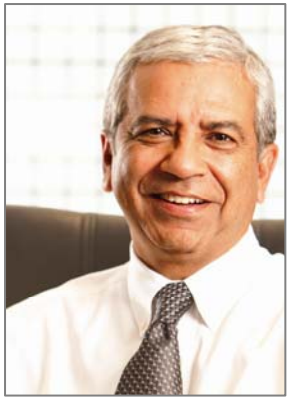
Benchmarking Industry Compliance Electronic Health Information at Risk: A Study of IT Practitioners

February 3, 2010

Crowe Horwath™

Ponemon INSTITUTE

Introductions



Raj Chaudhary
Crowe Horwath LLP
One Mid America Plaza, Suite 700
Oak Brook Terrace, IL 60181
Tel:630.586.5127
Mobile:574.210.7005
raj.chaudhary@crowehorwath.com
www.crowehorwath.com

Larry Ponemon
Ponemon Institute LLC
Michigan HQ: 2308 US 31 N.
Traverse City, MI 49686 USA
Tel: 231.938.9900
Toll Free: 800.887.3118
research@ponemon.org
www.ponemon.org

Crowe Horwath LLP

Crowe Horwath LLP (www.crowehorwath.com) is one of the largest public accounting and consulting firms in the United States. Under its core purpose of "Building Value with Values®," Crowe assists public and private company clients in reaching their goals through audit, tax, risk and consulting services. With 25 offices and 2,500 personnel, Crowe is recognized by many organizations as one of the country's best places to work. Crowe serves clients worldwide as an independent member of Crowe Horwath International, one of the largest networks in the world, consisting of more than 140 independent accounting and management consulting firms with offices in more than 400 cities around the world.

Ponemon Institute LLC

- ✓ The Institute was founded in 2002 and is dedicated to advancing responsible information management practices that positively affect privacy and data protection in business and government.
- ✓ The Institute conducts independent research, educates leaders from the private and public sectors, verifies the privacy and provides strategic advisory services for corporations establishing privacy risk management programs.
- ✓ Ponemon Institute is a member of **CASRO** (Council of American Survey Research Organizations). Dr. Ponemon serves as CASRO's chairman of Government & Public Affairs Committee of the Board.
- ✓ The Institute has assembled more than 50 leading multinational corporations called the **RIM Council**, which focuses the development and execution of ethical principles for the collection and use of personal data about people and households.
- ✓ The majority of active participants are privacy (CPOs) and information security (CISO) leaders.

Agenda

- HIPAA Compliance Observations
- Purpose and Scope of Study
- Benchmarking Study Results
- Q&A

HIPAA Compliance Observations

- Covered Entities - 2003 to 2008
  - Initial compliance reviews conducted – 2003 and 2005
  - Very few entities
    - Had independent assessments done
    - Or updated initial reviews
  - Small percentage formally tracked breaches
  - HIMMS study focused only on security in 2008
    - Business Associates not covered
  - Ponemon 2008 study of breaches
    - Sub-contractors a major cause
- Fast Forward to 2009

HIPAA Compliance Observations

- Covered Entities – Post ARRA and HITECH
  - Compliance Departments
    - Privacy in better shape than security
    - Disconnects between privacy and security
  - Audit Committees
    - HIPAA compliance risk – not on the agenda
  - Internal Audit Departments
    - Not even aware of HITECH
  - Payers Slightly Ahead of Providers
- Business Associates
  - Trying to comprehend the HIPAA enhancements of HITECH

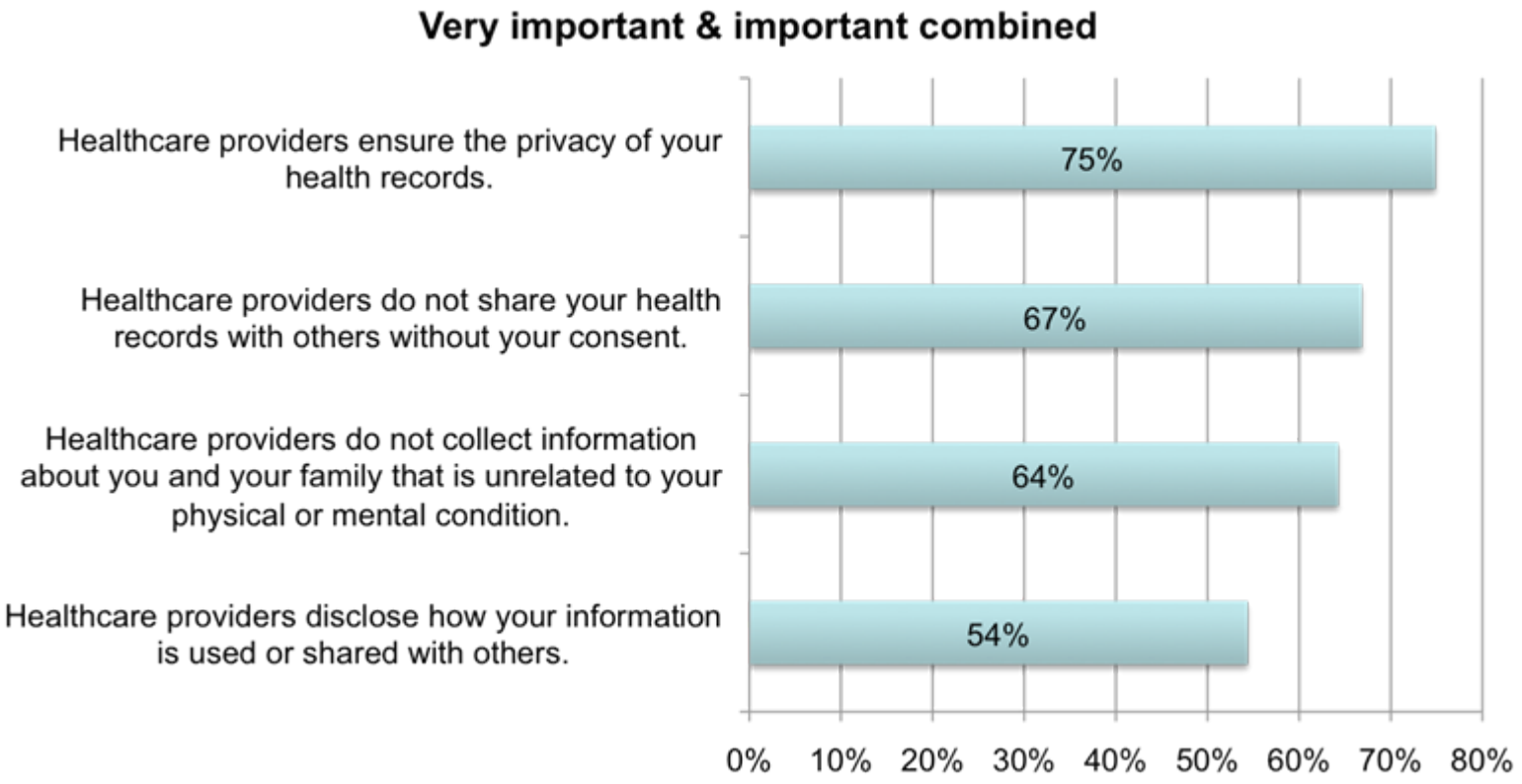
Purpose and Scope

- Determine readiness of healthcare companies
  - Covered Entities and Business Associates
  - Compliance with Privacy and Security provisions of HITECH
- Study covered readiness with respect to
  - Privacy
  - Data protection
  - Information security
  - Risk management activities
  - In addition to readiness
    - Assess potential gaps to compliance
    - Management support

Public's Perceptions

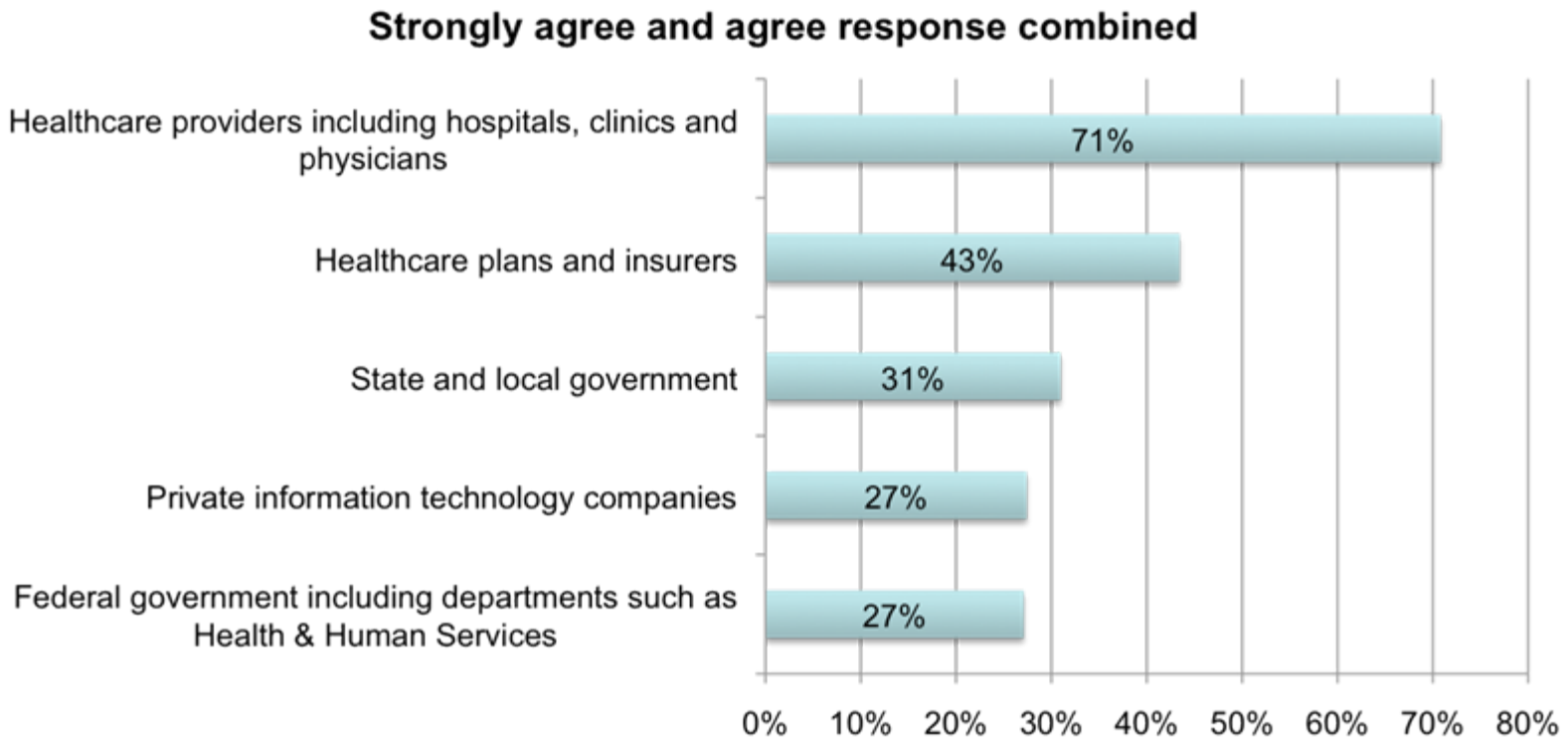
How important are the following issues?

