The Changing Role of the Privacy Function

Preview Report

CEB Data Privacy Leadership Council

CEB
WHAT THE BEST COMPANIES DO

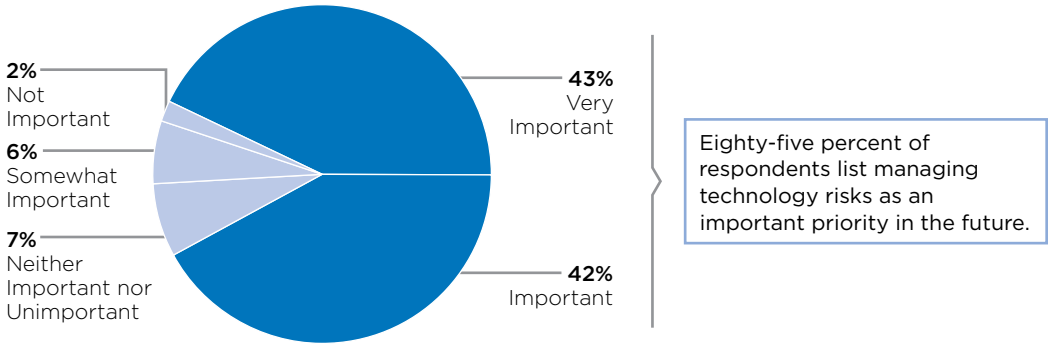
Data privacy and protection are increasingly top concerns not only for senior executives, but also for boards of directors.

- Almost two-thirds of directors plan to spend more time and energy focusing on IT-related risks.

PRIVACY CONCERNS CONTINUE TO GROW

Importance of Managing Technology-Related Risks in the Future

Percentage of Respondents

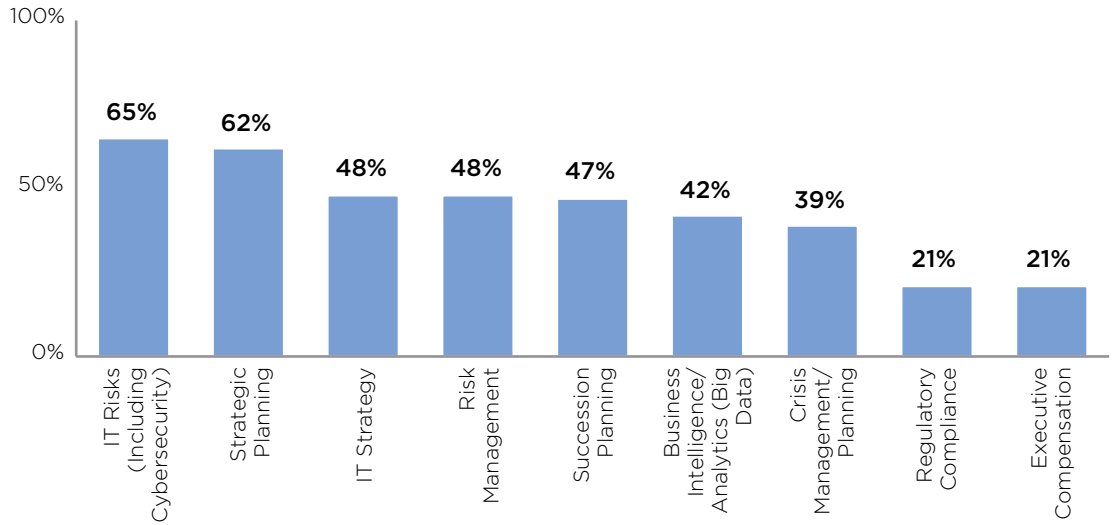


n = 139.

Source: CEB 2012 Information Risk Survey.

