ReedSmith

The business of relationships.

IT, Privacy & Data Security

Webinar

Incident Response and Cybersecurity: A View from the Boardroom

Gerard M. Stegmaier, Reed Smith
Partner – IT, Privacy & Data Security

Samuel F. Cullari, Reed Smith
Counsel – IT, Privacy & Data Security

Paul Luehr, Stroz Friedberg
Executive Managing Director

September 22, 2016

Threat Landscape: Data Breach Costs

$6.5 M

U.S. average cost of a data breach ($4 M globally)

29%

Increase since 2013, in global cost of a breach

$221

U.S. average cost for each exposed record ($158 globally)

Source: Ponemon Institute, “2016 Cost of Data Breach Study: Global Analysis,” Sponsored by IBM (June 2016)

Threat Landscape: Data Breach Costs (cont.)

66%

Indirect Costs:

- Staff hours
- Lost Goodwill
- Customer “Churn”

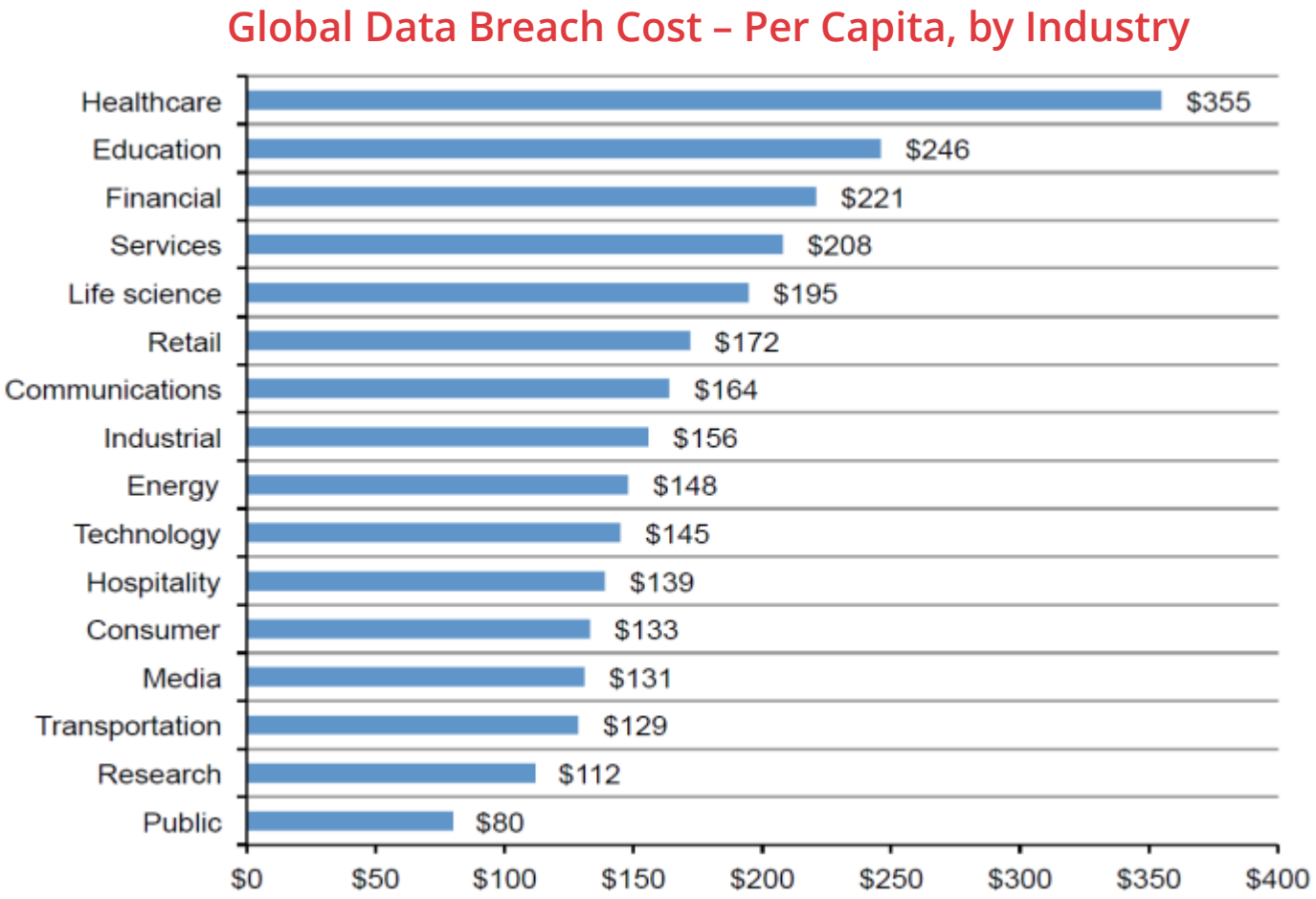
34%

Direct Costs:

