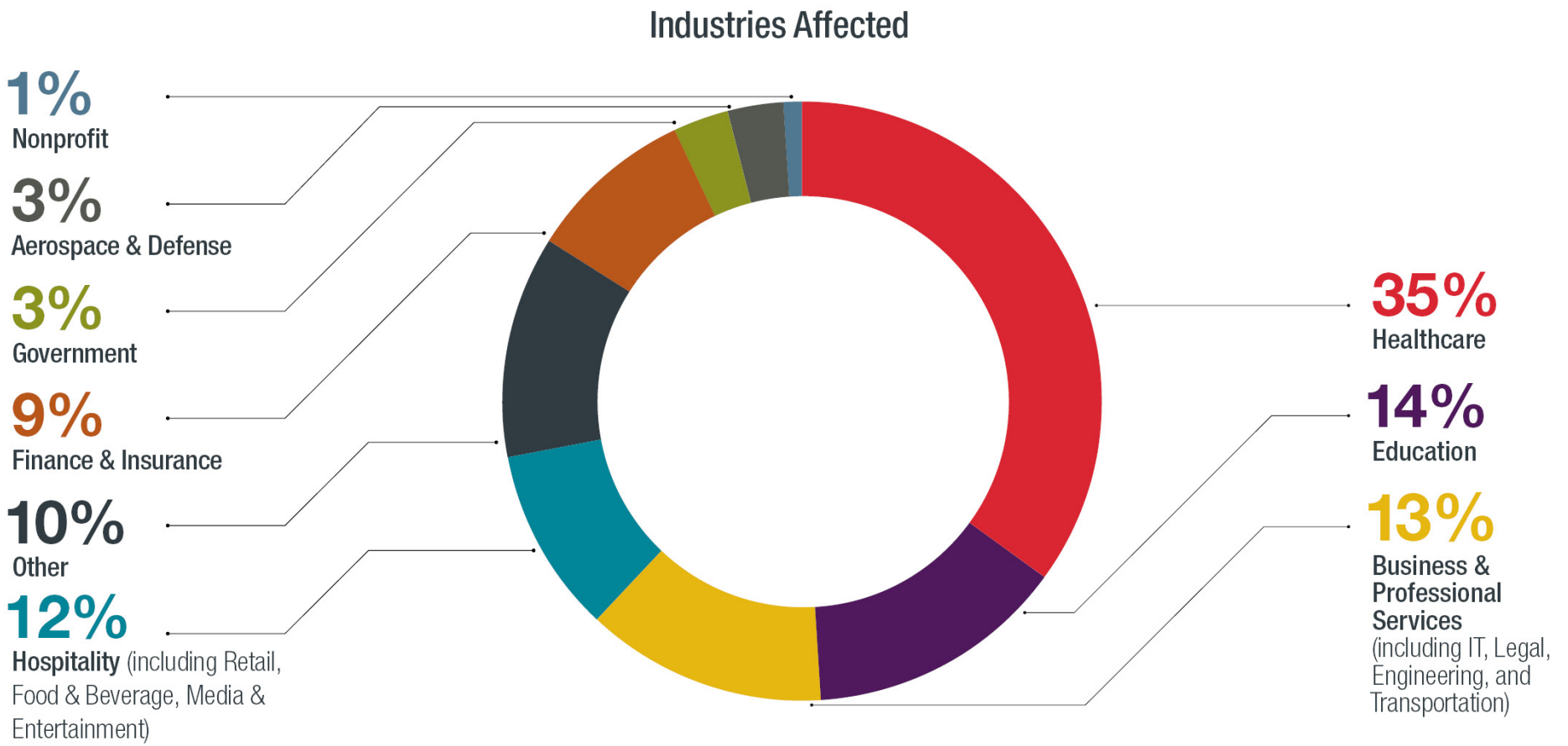
- Run of the mill to the best attackers get in through phishing
- It's not just about protecting sensitive data, operational resiliency is equal risk
- Acquisitions bring new risk
- Multifactor authentication is the gold standard
- It's not the cloud, it's you (or your vendor)
- Rise of the regulator
- New year, same old issues
- Everyone's involved
- GDPR countdown drives uncertainty
- Litigation uncertainty