Based on an independent sample of 883 adult-aged respondents. See Americans' Opinions about Healthcare Privacy (dated February 1, 2010).



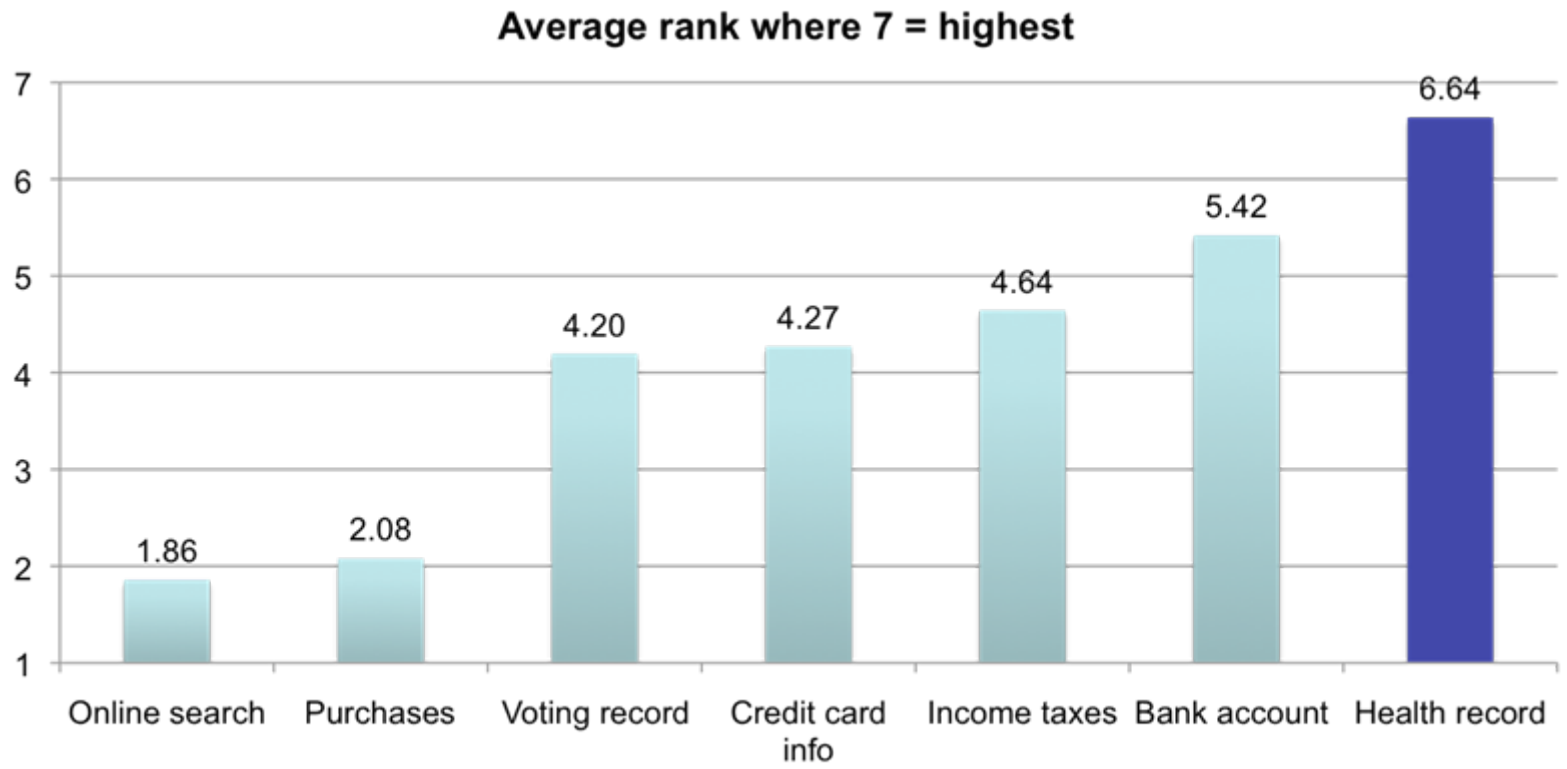
Who do you trust for privacy of your Healthcare records?

Based on an independent sample of 883 adult-aged respondents. See Americans' Opinions about Healthcare Privacy (dated February 1, 2010).



How important is the privacy of the following seven data types?

Based on an independent sample of 883 adult-aged respondents. See Americans' Opinions about Healthcare Privacy (dated February 1, 2010).



Benchmarking Results

Methods

- Benchmark methods utilized a standardized survey instrument that was completed by each responding organization. Individuals deemed to be most responsible for ensuring HIPAA and HITECH compliance were asked to field the instrument within their organizations
- Specific areas of the benchmark instrument includes:
  - Policies and standard operating procedures (SOPs)
  - Training, awareness
  - Downstream communications
  - Program management activities
  - Data security methods and tools
  - Compliance monitoring, assessment and audit
  - Redress and enforcement

About the benchmark sample

- Table 1 summarizes the sample response over a seven-week period ending in October 2009.
- A total of 260 organizations were selected for participation and contacted by the researcher.
- Eighty-five organizations completed the benchmark survey, but eight of these instruments were incomplete and, hence, removed from the final benchmark pool.
- A final sample of 77 organizations (30% response rate) was used in our analysis.

Table 1: Sample response	Freq.	Pct%
Healthcare providers	125	48%
Healthcare business associates	113	43%
Other organizations	22	8%
Total organizations contacted	260	100%
Returned benchmark surveys	85	33%
Incomplete benchmark surveys	8	3%
Benchmark sample	77	30%

