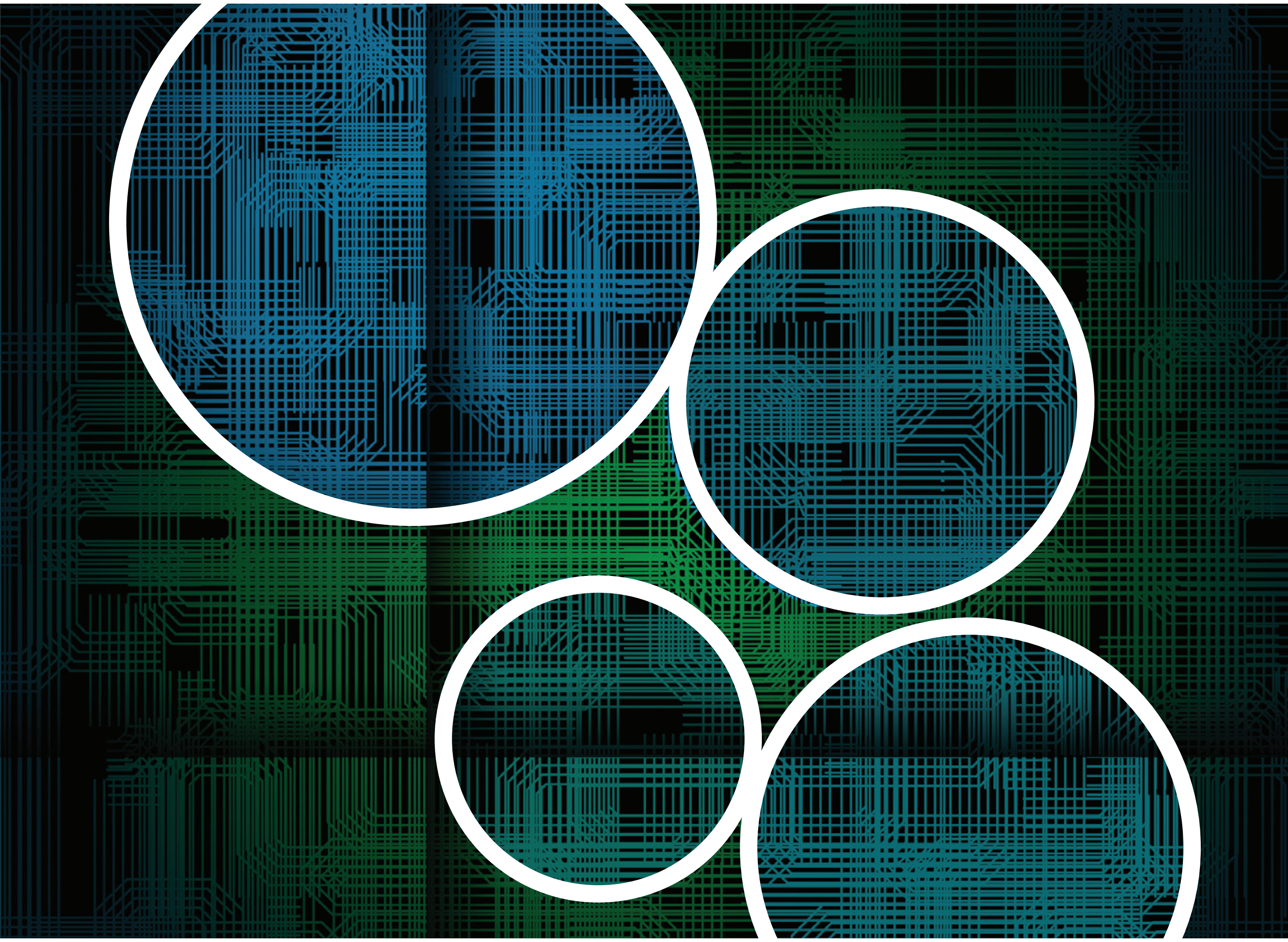
BakerHostetler

Be Compromise Ready: Go Back to the Basics

2017 Data Security
Incident Response Report



Contents

SUMMARY

Incident Response Trends

Cybersecurity carries a certain mystique. This comes from a combination of people not being “tech savvy,” sensationalized or incorrect headlines (“Guests Locked in Their Hotel Rooms by Ransomware”), superficial advice from so-called experts and technology-driven cure-alls. The reality is that if you focus on the basics, you will be better positioned to be “Compromise Ready.” Like other material risks companies face, cybersecurity readiness requires an enterprise wide approach tailored to the culture and industry of the company. There is no one-size-fits-all solution.

