UT LAW CLE | THE UNIVERSITY OF TEXAS SCHOOL OF LAW

PRESENTED AT

2016 Essential Cybersecurity Law

August 19, 2016
Austin, Texas

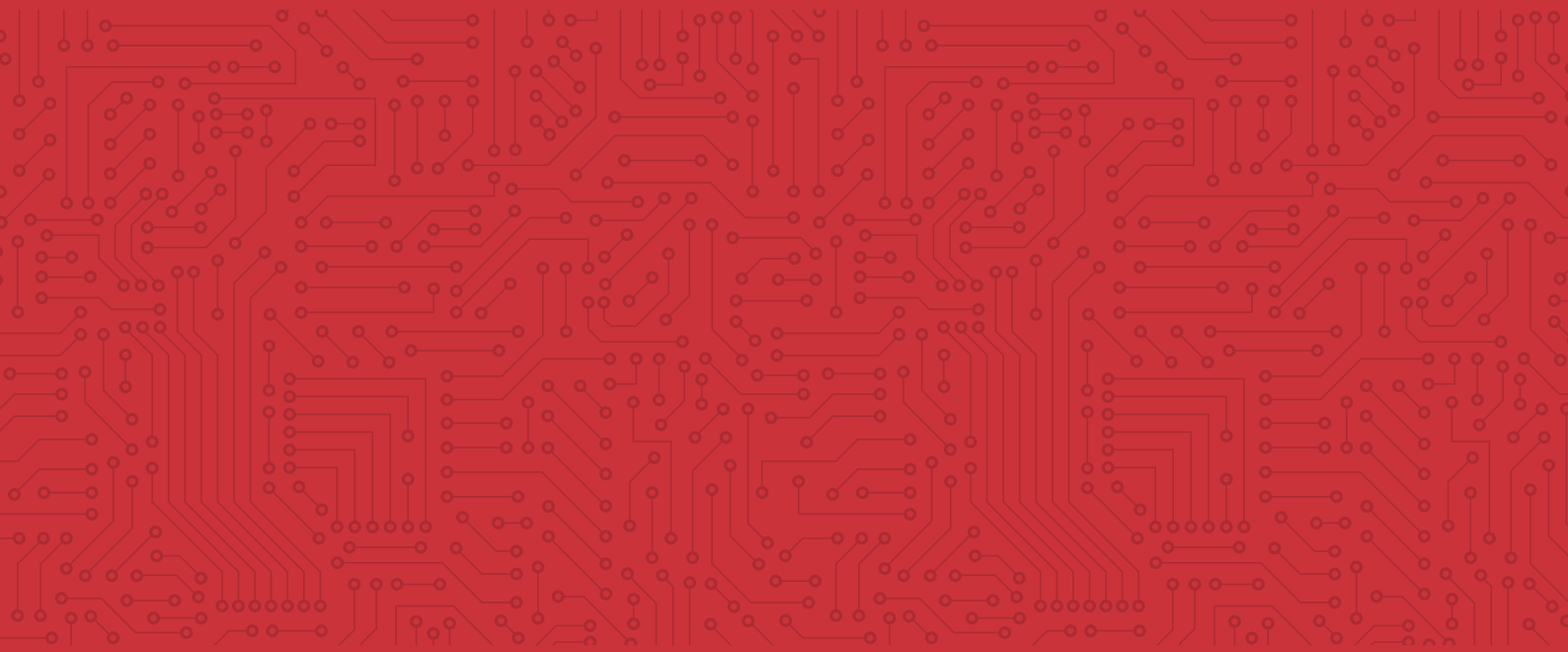
Is Your Organization Compromise Ready? 2016 Data Security Incident Response Report

William R. Daugherty

BakerHostetler

Is Your Organization Compromise Ready?

2016 Data Security Incident Response Report



SUMMARY

Incident Response Trends

The trends from last year's inaugural BakerHostetler Data Security Incident Response Report and this year's edition drive one primary recommendation—the continued need for companies to be "Compromise Ready."

Every company should be constantly focused on preventing, detecting, and having the right capabilities in place to respond to data security incidents. Accepting that incidents are inevitable does not mean that you stop trying to prevent them. Rather, in addition to reducing risk profiles through information governance and implementing preventative security measures, companies must focus on adapting measures to changing risks, faster detection, containment, and effective response. Central to this is improving preparedness based on internal and external "lessons learned."

The findings in this Report, developed from analyzing over 300 incidents we helped manage in 2015, are an important component of preparedness efforts. We have identified the issues and consequences companies actually experience. Budgets are tight, and employees are continuously being asked to take on more duties. Having insight into how these issues arise and the resulting financial impact can help companies prioritize and focus data security incident preparedness decision-making. This Report can also be used to win support for additional personnel and budget increases, and to help management and boards exercise appropriate oversight.

Not convinced that being compromise ready is important? Historically, the primary concern companies had about security incidents was the reputational impact caused by a public disclosure. Our experience shows reputational impact does not necessarily occur just by disclosing an incident. The hardest hits to a company's reputation are more likely to occur when the notification shows that the underlying cause should have been prevented or that the company is viewed as not handling the response well. And contrary to what many believe, a company that is quicker to notify is not always viewed more favorably.

We hope you find a way to use these findings to incrementally improve your company's level of preparedness.