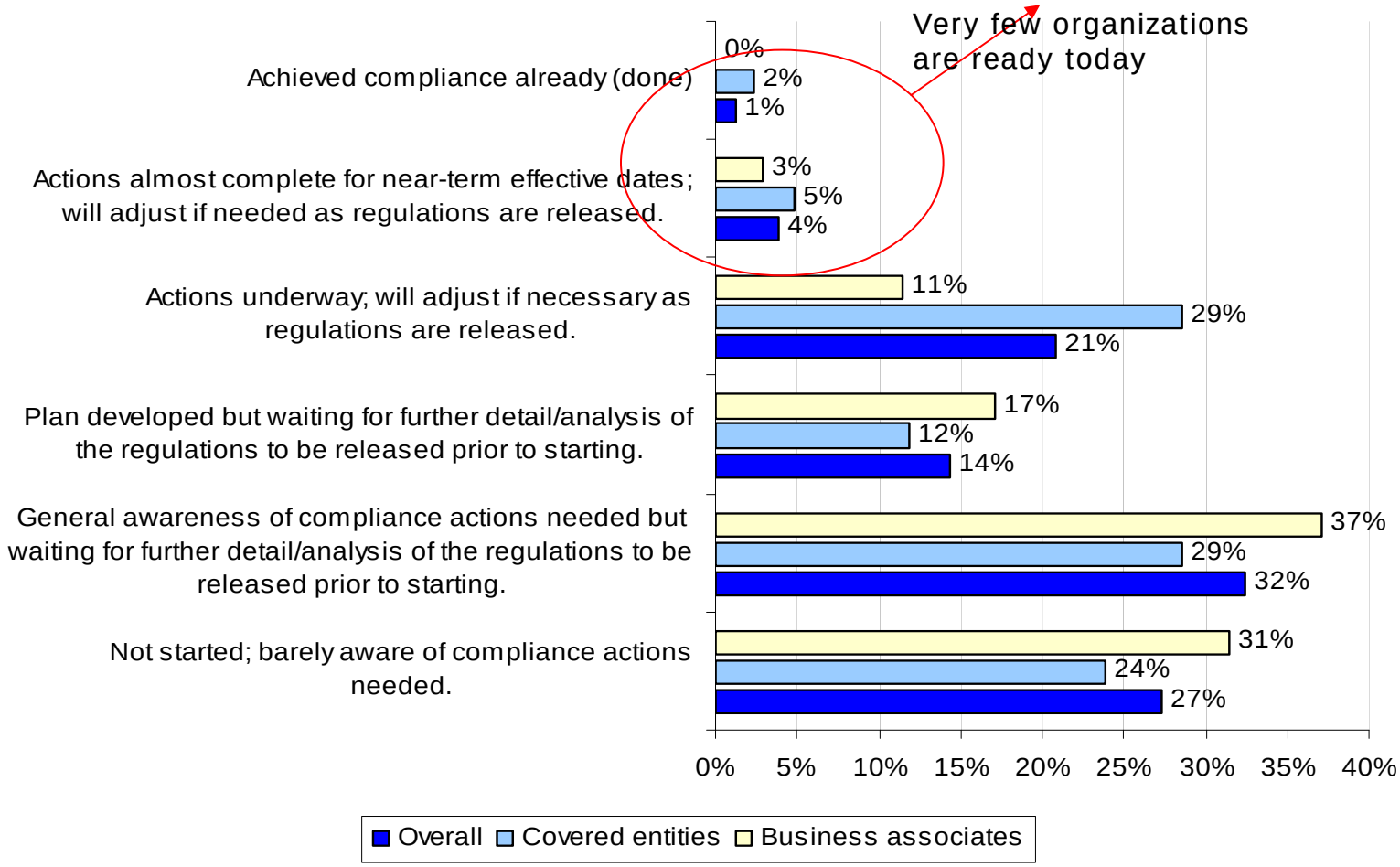
Ponemon INSTITUTE

Crowe Horwath™

Table 2 provides a detailed breakdown of the final sample, which includes 42 covered entities and 35 business associates.

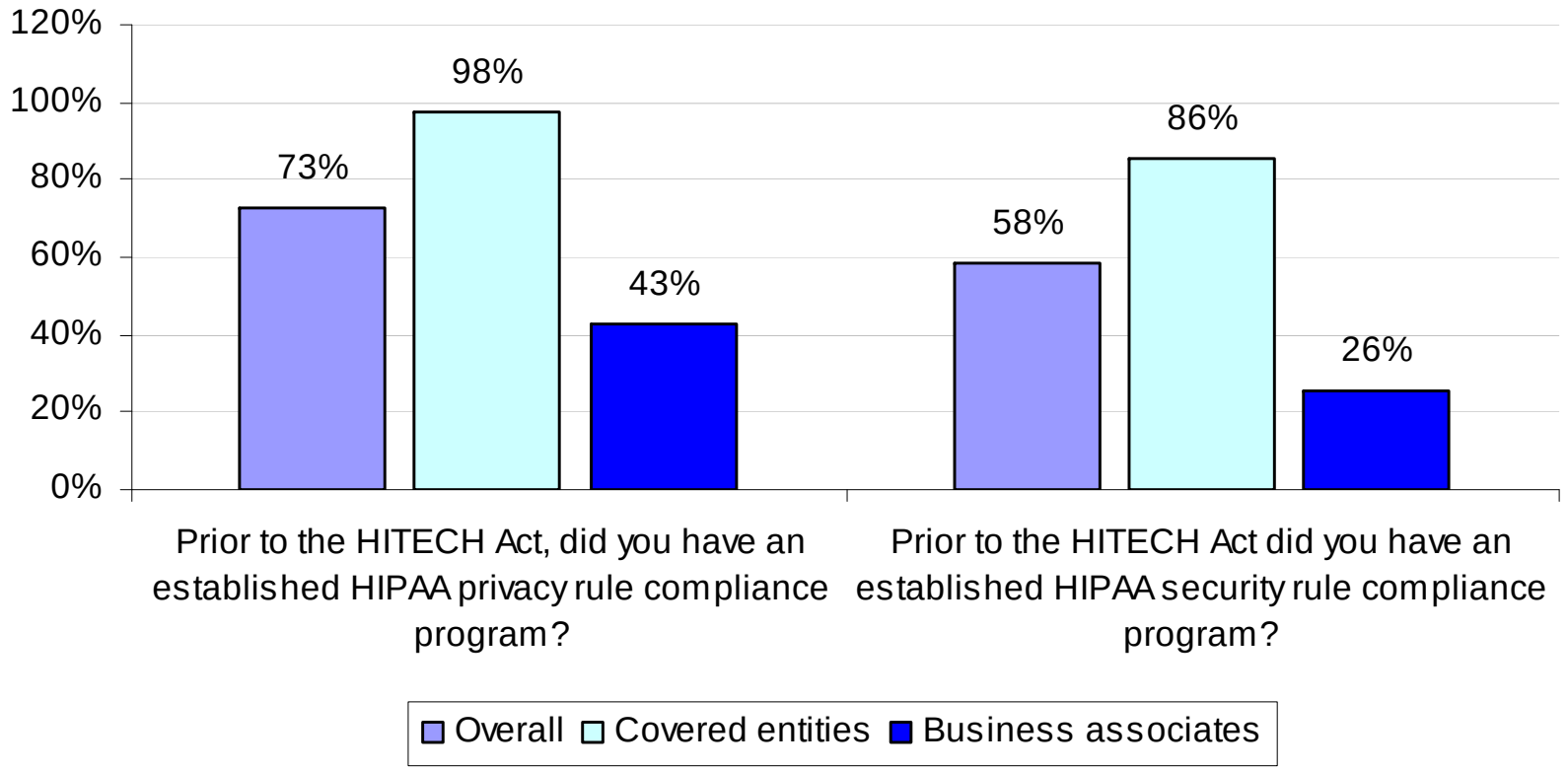
Table 2: Description of the benchmark sample	Overall	Covered Entity	Business Associate
Private healthcare provider	15	15	
Public healthcare provider	13	13	
Professional services to healthcare organizations	13		13
Insurance company with health-related products	11	11	
Retail pharmacy	4		4
Vendors of public health record management systems	4		4
Other business associate	4		4
Public/government healthcare payer	3	3	
Employer with a self-funded health plan	3		3
Healthcare payment processor	3		3
Pharmaceutical	2		2
Medical device retailer and distributor	2		2
Total	77	42	35