Incident Response Trends

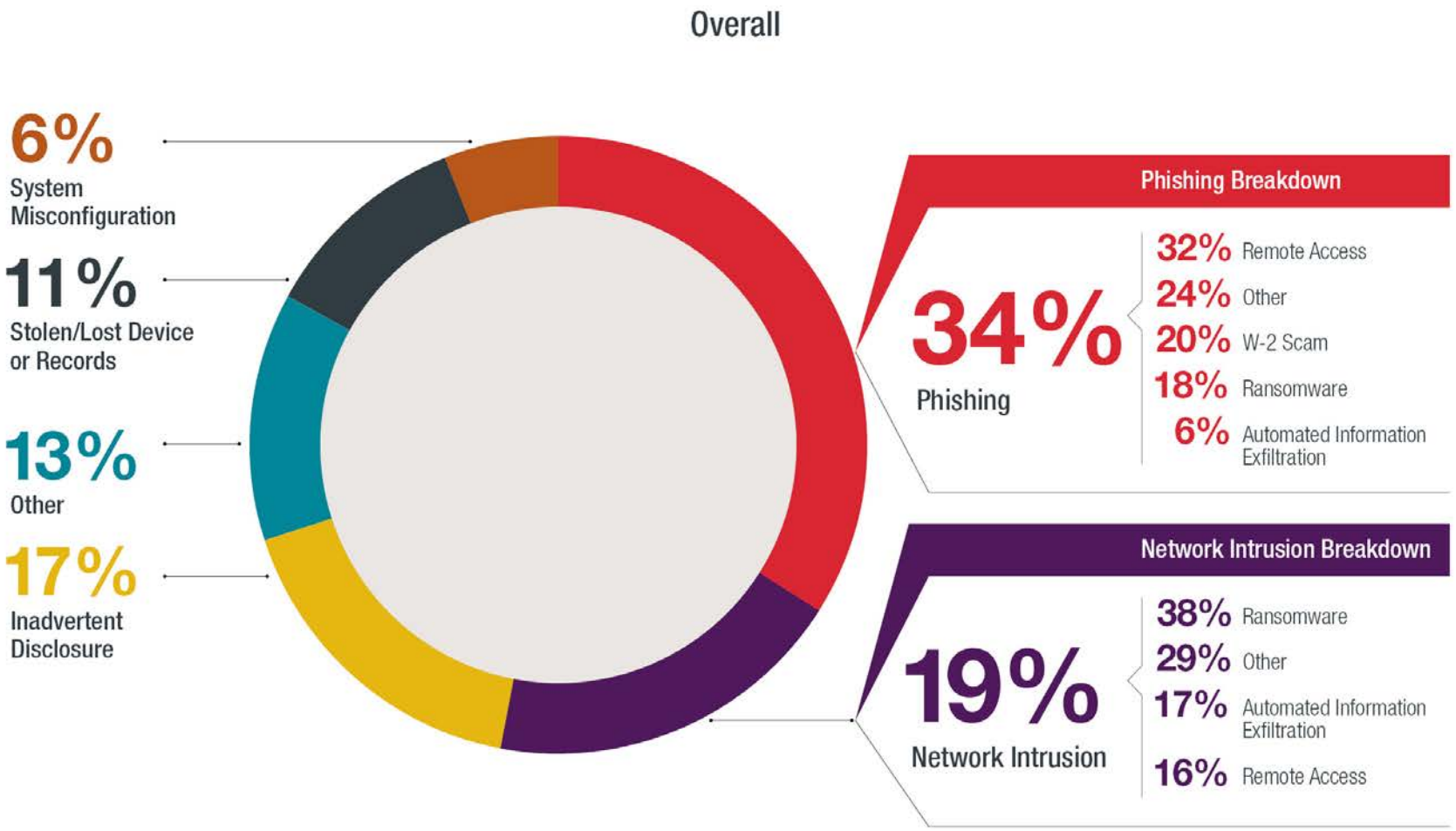
The overarching takeaway is that companies need to continue focusing on the basics to become and remain “Cyber Resilient”

- No one is immune
- Operational resiliency
- The people problem
- Practice
- Response metrics
- Choose carefully
- Let forensics drive the decision making
- Biggest consequences?

