BakerHostetler

Cybersecurity and the Board of Directors

October 18, 2017

Introductions

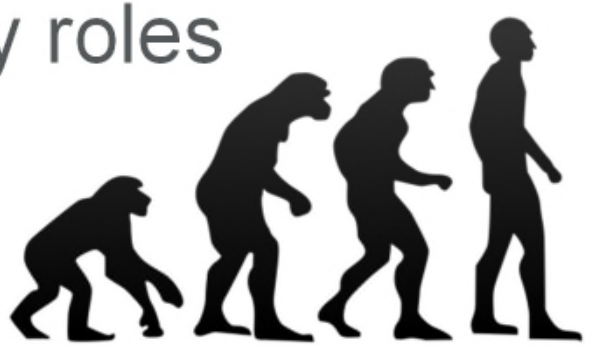
- Lloyd's of London Insurer & Cyber-Risk Mitigation Provider
- Only Insurer with an in-house data breach response team of privacy attorneys
- Over 6,000 breaches handled
- Risk management and pre-loss focus
- Advisen Best Cyber Risk Insurer 2016
- Advisen Cyber Risk Event Response Team of the Year 2014-2016
- Advisen Cyber Risk Pre-Breach Team of the Year 2017

BakerHostetler

- Chambers USA 2016 nationally ranked & Legal 500 ranked Privacy and Data Protection practice
- Privacy and Data Protection "Practice Group of the Year" by Law360
- Over 2,000 incidents handled (450+ in 2016 alone)
- Team includes 40+ attorneys specializing in privacy and data security law across the country

Evolution of Approaches

- Unaware
- “We have a vendor”
- “We have an IT department”
- “We don’t have anything hackers want”
- Delegated to IT/security
- Adding dedicated privacy/security roles
- Management buy-in
- Enterprise-wide risk approach



Be “Compromise Ready”

- Threat information gathering
- Technology – preventative & detective
- Personnel – awareness & training
- Security assessments
  - Understand where assets and sensitive data are located
  - Implement reasonable safeguards
  - Increase detection capabilities
- Vendor management
- Incident response plan and tabletop exercises
- Insurance
- Ongoing diligence and oversight

Cybersecurity – Boardroom/Executive Issue

BakerHostetler

Bloomberg Businessweek
Companies & Industries

SUBSCRIBE NOW

As Data Breach Woes Continue, Target's CEO Resigns

By Michael Riley and Dune Lawrence | May 15, 2014

Target CEO Gregg Steinhafel checks out Black Friday sale items on Nov. 22, 2013, in Bloomington, Minn.

Target's chairman and chief executive officer, Gregg Steinhafel, a 35-year c
veteran, is stepping down, as the massive pre-Christmas data breach suffer
Minnesota retailer continues to roil the company. The decision is effective
immediately, according to a statement posted today on the company's web
Mulligan, Target's chief financial officer, has been appointed as interim pre

THE WALL STREET JOURNAL. | TECH

WORLD CUP 2014

Corporate Boards Race to Shore Up Cybersecurity

Directors Grapple With Issues Once Consigned to Tech Experts

ARTICLE FREE PASS

$2 A WEEK SUBSCRIBE NOW

By DANNY YADRON

Ellen Richey, Visa's chief legal officer, wants more data encrypted. Bloomberg News

After a series of high-profile data breaches and warnings, corporate boards are w
to cyberthreats, grappling with security issues they once relegated to technology
experts.

Computer hacking is on the agenda these days when Kellogg Co. (K-0.22%)'s

THE D&O DIARY

A PERIODIC JOURNAL CONTAINING ITEMS OF INTEREST FROM THE WORLD OF DIRECTORS & OFFICERS LIABILITY, WITH OCCASIONAL COMMENTARY

Home » Cyber Liability » Wyndham Worldwide Board Hit with Cyber Breach-Related Derivative Lawsuit

Wyndham Worldwide Board Hit with Cyber Breach-Related Derivative Lawsuit

By Kevin LaCroix on May 7, 2014
Posted in Cyber Liability, Director and Officer Liability

WYNDHAM

In what is the latest example of the potential cybersecurity-related liability of corporate boards, a shareholder for Wyndham Worldwide Corporation has initiated a derivative lawsuit against certain directors and officers of the company, as well as against the company itself as nominal defendant, related to the three data breaches the company the company and its operating units sustained during the period April 2008 to January 2010. As discussed here, the company is already the target of a Federal Trade Commission enforcement action in connection with the breaches.