State of HITECH Act compliance readiness



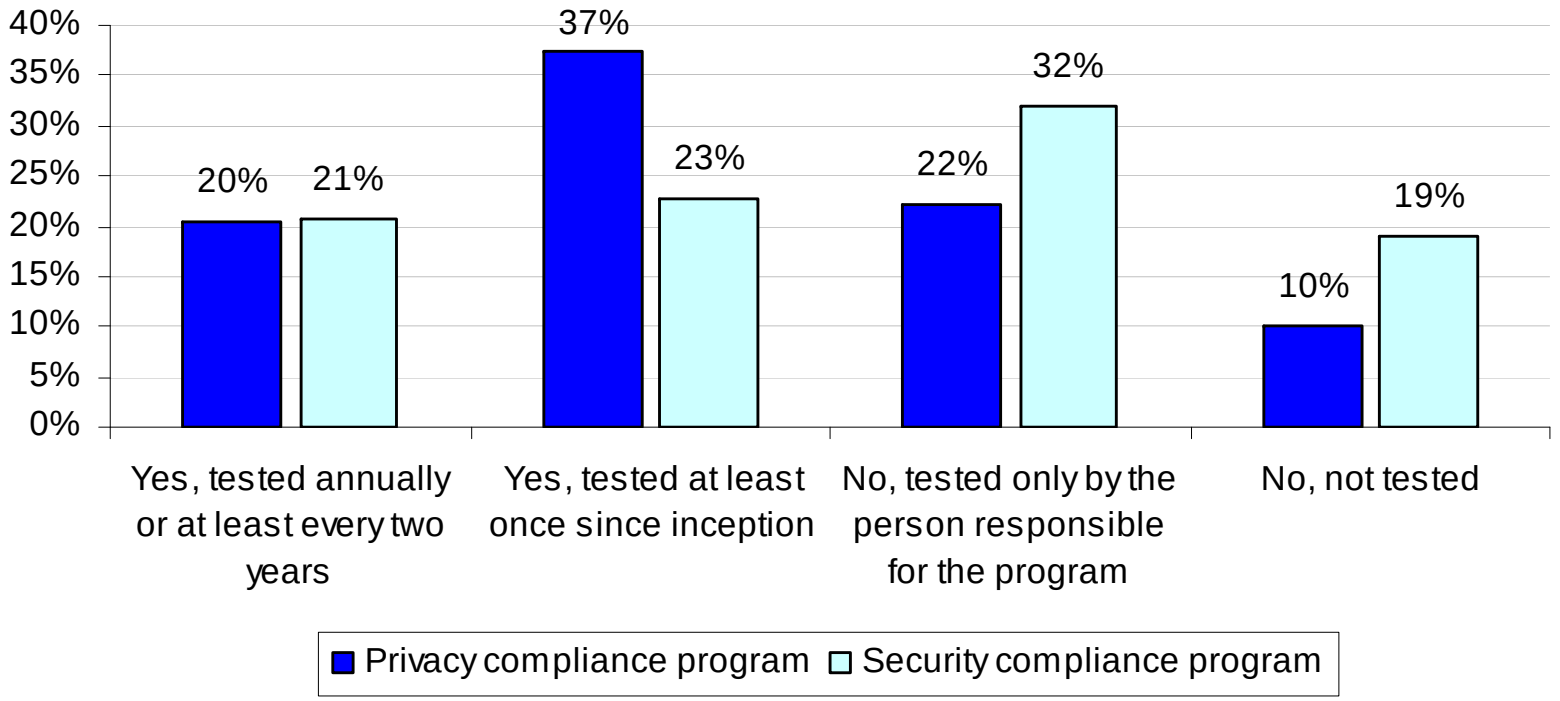
HIPAA programs prior to HITECH

Percentage Yes response



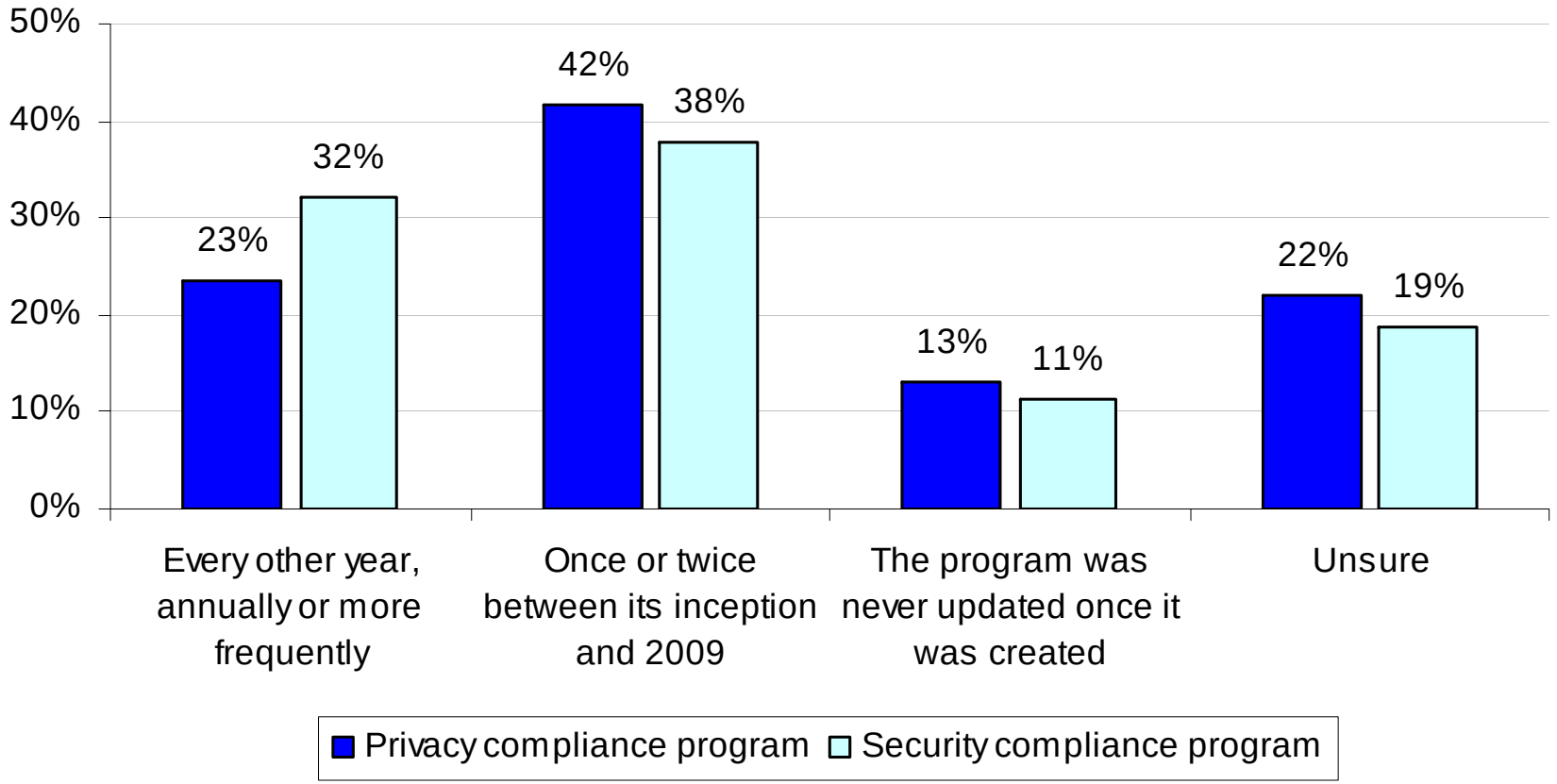
Testing the adequacy of the HIPAA compliance program

Has your HIPAA compliance program been tested for adequacy by an independent party (internal or external) not responsible for program management?



Updating the HIPAA compliance program

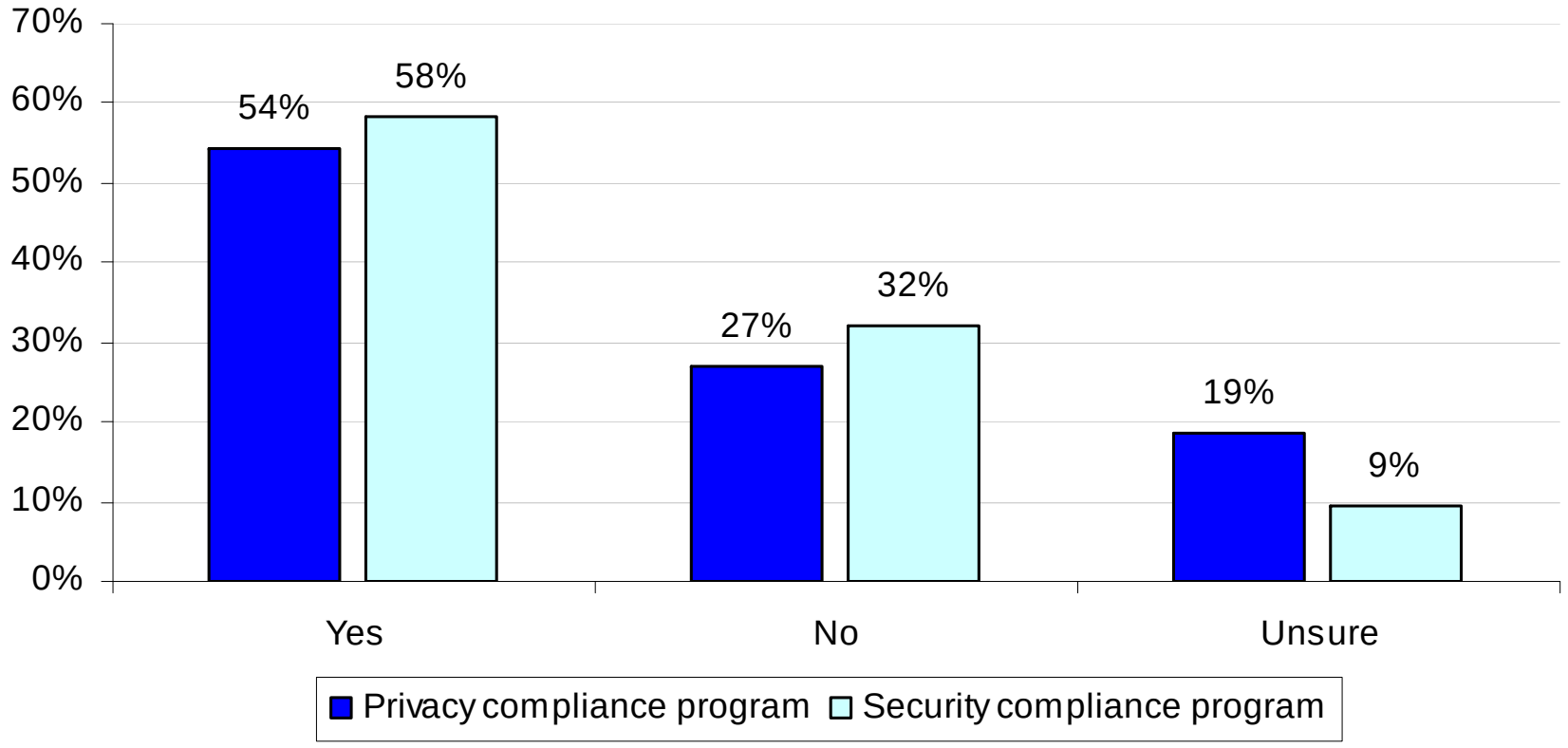
How frequently has your HIPAA compliance program been updated?