Change in the Amount of Time Directors Should Be Spending on Initiatives

Percentage of Directors Indicating Some Increase or Significant Increase in Time/Focus



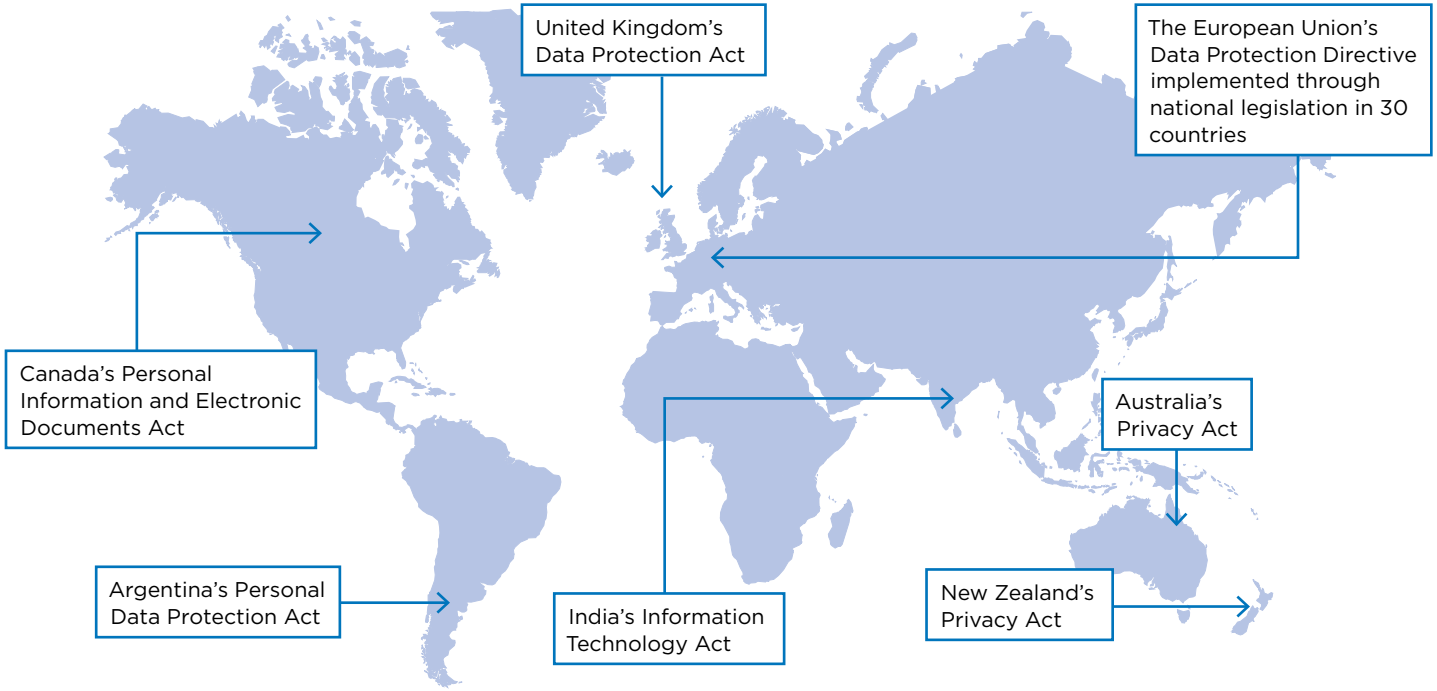
Source: PwC 2014 Annual Corporate Directors Survey.

In response to the concern over privacy incidents, regulatory scrutiny has increased, growing in scope and complexity.

- As of April 2014, 101 countries maintained data privacy laws, and 21 additional countries have Bills before their legislatures.
- In 2014, there were at least 20 pending privacy-related bills in the U.S. Congress.

AN INCREASINGLY COMPLEX REGULATORY ENVIRONMENT

Select Data Privacy Legislation by Country



Source: CEB analysis,

Select U.S. Federal Legislation

- Children's Online Privacy Protection Act
- Gramm-Leach-Bliley Act
- Fair Credit Reporting Act/Fair and Accurate Credit Transactions Act (FCRA/FACTA)
- Right to Financial Privacy Act
- Electronic Communications Privacy Act
- Computer Fraud and Abuse Act (CFAA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Heath Act (HITECH)
- CAN-SPAM and Telephone Marketing Restrictions