We started analyzing data collected from the hundreds of security incidents we manage annually to provide a resource for businesses to help focus their time and budgets in the right places. Clients have used our reports to prioritize and gain executive support for their security spending, educate their board and executive leadership team, fine-tune their incident response plans, vet and select forensic firms, build scenarios for tabletop exercises, and determine the type of cyber liability insurance needed. Our third year of reporting takes a look at the more than 450 incidents we worked on in 2016.

450+
incidents in 2016

Use this Report as a “crowdsourced” tool for identifying risks, response metrics and risk mitigation investment priorities.

The overarching takeaway is that companies need to continue focusing on the basics to become and remain “Compromise Ready.”

No one is immune. All entities face cyber risks because they have data that can be monetized or because they rely on technology to operate their business.

Operational resiliency. Theft of data is not the only risk. Ransomware and IoT-fueled DDoS attacks can shut down operations.

The people problem. Awareness and training help, but networks are built, maintained and used by people. People will continue to make mistakes and be phished or socially engineered.

Practice. Having an incident response plan is a good first step, but ongoing testing through tabletop exercises is better.

Response metrics. The time from incident occurrence to detection and from detection to containment show where improvement can be made. Identifying a forensic firm and onboarding that firm before an incident occurs is a primary way to improve.

Choose carefully. Not all forensic firms are created equal—vet them by experience, tools they use (e.g., image and analysis or endpoint agents) and approach.

Let the forensics drive the decision-making. Investigations take more than 40 days to complete, and what you know in the beginning is often incomplete or wrong. Unless you fall outside the normal range, timing of disclosure of an incident rarely is the sole source of a post-incident financial consequence.

Biggest consequences? Poor communications cause rifts in relationships with customers, stakeholders and employees. Although companies focus heavily on regulatory investigations and litigation, it is not a foregone conclusion that these will occur.

AT A GLANCE

Incident Response Trends

Causes

10% of all incidents involved ransomware

43%
Phishing/Hacking/ Malware

25%
of these involved phishing

23%
of these involved ransomware

32%
Employee Action/ Mistake

18%
Lost/Stolen Device or Records

4%
Other Criminal Acts

Internal Theft

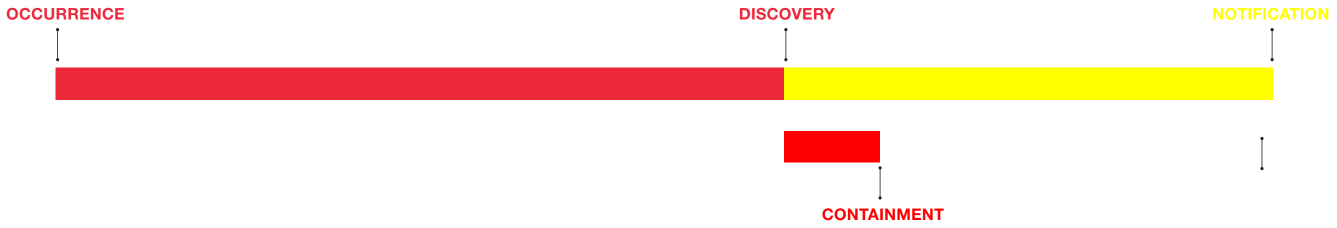
Incident Response Timeline

61
DAYS
Occurrence to discovery

8
DAYS
Discovery to containment

Engagement of forensics until forensic investigation complete

41
DAYS
Discovery to notification


OCCURRENCE
DISCOVERY
NOTIFICATION
CONTAINMENT