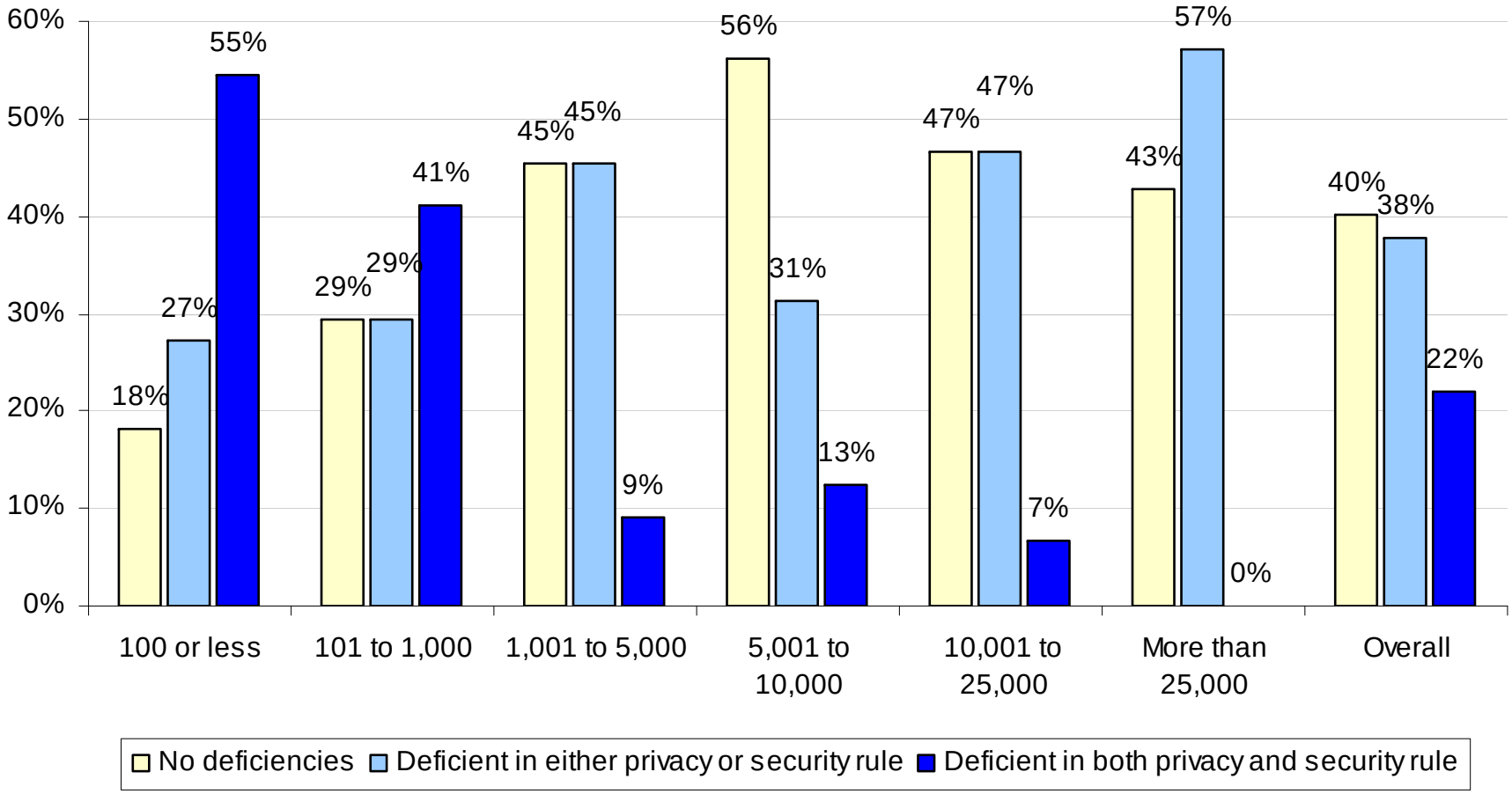
Pc

Known deficiencies in the HIPAA compliance program

Were there known deficiencies in your HIPAA compliance program?

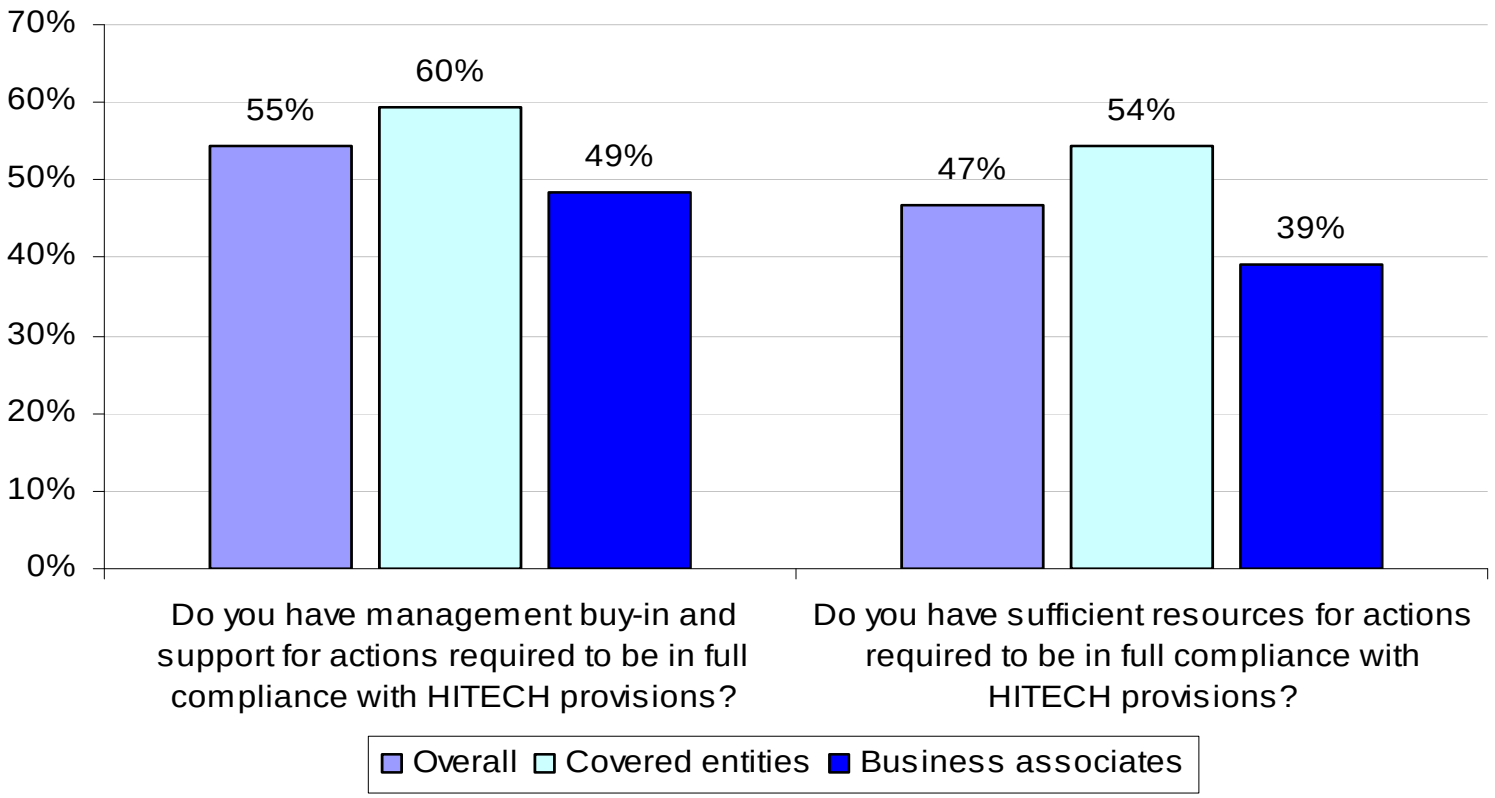


HIPAA deficiencies by organizational size (headcount)