Industries Affected



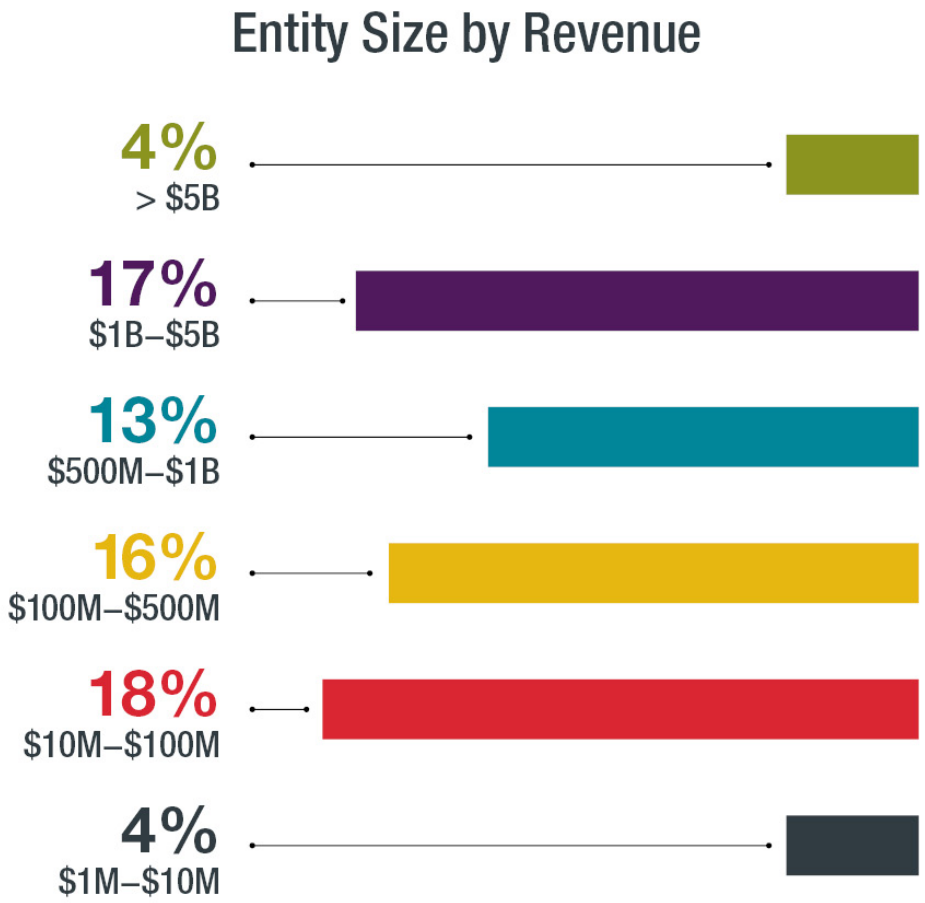
Why Do Incidents Occur?



Ransomware is not Going Away

- Critical reliance on technology
- New iterations affect mobile and IoT devices
- Low entry cost for cybercriminals
- Business oriented ransomware models are:
  - Developing new strains
  - Engaging in customer service
  - Data mining

Companies of all Sizes Impacted



Forensic Investigations

Average Forensic Investigation Costs

$84,417
All Incidents

$436,938
20 Largest Investigations

100%
Increase Over Last Year

Use of Outside Forensics

65%
of Network Intrusion Incidents

41.5%
of Data Breach Incidents

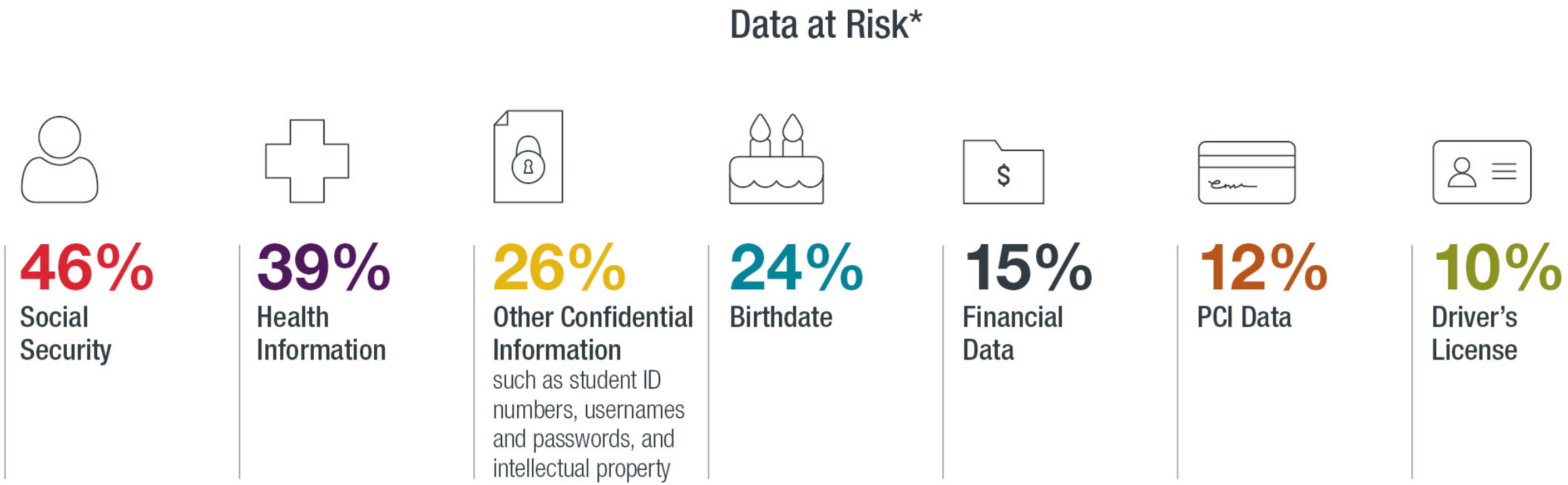
Average Completion Time for Forensic Investigation