Risks and Costs

- Reputational – Lost Sales
- Disruption
- Remediation
- Stock drop?
- Regulatory
- Payment Card Network Liability
- Litigation
  - Consumer
  - Issuing Banks
  - Derivative

Cyber Risk Landscape

Sony Hackers Used Phishing Emails to Breach Company Networks

YAHOO!

Yahoo hack may become test case for SEC data breach disclosure rules

Neiman Marcus

The New York Times
Neiman Marcus Data Breach Worse Than First Said

Phishing attacks targeting W-2 data hit 41 organizations in Q1 2016

HBO data breach included thousands of internal documents

It's always more than you think...

Insurance giant Anthem hit by massive data breach

Anthem

Bloomberg

Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It

Incident Response Trends

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.

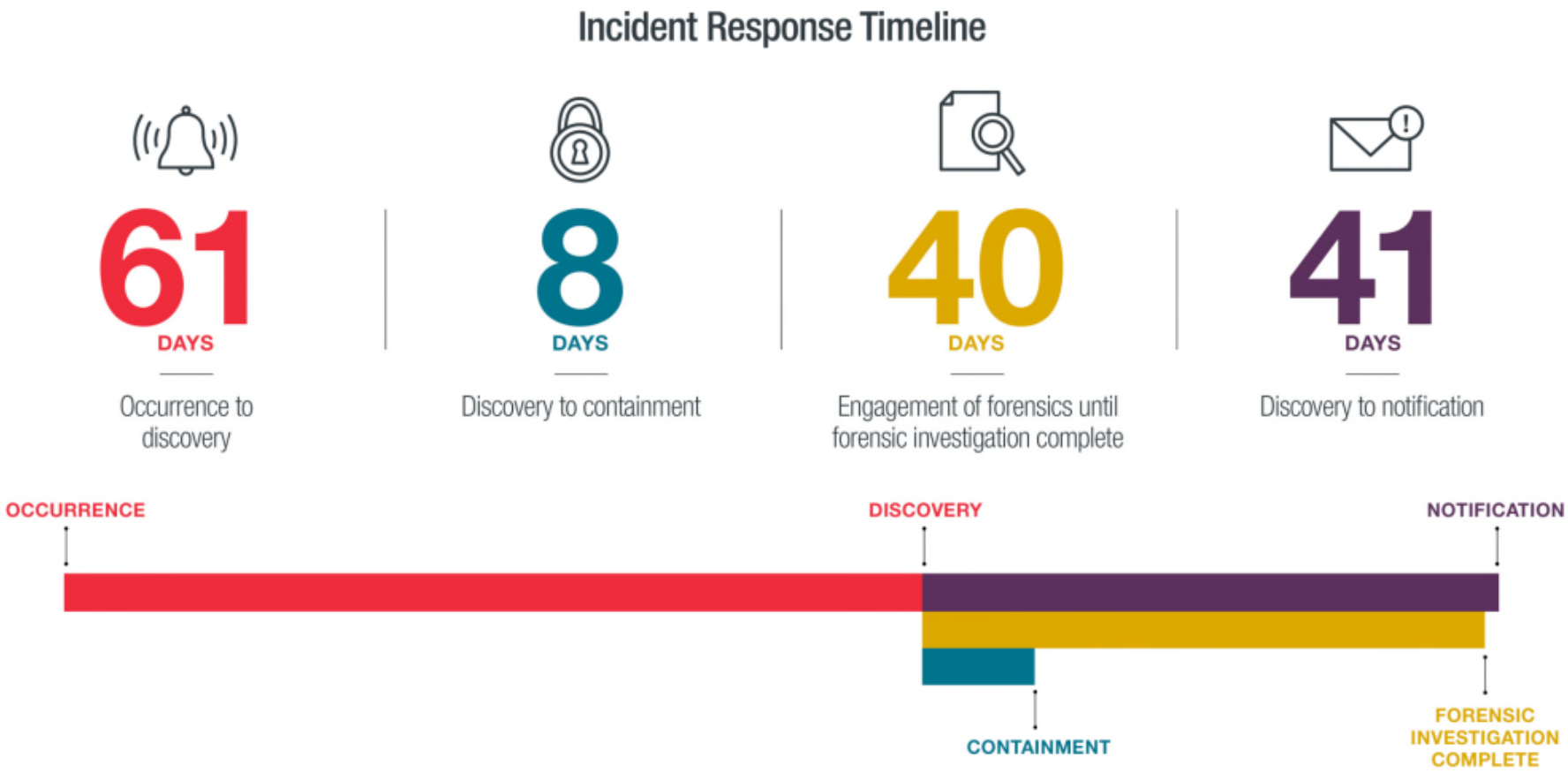
Response metrics.
The time from incident occurrence to detection and from detection to containment show where improvement can be made. Identifying a forensic firm and onboarding that firm before an incident occurs is a primary way to improve.