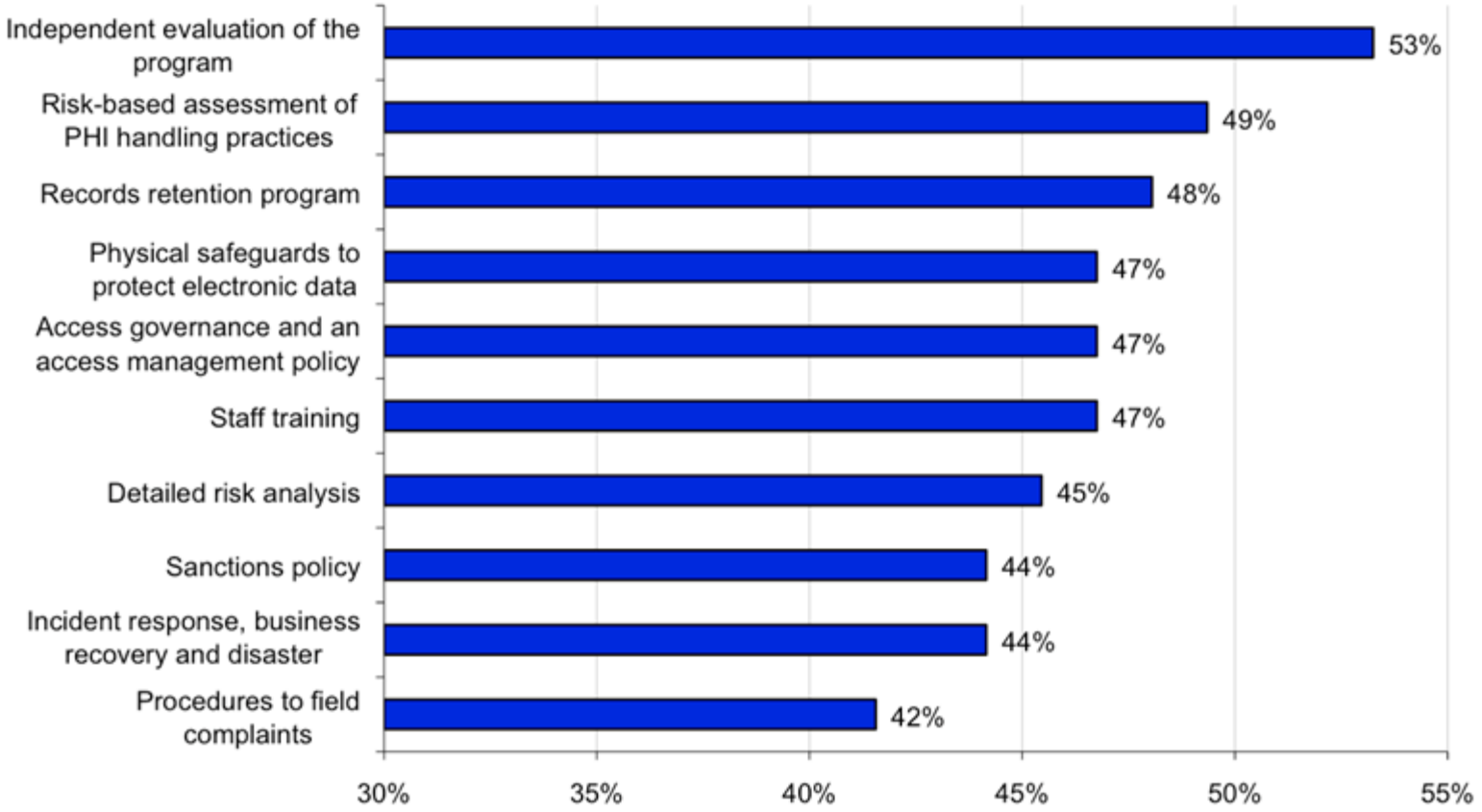


Management buy-in and sufficiency of resources

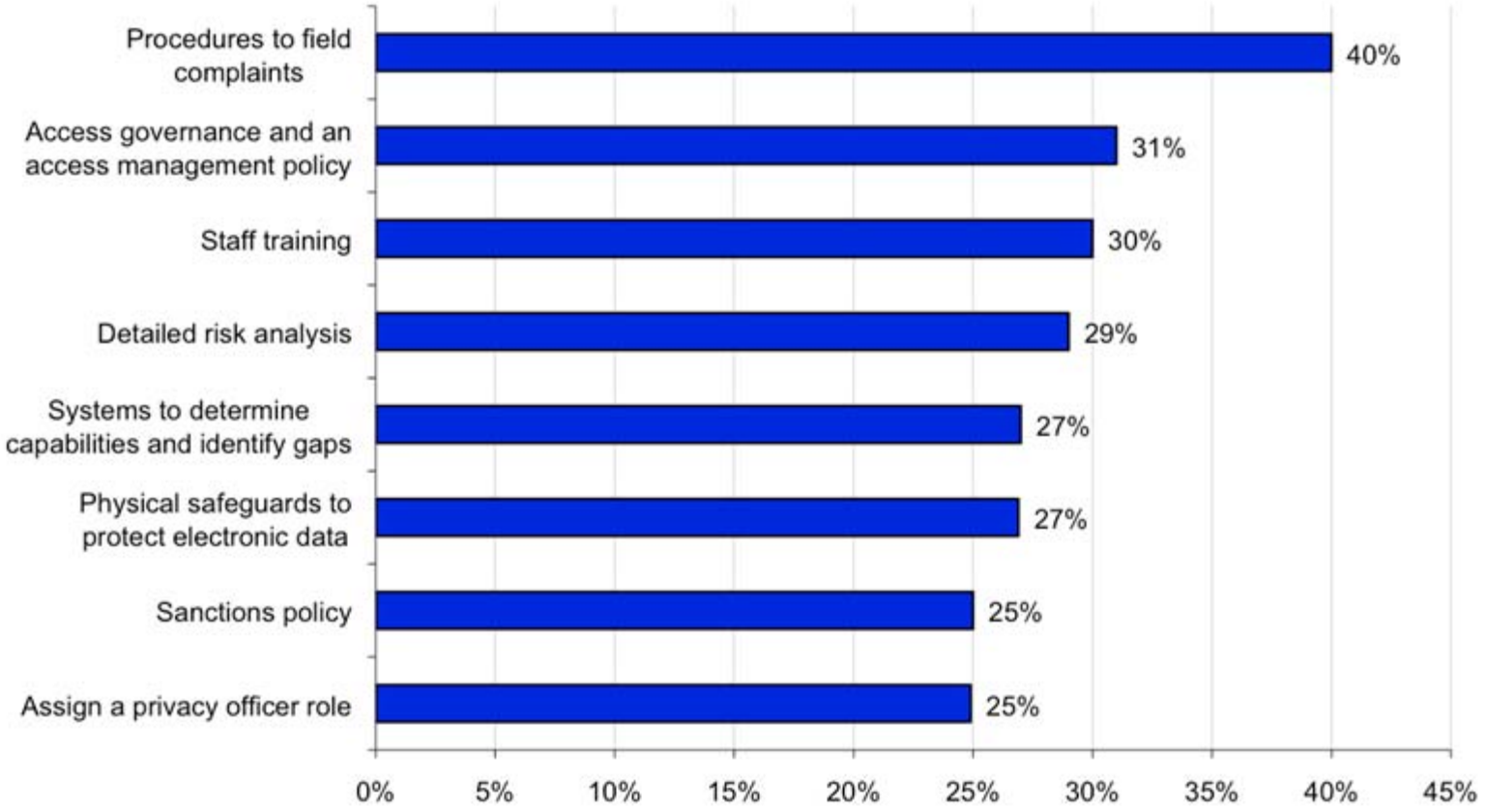
Percentage Yes response



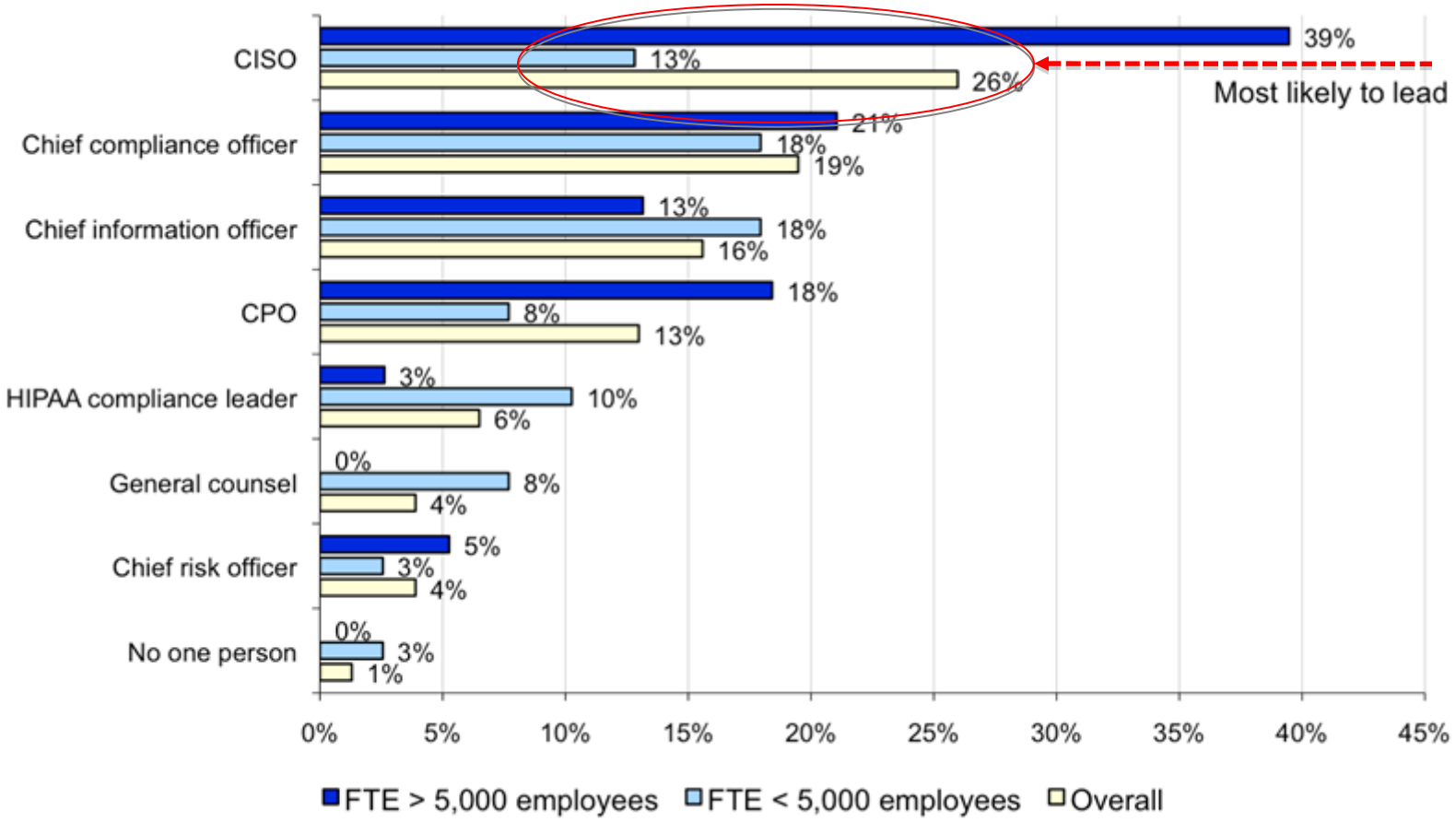
HIPAA compliance requirements that are not formally implemented



