Investigation and Notification of Data Breaches: A U.S. Perspective

Melinda L. McLellan
Partner, BakerHostetler

James A. Sherer
Partner, BakerHostetler
Incident Causes

Overall

6% System Misconfiguration
11% Stolen/Lost Device or Records
13% Other
17% Inadvertent Disclosure

Phishing

34%

32% Remote Access
24% Other
20% W-2 Scam
18% Ransomware
6% Automated Information Exfiltration

Network Intrusion

19%

38% Ransomware
29% Other
17% Automated Information Exfiltration
16% Remote Access

Source: 2018 BakerHostetler Data Security Incident Response Report
What Data is at Risk?

Some combination of this data in conjunction with a first name (or initial) and last name is generally the protected personally identifiable information (PII) by most state data breach statutes.

Source: 2018 BakerHostetler Data Security Incident Response Report
Forensic Investigations

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

**Use of Outside Forensics**
- 65% of Network Intrusion Incidents
- 41.5% of Data Breach Incidents

**Forensic Investigation Costs**
- $84,417 for All Incidents
- $86,751 for Network Intrusion Incidents
- $436,938 for 20 Largest Investigations

**Additional Data**
- Average Completion Time for Forensic Investigation: 36 Days
- Evidence of Data Exfiltration in Network Intrusion Incidents: 24%

*Source: 2018 BakerHostetler Data Security Incident Response Report*
Hackers use emails from a target organization’s CEO, asking human resources and accounting departments for employee W-2 information:

New Area Prone to Attack:

In 2017, hackers phished online payroll management account credentials used by corporate HR professionals.
Incident Response Timeline

- Occurrence to Discovery: 66 Days
- Discovery to Containment: 3 Days
- Time to Complete Forensic Investigation: 36 Days
- Discovery to Notification: 38 Days

Source: 2018 BakerHostetler Data Security Incident Response Report
Questions