300+
incidents in 2015

This Report shares "lessons learned" from more than 300 incidents in 2015.

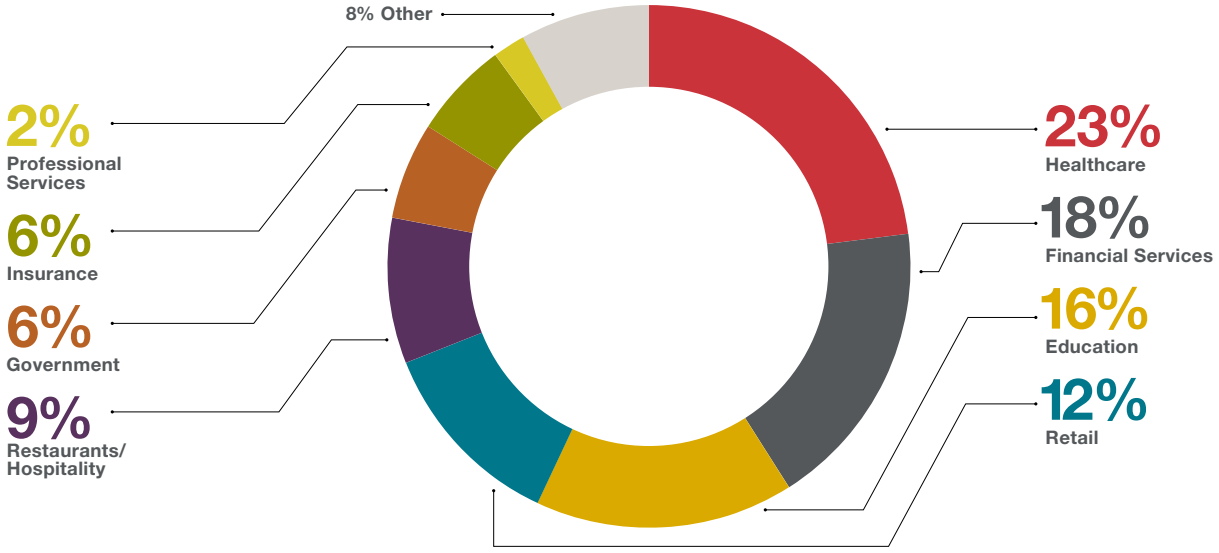
The incident response trends indicate:

- The range of incident causes is broad
- All industries are affected
- Detection capabilities need to improve
- It is difficult to provide meaningful notification quickly
- Identifying a forensic service provider before an incident occurs should be a priority
- Mitigation services are not always offered
- Regulatory investigations are more common than lawsuits after notification occurs

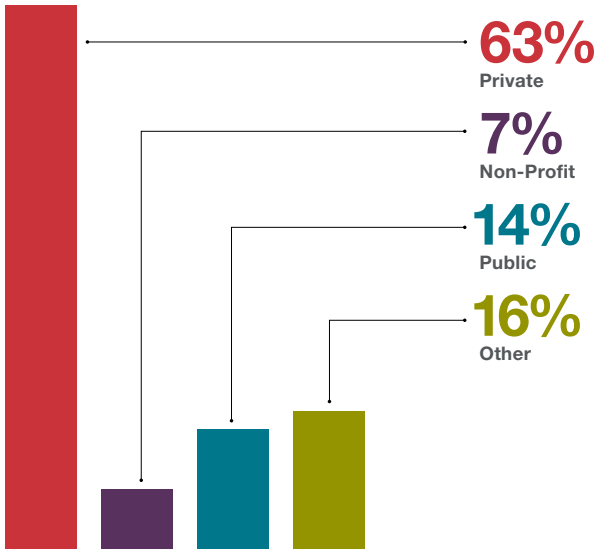
AT A GLANCE

Incident Response Trends

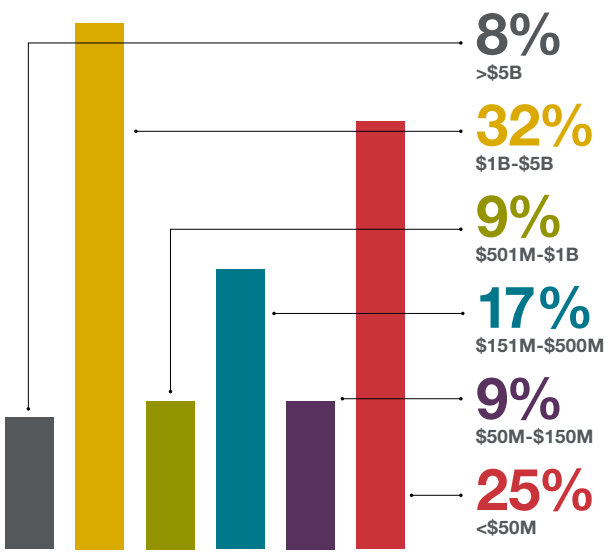
Industries Affected



Company Breakdown



Company Size by Revenue



Also available as part of the eCourse
Essential Cybersecurity Preparedness and Response: Internal Controls, Developing an Incident Response Plan and Responding to a Data Breach.

First appeared as part of the conference materials for the
2016 Essential Cybersecurity Law session
"Internal Controls and Compliance"