- Outside Counsel
- Outside Experts
- ID Theft Insurance
- Notification Costs

Source: Ponemon Institute, “2016 Cost of Data Breach Study: Global Analysis,” Sponsored by IBM (June 2016)

Threat Landscape: Per Capita Costs



Source: Ponemon Institute, "2016 Cost of Data Breach Study: Global Analysis," Sponsored by IBM (June 2016)

The Evolving Regulatory Landscape (cont.)

Where's Your Data?

Not If, But When the Breach Hits

The Board's Role in Overseeing Cyber and Privacy Risk

Reed Smith LLP

The *Caremark* Standard

- In 1996, the Delaware Chancery Court decided *In re Caremark Int'l Inc. Derivative Litigation*
  - Directors must "appropriately monitor and supervise the enterprise," including by making a good faith effort to implement an adequate corporate information and reporting system.
  - Failing to monitor can constitute an "unconsidered failure of the board to act in circumstances in which due attention would, arguably, have prevented the loss."

Caremark Refined: *Stone v. Ritter*

- In 2006, the Delaware Supreme Court refined the parameters of *Caremark*
  - A board could be liable to shareholders if it:
    - "utterly failed to implement any reporting or information system or controls" or
    - "having implemented such a system or controls, consciously failed to monitor or oversee its operations."
  - The imposition of liability "requires a showing that the directors knew that they were not discharging their fiduciary obligations."

Caremark's Requirements for Directors

- Understand Nature of the Risks
  - Understanding of the specific cyber and privacy risks facing the company.
- Understand Systems in Place to Address the Risks
  - Understanding of the policies, controls, and procedures in place to identify, manage, and mitigate cyber and privacy risks.
- Make Decisions Based on Those Understandings

Caremark in Action: Wyndham Derivative Litigation

- After the data breaches affecting Wyndham Worldwide Corp., shareholders brought a derivative action against Wyndham's board based on its alleged failure to implement adequate security mechanisms.
- In 2014, a court dismissed the suit, finding that the board discharged its duties under *Caremark* by:
  - Discussing data breaches at 14 meetings between 2008 and 2012
  - Having the Wyndham Audit Committee discuss data breaches 16 times during the same period
  - Engaging an outside technology firm to assess Wyndham's information security policies

Before a Breach

Inventory Data

- Value, sensitivity
- What, where, how is it stored, used, and shared

Review Policies & Agreements

- Privacy policies and disclosures
- Vendor agreements
- Data Security

Before a Breach (cont.)