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.

Detection, Containment, Notification



BakerHostetler Data Security Incident Response Report 2017

Board Oversight of Cybersecurity Risk

BakerHostetler

- Directors do not have to become experts on cybersecurity and can rely on information and reports from management regarding cybersecurity
- The Board should:
  - Become knowledgeable regarding the company's cybersecurity risk;
  - Be comfortable that the company has appropriate controls in place to manage that risk; and
  - Monitor controls periodically to ensure that they are functioning as intended and that issues are being identified and addressed.

Duties and Consequences

- Duties owed by Directors and Officers
  - Duty of oversight
  - Duty to protect organizational assets
    - Extended to “digital assets”
- Known consequences
  - Easy to calculate?
  - Impact on stock price?
  - Direct costs: notification, litigation, regulatory actions, remediation
  - Indirect costs: reputational harm, diminished sales

NACD Published Guidance

1. Directors need to understand and approach cybersecurity as an enterprise-wide risk management issue, not just an IT issue.
2. Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances.
3. Boards should have adequate access to cybersecurity expertise, and discussions about cyber-risk management should be given regular and adequate time on the board meeting agenda.
4. Directors should set the expectation that management will establish an enterprise-wide risk management framework with adequate staffing and budget
5. Board-management discussion of cyber risk should include identification of which risks to avoid, accept, mitigate, or transfer through insurance, as well as specific plans associated with each approach.