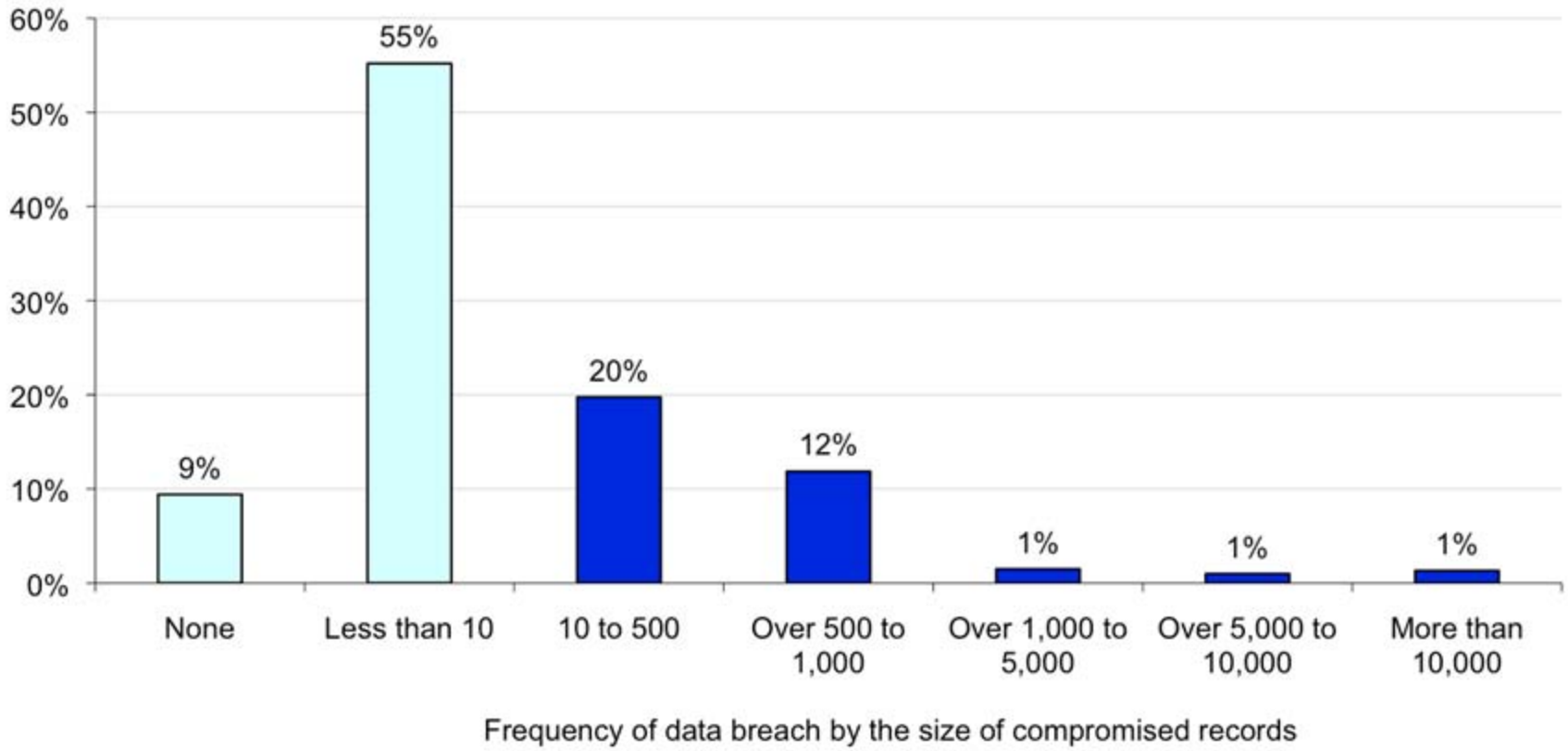
HIPAA compliance features that have a significant impact on business operations



Most responsible for HITECH compliance

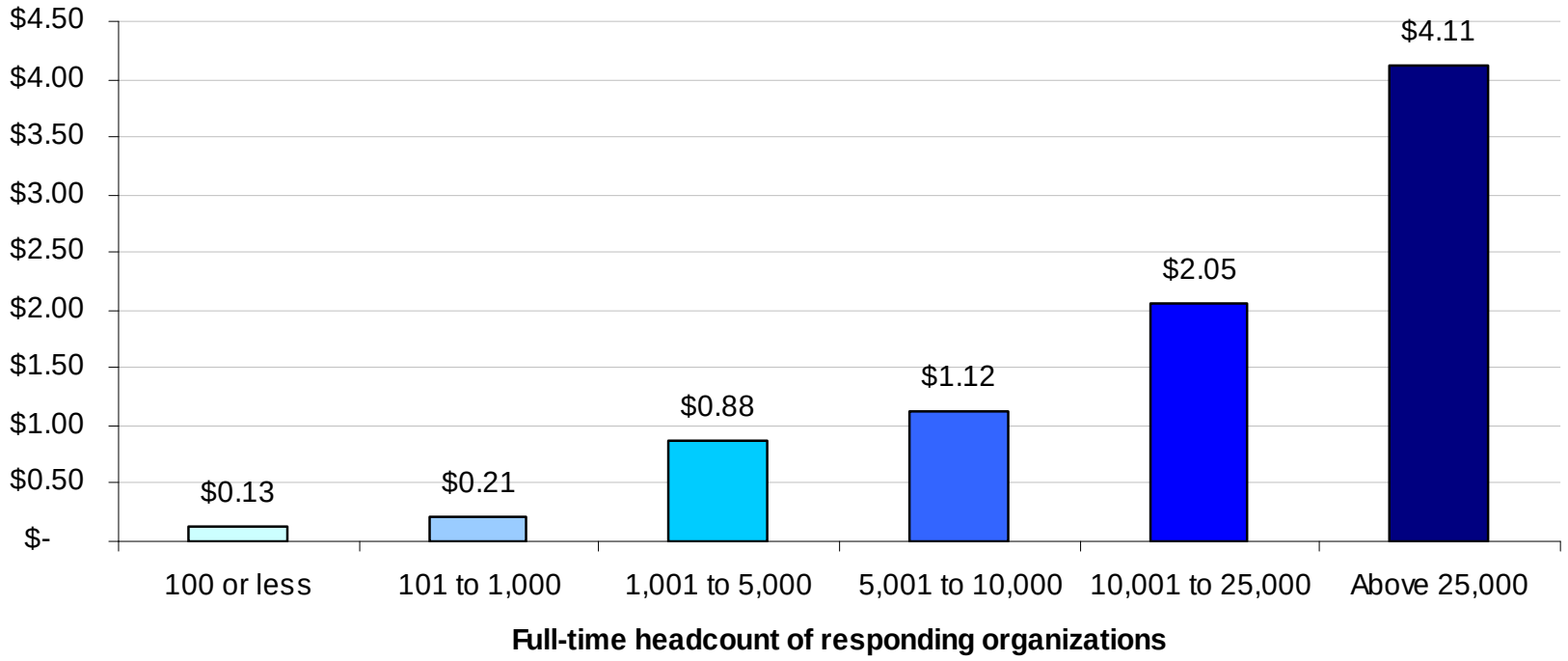


Frequency and size of data breach incidents over a two-year period



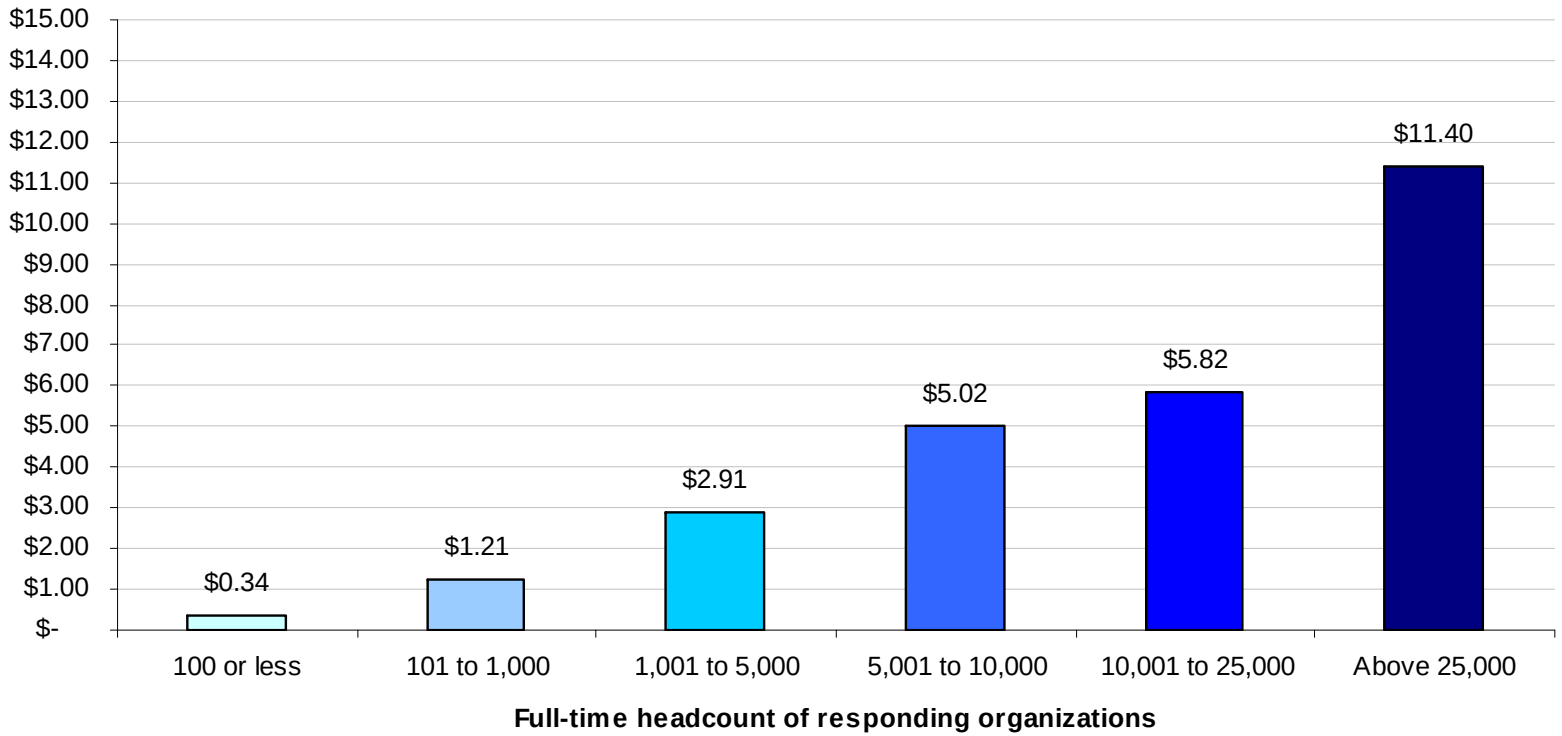
Estimated cost of compliance budgets by organization headcount