24%
Evidence of Data Exfiltration in Network Intrusion Incidents

Critical Steps:

- Identify a forensic firm
- Conduct onboarding
- Collect good log data accessible from a centralized source

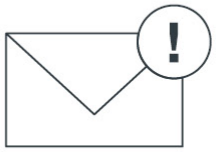
Data at Risk



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

Notification Summary

Number of Individuals Notified



AVERAGE:

87,952

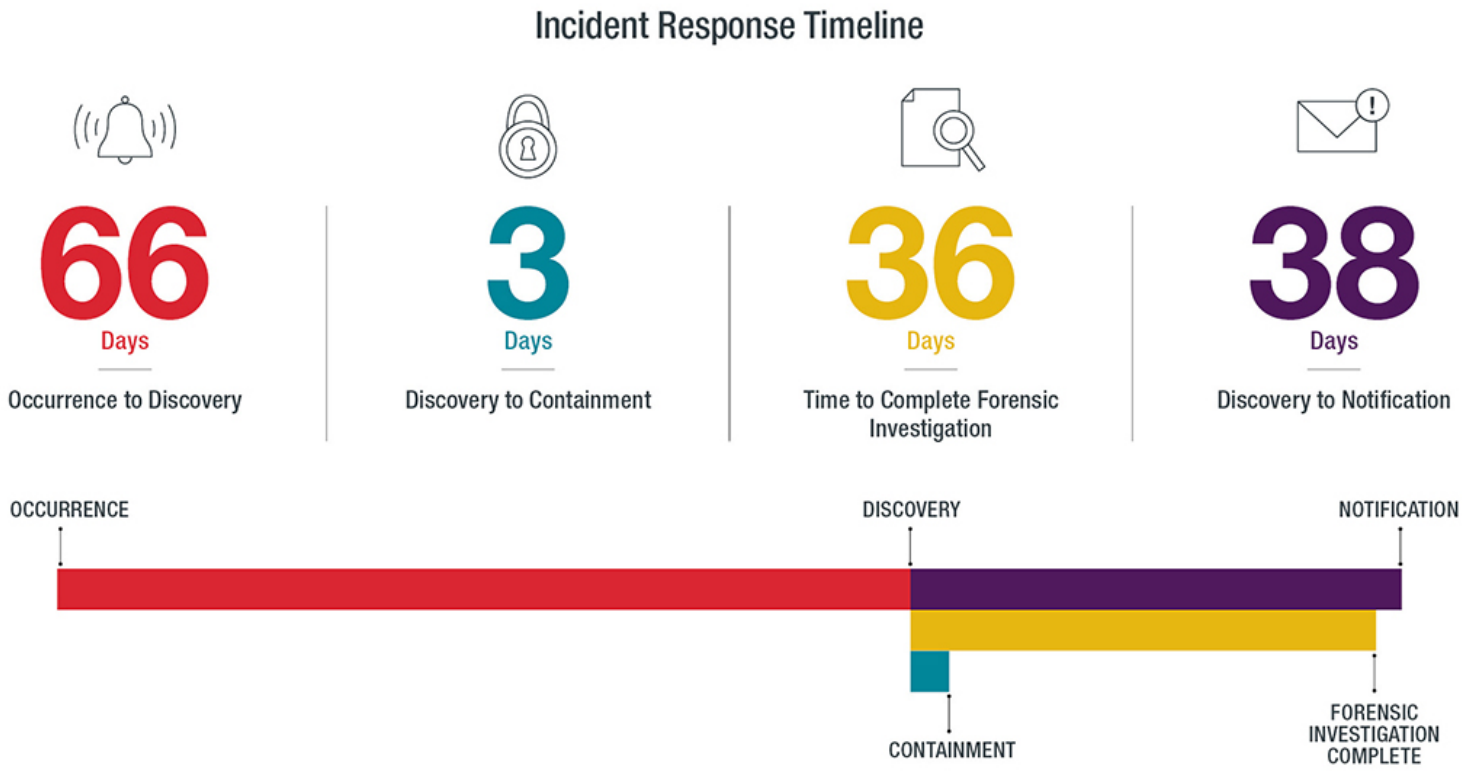
Notifications by Industry

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.