NACD Director's Handbook on Cyber-Risk Oversight

Management Action Considerations

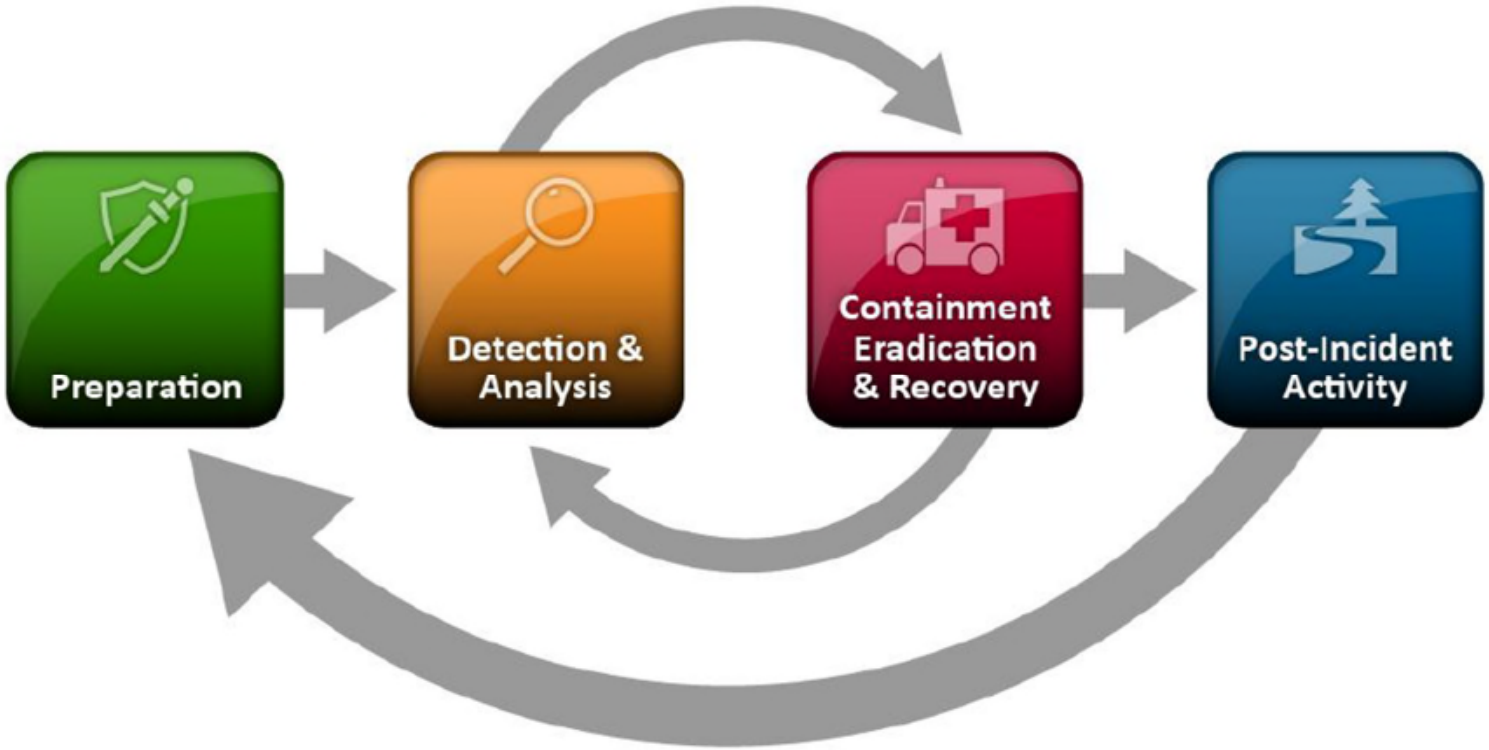
- Consider establishing a risk committee or use audit committee
- Review risk assessments
- Educate current Directors
- Evaluate whether company has appropriate privacy and security roles (e.g., CISO, CPO)
- Evaluate privacy and security budgets
- Regular reporting from management
- Address risk shifting through insurance

Preparing for a Data Breach and How to Respond

BakerHostetler

- Questions for your organization
  - Which states do you conduct business in?
  - Are there states with stricter data breach and privacy laws than others?
  - What constitutes a data breach in those states?
  - What are the reporting requirements?
  - Are there any safe harbors under the state laws?
- Many states do not require notification where data is encrypted.

Developing an Effective Incident Response Plan (“IRP”)



Source: NIST 800-61, Incident Response

The Board's Responsibility During Incident Response

BakerHostetler

- Timing of notification of the Board of a Security Incident
  - When management can assess potential impact
  - Start with the Chairperson of the Board and head Audit or Risk Committee, and other Board members as necessary
- Identify who communicates with the Board about a Security Incident
  - Key members of the executive management team
  - Key individuals involved with the investigation, such as the Chief Information Security Officer, the Privacy Officer, and legal counsel
- Management's responsibility for providing updates
  - When there are significant findings from the investigation
  - At key events and deadlines such as dates when notification letters, media notice, posting of web site notices, and regulatory notices will be completed
- Oversight of response service provider engagement, communications, and impact assessment

The Board's Responsibility During Incident Response

BakerHostetler

- Oversight of Vendor Retention
  - Forensics
  - Crisis Management
  - Outside Legal
  - Fulfillment House and Call Center
- Communications to External Parties
  - Credit Card Brands
  - Law Enforcement
  - Regulators
  - Affected Individuals
- Impact on Business Operations

Communications Strategy

- **When**: Do you have useful and reliable information that will not change?
  - Ideally, not sooner than containment
- **What**: Can you answer four key questions?
  - Hard to get to this point faster than 30 days
- **How**: Legal v. Relationship?
- **By Whom**: When is hearing from the CEO most impactful?