Conduct Assessments

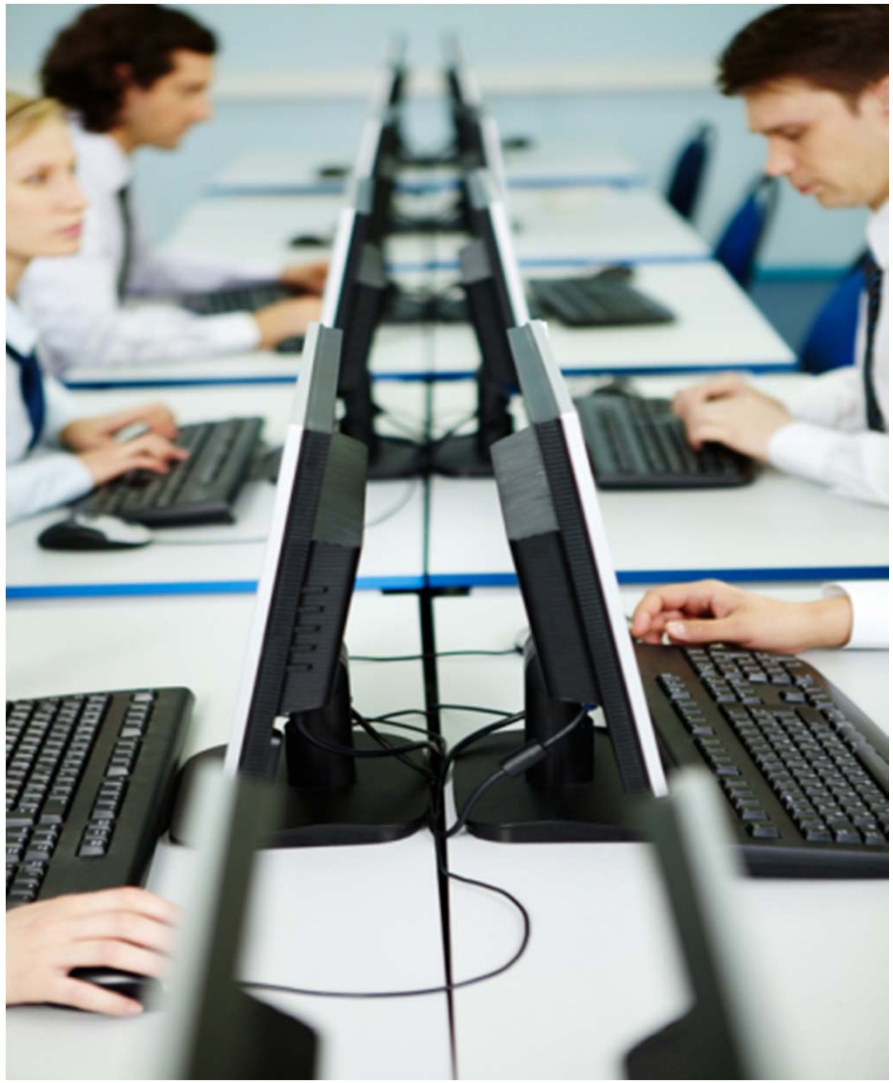
- Periodic privacy reviews
- Annual risk/gap assessments

Train employees

- Privacy and data security responsibilities
- Incident response

Set the Tone

- Privacy and data security are core company values



Before a Breach (cont.)

- Three Critical Areas of Operations
  - Performing Regular Risk Assessments
  - Developing a Robust Incident Response (IR) Plan
  - Creating an Effective Governance Structure

Before a Breach (cont.)

The Assessment Process:

