2017 Data Security Incident Response Report

Be Compromise Ready: Go Back to the Basics

BakerHostetler

May 9, 2017
Contact Information

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

Casie D. Collignon
Partner
Denver
303.764.4037
ccollignon@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

- 40+ member team
- 15+ members for incident response
- Chambers ranked
- Legal 500 ranked
- Law360 Privacy Team of the Year (2013 - 2015)
- Law360 Privacy MVPs (2013 - 2016)
- Law360 Privacy “Rising Stars” (2013 - 2016)
- Over 2,000 incidents
The 2017 Report

- 450+ incidents
- All industries represented
- Companies of all sizes impacted
- Ransomware is not going away
- People are your greatest risk
- Basic steps to be compromise ready
Incident Response Trends

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

- Healthcare: 35%
- Finance & Insurance: 16%
- Education: 14%
- Retail/Restaurant/Hospitality: 13%
- Other: 9%
- Business & Professional Services: 8%
- Government: 5%
Why Do Incidents Occur?

- **43%**: Phishing/Hacking/Malware
- **32%**: Employee Action/Mistake
- **18%**: Lost/Stolen Device or Records
- **4%**: Other Criminal Acts
- **3%**: Internal Theft

23% of these involved ransomware
25% of these involved phishing
Healthcare

**Causes**
- Phishing/Hacking/Malware
- Employee Action/Mistake
- Lost/Stolen Device or Records
- Other Criminal Acts
- Internal Theft
- Unknown

**HEALTHCARE**

- 38%
- 19%
- 6%
- 1%
- 36%
Finance & Insurance

FINANCE & INSURANCE

Causes
- Phishing/Hacking/Malware
- Employee Action/Mistake
- Lost/Stolen Device or Records
- Other Criminal Acts
- Internal Theft
- Unknown

1% 4% 11% 18% 27% 39%
Retail/Restaurant/Hospitality

RETAIL/RESTAURANT/HOSPITALITY

65%

9%
12%
14%

Causes
- Phishing/Hacking/Malware
- Employee Action/Mistake
- Lost/Stolen Device or Records
- Other Criminal Acts
- Internal Theft
- Unknown
Ransomware is here to Stay

• 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
Forensic Investigations

Critical Steps:
• Identify a forensic firm
• Conduct onboarding
• Use a centralized logging source

Completion of a network intrusion investigation after hire

Average cost of network intrusion investigation

Evidence of data exfiltration in network intrusion incidents

44 DAYS

$93,322

34%
Data at Risk

- 43% involved SSNs
- 37% involved health information
- 12% involved payment card data
- 10% involved intellectual property
- 10% involved usernames and passwords
Notification Summary

Average number of individuals notified: 77,230
Incident Response Timeline

- **61 DAYS**
  - Occurrence to discovery

- **8 DAYS**
  - Discovery to containment

- **40 DAYS**
  - Engagement of forensics until forensic investigation complete

- **41 DAYS**
  - Discovery to notification
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 policies/procedures addressing information security
• Safeguards and corrective actions taken
• Complaints received
• Details of the mitigation efforts

29%
Incidents Made Public

Frequency of regulatory investigations and litigation after the incident is made public

- 11% Regulatory Investigations or Inquiries
- 3% Litigation
Tailoring Offerings to Data at Risk

More individuals are taking advantage of free credit monitoring services. Average redemption rate rose from 10% in 2015.

- 26% Average credit monitoring redemption rate
- 64% Credit monitoring offered

*Be aware of potential impact on litigation.
The per-card range of the initial demand for operating expense and fraud

2014
$3-$25

2015
$7-$65

2016

$30 - median assessment per card
125,000 - median number of at-risk cards
EU Security Incident Response Rules

• Describe nature of the breach
• 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 – 7 Steps to Making Your Organization Compromise Ready

1. Increase Awareness of Cybersecurity Issues
2. Identify and Implement Basic Security Measures
3. Create a Forensic Plan
4. Build Business Continuity Into Your Incident Response Plan (IRP)
5. Manage Your Vendors
6. Prepare for Ransomware
7. Purchase the Right Cyber Insurance Policy
Data Security Litigation Trends

Industries Impacted by Data Breach Litigation

- 64% Healthcare
- 12% Supermarket Business
- 12% Hotel & Restaurant
- 8% Pharmacy & Retail
- 4% Education
Type of Data Breach

- **64%** Network Intrusion
- **24%** Lost or Stolen Computers
- **8%** Phishing
- **4%** Unauthorized Employee Access
Causes of Action

92% NEGLIGENCE

56% BREACH OF CONTRACT
56% VIOLATIONS OF STATE CONSUMER LAWS
36% VIOLATIONS OF STATE DATA BREACH NOTICE STATUTES
32% STATE PRIVACY STATUTES
Injuries Claimed

- 80% Potential Identity Theft
- 72% Actual Financial Harm
- 44% Actual Identity Theft
- 36% Overpayment for Services/Unjust Enrichment
- 32% Loss of Inherent Value of Information
Filed Motions to Dismiss

On average, it took approximately 303 days from the time a complaint was filed to the time the court ruled on a motion to dismiss.
What these Stats Mean for Developing a Defense Strategy

• Should a standing motion be filed at all?
  – How does the jurisdiction view standing?
  – What happens if the case is dismissed?
  – Has any plaintiff suffered identity theft or harm?

• What claims are surviving dismissal and are your motions setting you up for successful class certification motions?
  – Unjust enrichment
  – Implied contracts / implied terms in contracts
  – Negligence
  – Overpayment
  – Injunctions
These materials have been prepared by Baker & Hostetler LLP for informational purposes only and are not legal advice. The information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this information without seeking professional counsel. You should consult a lawyer for individual advice regarding your own situation.