2011 SEC Guidance on Cyber Risk Disclosure

- "[R]egistrants should consider the possibility of cyber incidents occurring and the quantitative and qualitative magnitude of those risks, including the potential costs and other consequences resulting from misappropriation of assets or sensitive information, corruption of data or operational disruption."

Cyber Risks and Your Company 10-K

BakerHostetler

- Sections Implicated:
  - Risk Factors
  - MD&A
  - Description of Business
  - Legal Proceedings
  - Financial Statement Disclosures (e.g. material prevention costs, or losses sustained)

NY DFS Board Responsibilities

- Must approve written policies and procedures for the protection of company Information Systems and Nonpublic Information stored thereon
- Must receive written briefing at least annually from CISO covering, among other things, organization's material cyber risks, effectiveness of organization's cybersecurity program, and material Cybersecurity Events involving the organization during the period covered by the briefing
- Must certify compliance with the Regulations
  - Chairperson must personally sign off

Regulatory “Hot Buttons”

- Encryption of Portable Devices
- Patching
- Security Awareness and Training
- Two-Factor Authentication for Remote Access
- Ignoring Risk Assessments
- Slow Detection
- Slow Notification
- Repeat Offenders

Lessons Learned - D & O Litigation

Home Depot Settlement – required certain corporate governance reformed aimed at correcting "deficiencies …regarding the Board's oversight and responsibility for data security."

1. Document the duties and responsibilities of CISO
2. Periodically conduct Table Top Cyber Exercises
3. Monitor and periodically assess IOC's
4. Maintain executive-level committee focused on Company data security
5. Receive reports on Company IT budget and the percentage of IT budget spent on cybersecurity measures
6. Maintain an Incident Response Team and Incident Response Plan

Bringing Cybersecurity onto the Board

- Cybersecurity Disclosure Act of 2017 – proposed legislations would require the SEC to issue final rules requiring all reporting companies:
  1. to disclose whether any member of the governing body has any expertise or experience in cybersecurity, and the nature of that expertise and experience; OR
  2. if no governing body member has expertise or experience in cybersecurity, to describe what other cybersecurity steps taken by the reporting company were taken into account by persons responsible for nominating individuals to the governing body.