Business priorities, constraints

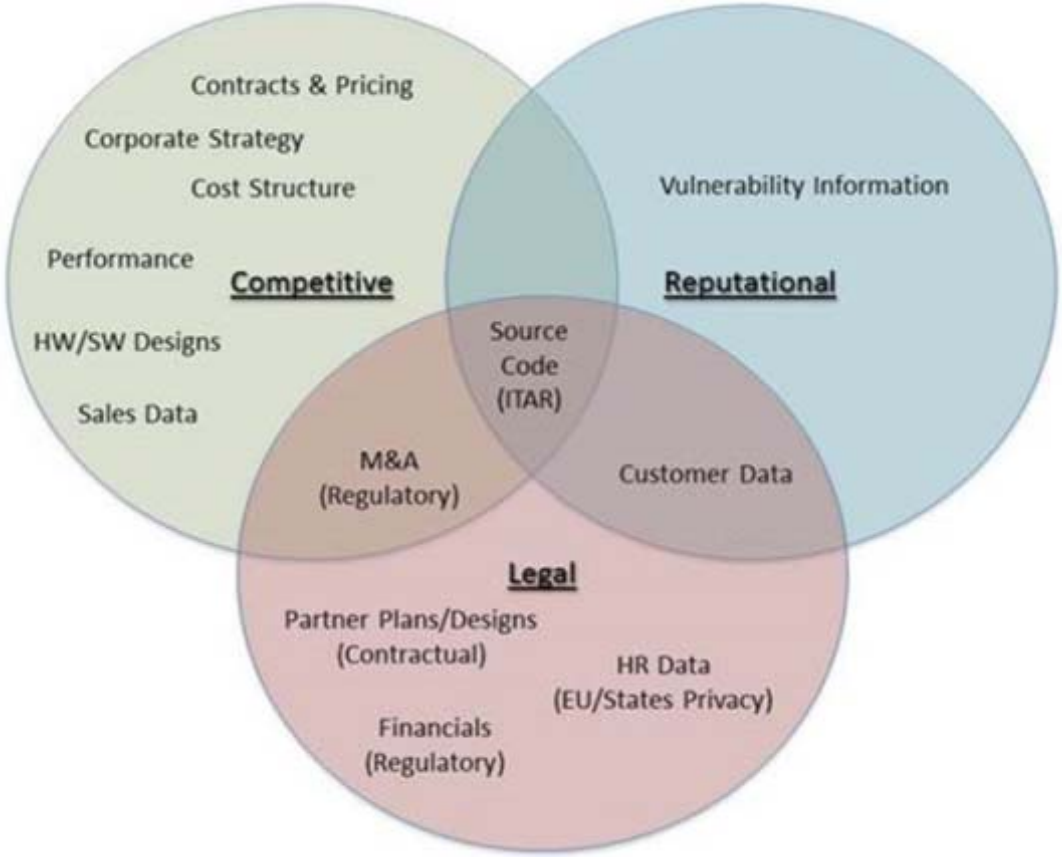
Operational environment

Security Standard:
NIST, ISO 27001, SANS 20, HIPAA, etc.

Prioritized security risk findings & recommendations

Before a Breach (cont.)

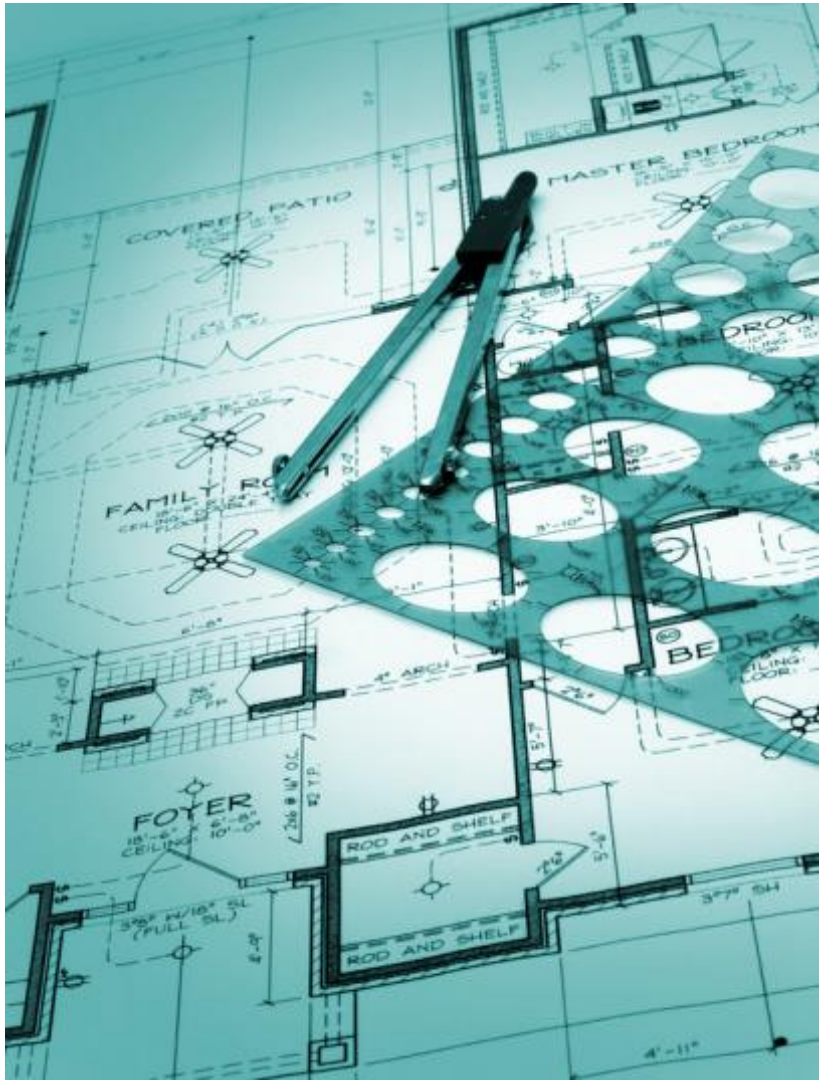
Understand Risk



Before a Breach (cont.)