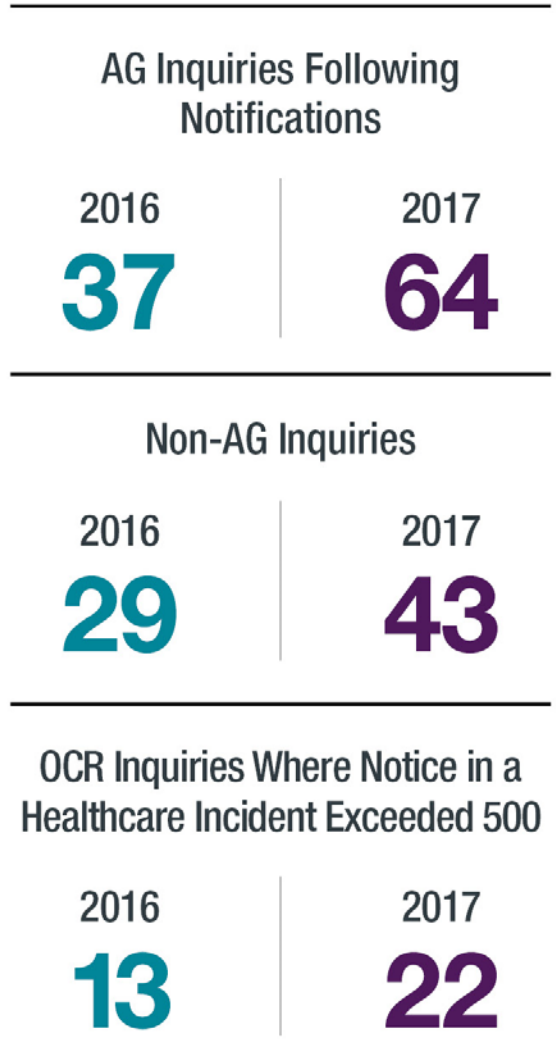
Incident Response Timeline



Attorneys General are Active

Be prepared to provide the following information:

- Detailed timeline of the incident
- Narrative describing the incident
- How the incident was discovered
- Company polices/procedures addressing information security
- Safeguards and corrective actions taken Complaints received
- Details of the mitigation efforts



Payment Card Data

2017 Per Card Assessment Range for Operating Expense and Fraud

$4-$20

Credit Monitoring Offered When Notification Occurred

60%

Average Redemption

35%

- Timing
- Cost
- Fines
- Trends

EU Security Incident Response Rules

- Describe nature of the brief
- Include contact information for the organization’s Data Protection officer
- Detail the consequences of the breach
- List remediation and mitigation steps they have taken or will take in response.

Back to the Basics – 12 Steps to Building Cyber Resilience
Compromise Response Intelligence in Action

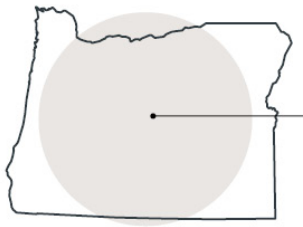
---

1. Increase Awareness of Cybersecurity Issues
2. Identify and Implement Basic Security Measures
3. Create a Forensics Plan
4. Build Business Continuity Into Your Incident Response Plan (IRP)
5. Manage Your Vendors
6. Combat Ransomware
7. Purchase the Right Cyber Insurance Policy
8. Implement a Strong Top-down Risk Management Program
9. Adopt Updated Password Guidance, and Implement MFA or Other Risk-based Authentication Controls
10. Keep Data Secure in the Cloud
11. Prepare for More Regulatory Inquiries
12. Publicly Traded Entities Should Update Risk Factors Regarding Privacy and Security

Data Security Litigation Trends

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.

Data Security Litigation: Take Action

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.

Developing a Defense Strategy

- Consider a variety of factors before seeking dismissal for lack of standing, including:
  1. How does the jurisdiction view standing?
  2. Has the plaintiff suffered identity theft or other harm?
  3. What happens if the case is dismissed?
- Be prepared to respond as plaintiffs continue to test new angles to advance beyond the dismissal stage, such as unjust enrichment or breach of contract

BakerHostetler

Atlanta
Chicago
Cincinnati
Cleveland
Columbus
Costa Mesa
Denver
Houston
Los Angeles
New York
Orlando
Philadelphia
Seattle
Washington, DC

bakerlaw.com