Getting Up to Speed – 6 Questions for Your Next Board Agenda

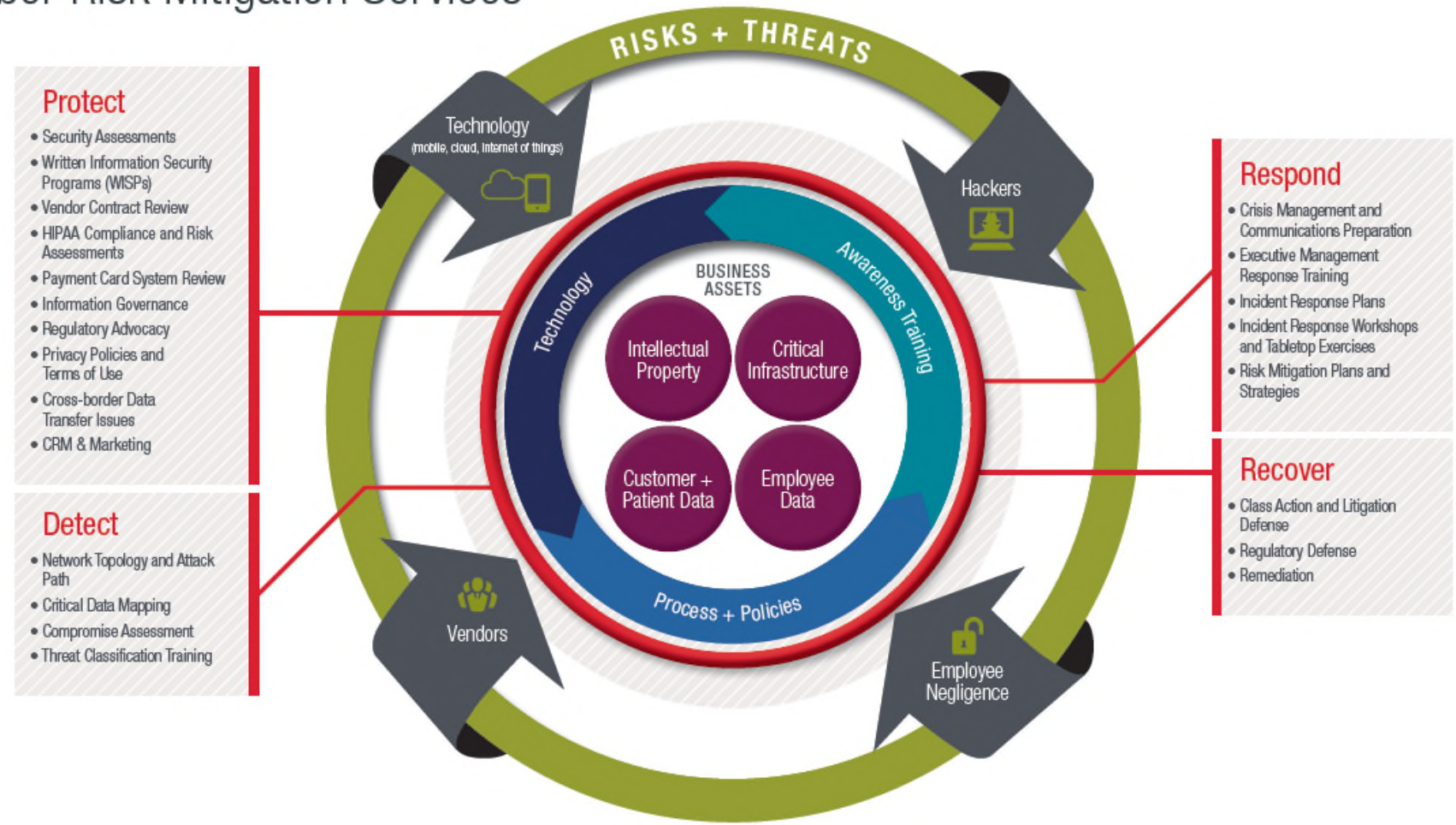
BakerHostetler

1. Does the organization follow any prescribed security framework?
2. What are the top five risks the organization has related to cybersecurity?
3. How are employees made aware of their role related to cybersecurity?
4. Are external and internal threats considered when planning cybersecurity program activities
5. How is security governance managed within the organization?
6. In the event of a serious breach, has management developed a robust response protocol?

ISACA and IIA, “Cybersecurity: What the Board of Directors Needs to Ask.”

BakerHostetler

Cyber Risk Mitigation Services



BakerHostetler

Questions?

Theodore J. Kobus III
New York
T +1.212.271.1504
tkobus@bakerlaw.com

Disclaimer

The descriptions contained in this communication are for preliminary informational purposes only and should not be taken as legal advice. The product is available on an admitted basis in some but not all US jurisdictions through Beazley Insurance Company, Inc., and is available on a surplus lines basis through licensed surplus lines brokers underwritten by Beazley syndicates at Lloyd's. The exact coverage afforded by the product described herein is subject to and governed by the terms and conditions of each policy issued. The publication and delivery of the information contained herein is not intended as a solicitation for the purchase of insurance on any US risk. Beazley USA Services, Inc. is licensed and regulated by insurance regulatory authorities in the respective states of the US and transacts business in the State of California as Beazley Insurance Services (License#: 0G55497). CBEM606_US_10/17

BakerHostetler

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

bakerlaw.com