Create a Robust IR Plan

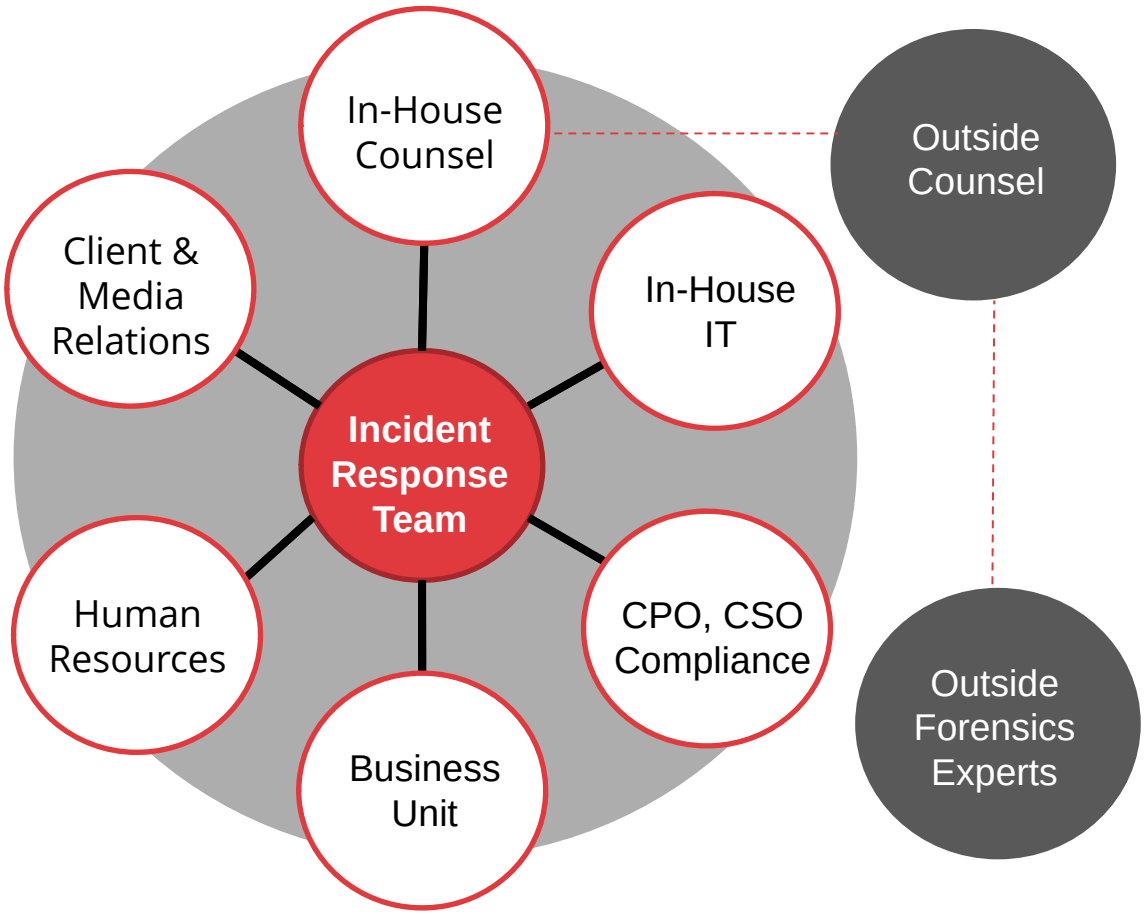
- Management endorsement
- Cross-disciplinary team
- Contact lists
- Legal analysis and timeline
- Categories of adverse events
- Escalation process
- Communications plan