Direct cost figures reported with $000,000 omitted

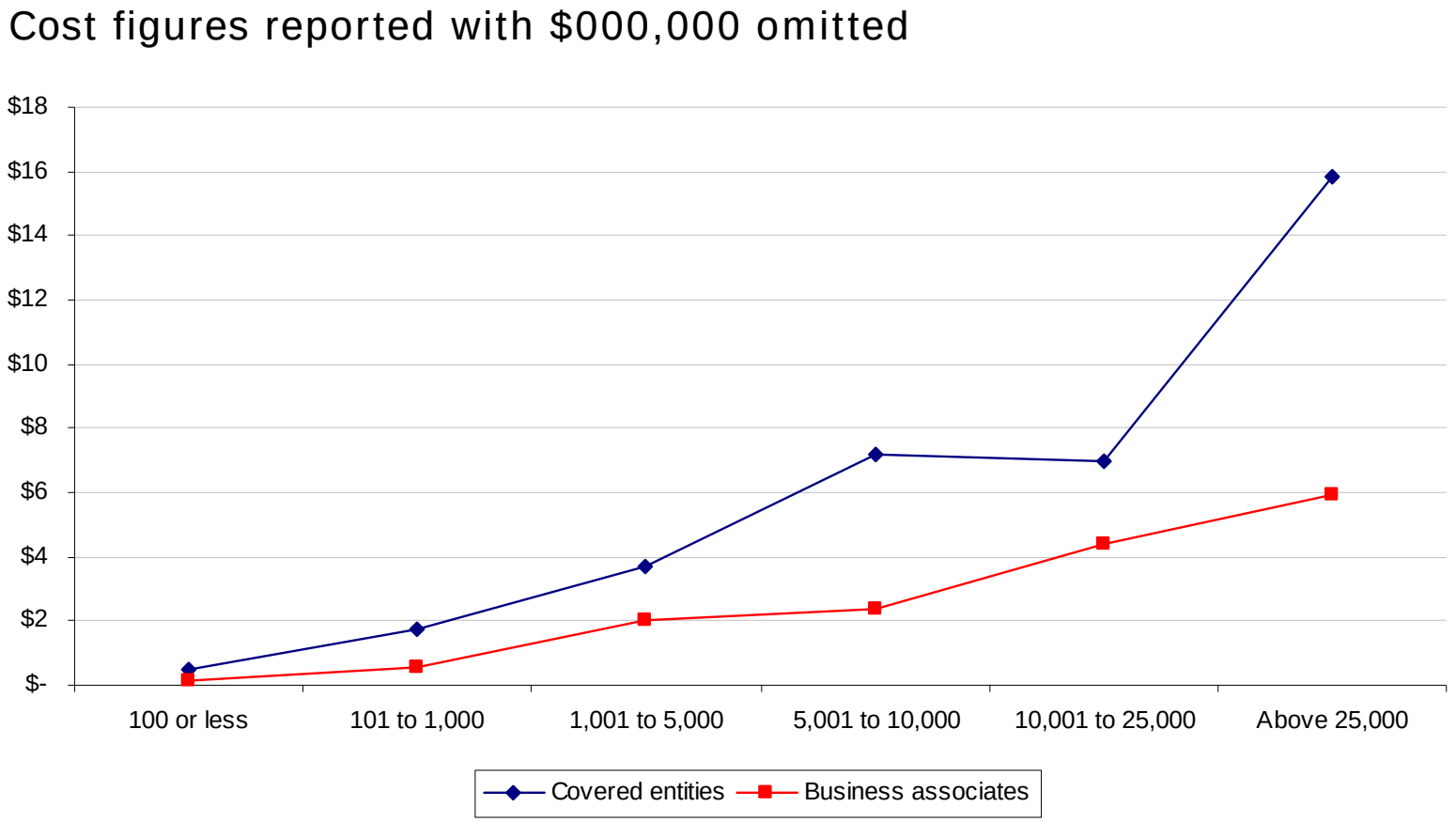


Estimated cost of compliance budgets by organization headcount

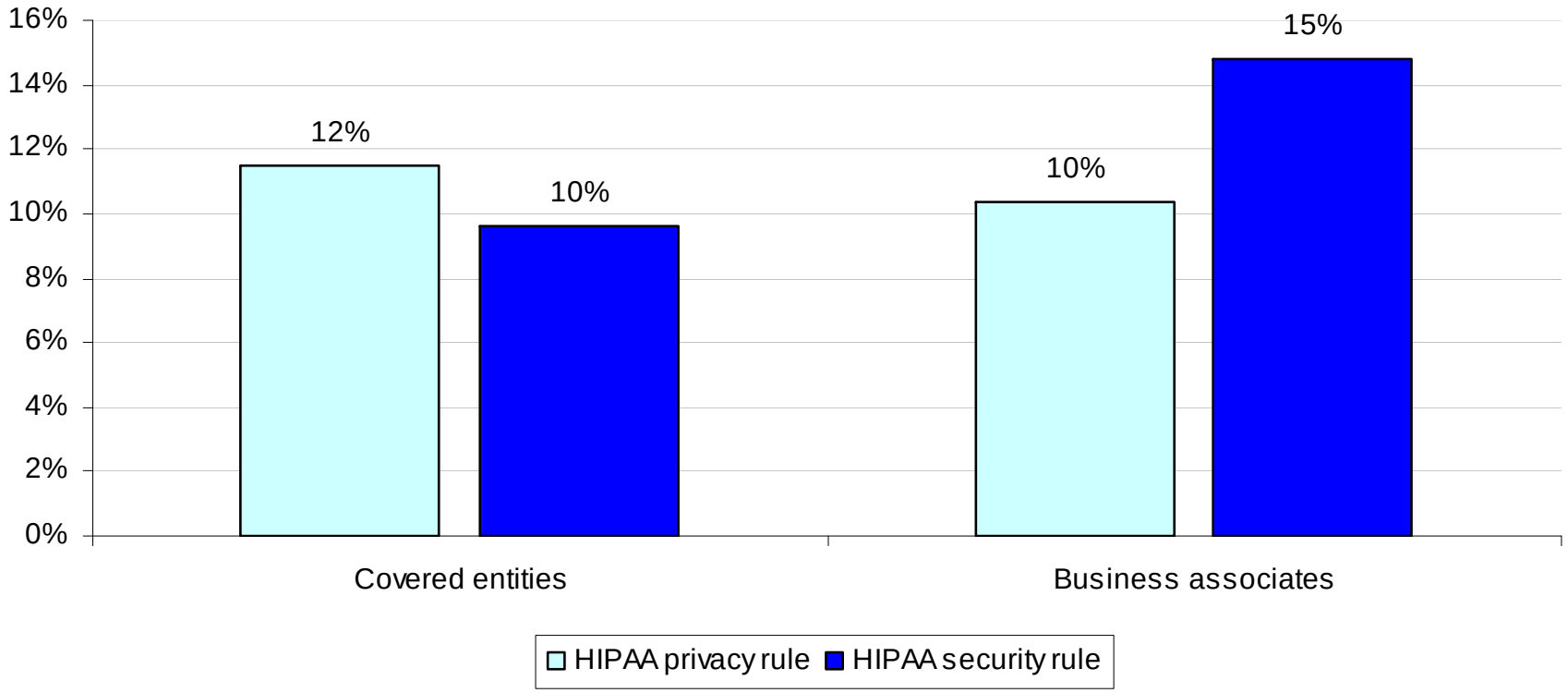
Indirect cost figures reported with $000,000 omitted



Extrapolated cost of compliance budgets for covered entities vs. business associates



Privacy rule and security rule budget allocation for covered entities & business associates



Concluding Comments

- ✓ Both covered entities and business associates face serious challenges in achieving substantial compliance with HIPAA privacy rule and security rule requirements.
- ✓ HIPAA leaders in both privacy and security need to do a better job in making senior management aware of their organization's current program deficiencies. Accordingly, the lack of senior level support and buy-in is one reason why many organizations are unable to obtain sufficient resources for achieving compliance goals.
- ✓ There seems to be a high level of uncertainty about what needs to be done to achieve substantial compliance. This uncertainty can lead to difficulties in allocating resources appropriately and gaining senior management support.
- ✓ Organizations need to determine specific gaps in their privacy and security compliance programs as a first step to compliance with HITECH.
- ✓ Many healthcare organizations need to be more proactive in managing compliance risk, in minimizing data breach of protected health information, and in avoiding regulatory intervention.
- ✓ While many participating organizations appear to have mature HIPAA compliance programs (especially covered entities), there is significant room for improvement especially on issues relating to risk assessment, training and policy dissemination.

Questions?

Raj Chaudhary
Crowe Horwath LLP
One Mid America Plaza, Suite 700
Oak Brook Terrace, IL 60181
Tel:630.586.5127
Mobile:574.210.7005
raj.chaudhary@crowehorwath.com
www.crowehorwath.com

Dr. Larry Ponemon
Ponemon Institute LLC
Michigan HQ: 2308 US 31 N.
Traverse City, MI 49686 USA
Tel: 231.938.9900
Toll Free: 800.887.3118
research@ponemon.org
www.ponemon.org

To download the benchmark findings whitepaper, please visit www.crowehorwath.com/benchmark