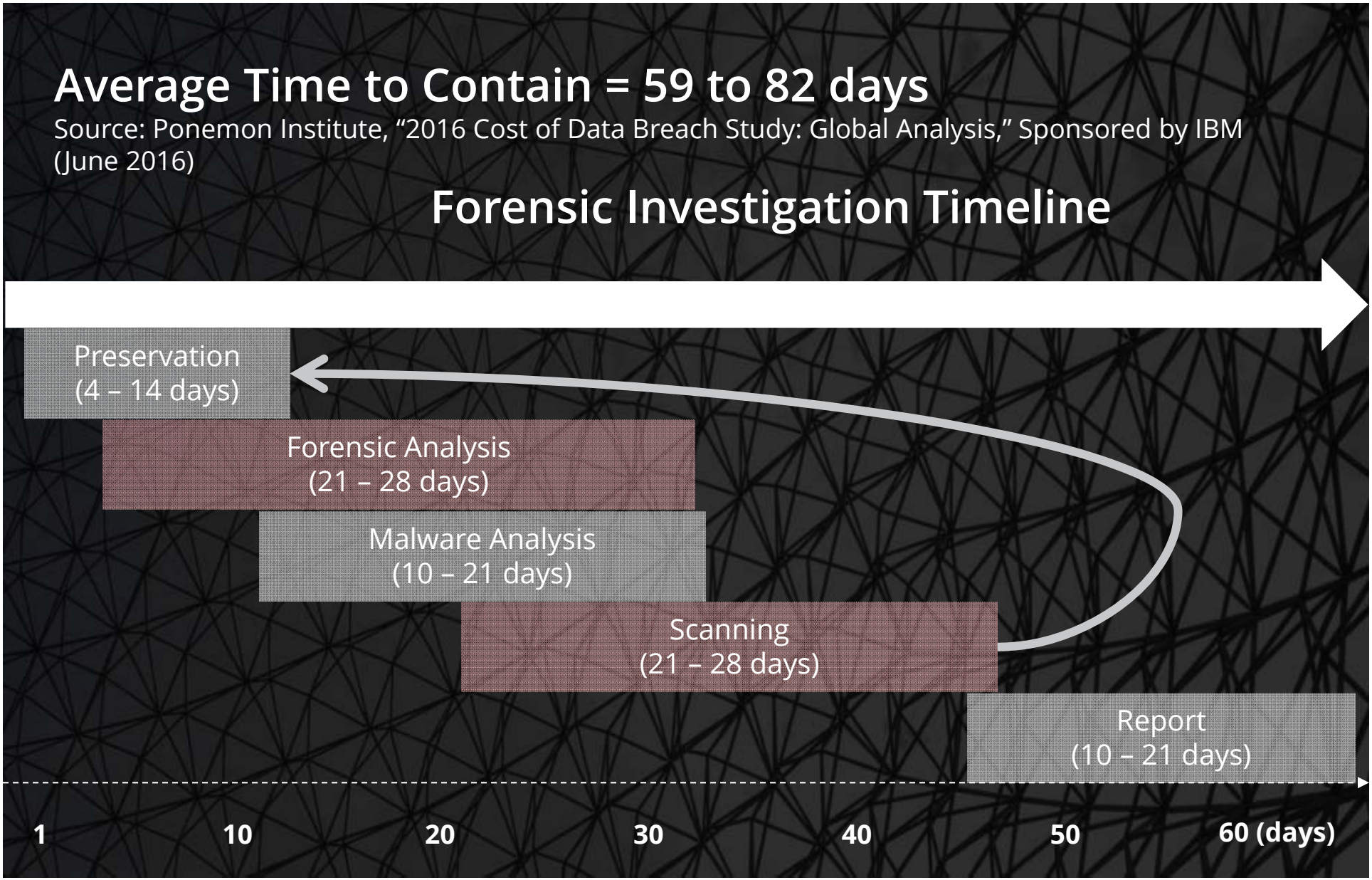
Response Plan: People

Deploy an Effective IR Team

- Multiple representatives
- Led by counsel
- With contact sheet for:
  - Outside counsel
  - Forensic experts
  - Crisis communicators
  - Notification firms
  - Insurance agent/broker
  - Law enforcement



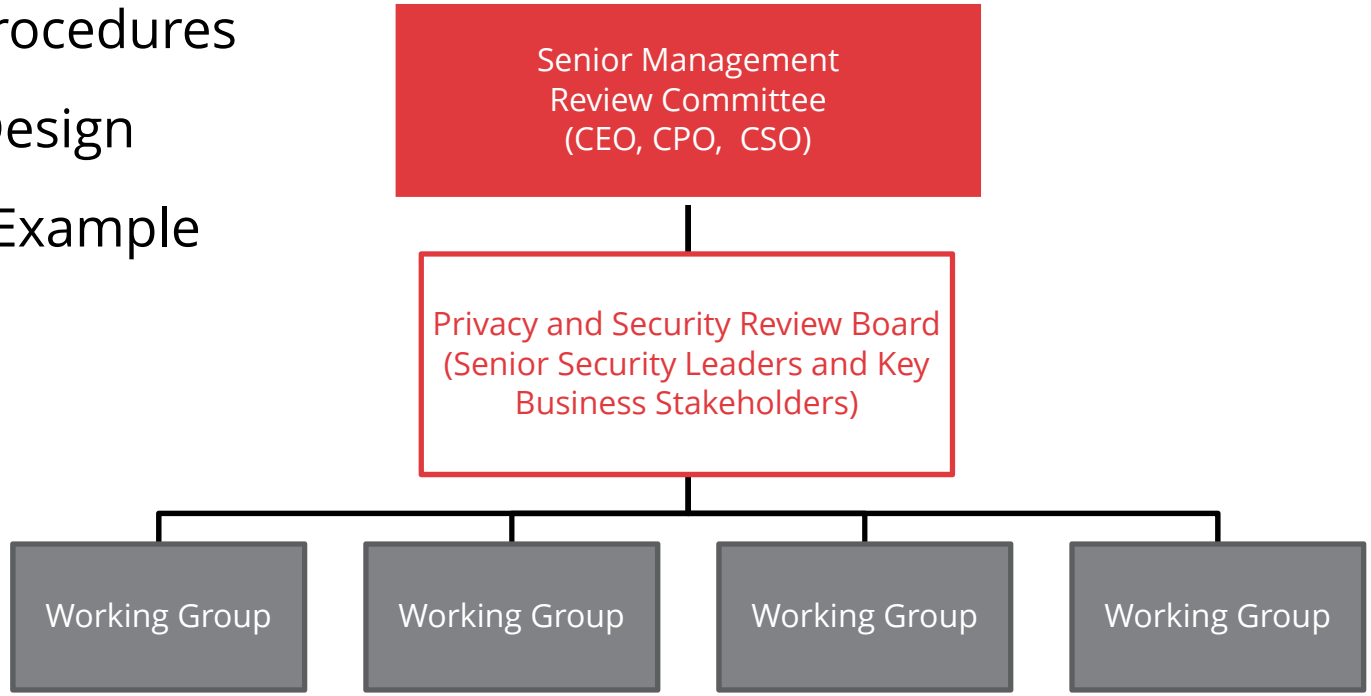
Response Plan: Timing Expectations



Before a Breach

Establish Sound Governance

- Roles and Responsibilities
- Policies & Procedures
- Privacy by Design
- Security by Example



How Boards Discharge their Duties

- Understand the Nature of the Risks
  - Engage outside experts
  - Hold training sessions on cyber and privacy risks
  - Discuss cyber and privacy risks at board meetings
- Understand Systems in Place to Address the Risks
  - Appoint a subcommittee for cyber and privacy risks
  - Hire a Chief Information Security Officer
  - Adopt tailored security and incident response plans
  - Receive regular gap analyses of the company's plan

Now That's a Good Question. . .

1. What information is most valuable to the organization?
2. Where and how is it stored, used, shared? By Whom?
3. What factors pose a threat to that data?
4. What type of plans do we have in place to protect our data?
   - Security Plan
   - Incident Response (IR) Plan
5. When are these plans tested? How?
6. Who is in charge of the security program?
7. Who receives regular privacy and security training?
8. Crowd favorites?

Questions?

Gerard M. Stegmaier
Partner, Reed Smith
IT, Privacy & Data Security
+1 202 414 9293
gstegmaier@reedsmith.com
LinkedIn: linkedin.com/in/gerardstegmaier
Twitter: @1sand0slawyer

Samuel F. Cullari
Counsel, Reed Smith
IT, Privacy & Data Security
+1 215 241 7904
scullari@reedsmith.com
LinkedIn: linkedin.com/in/samuel-cullari-204a114

Paul Luehr
Executive Managing Director
Stroz Friedberg
+1 612 605 3007
pluehr@strozfriedberg.com
LinkedIn: linkedin.com/in/paul-luehr-16127713