Source: CEB analysis,

Common Areas of U.S. State Regulation

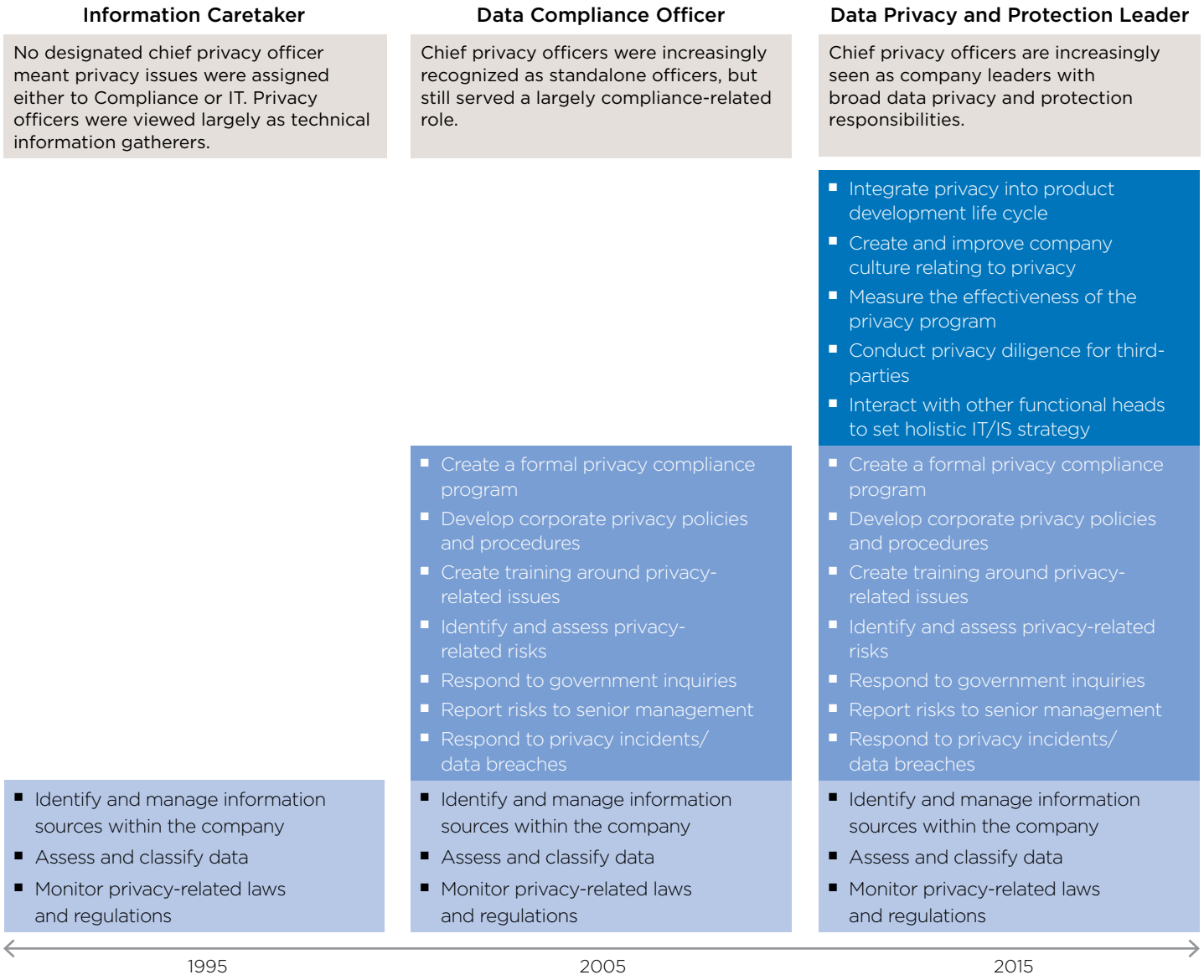
- Security Breach Notifications
- Identify Theft
- Use of Social Security Numbers
- Spam and Pretexting
- Telephone/Fax Marketing
- State Wiretapping and/or Employee Monitoring
- Computer Crime
- Medical Privacy
- Financial Privacy
- Encryption and Written Security Protocols

The role of the chief privacy officer has evolved from an information caretaker to a data privacy and protection leader.

- Chief privacy officers have become more significant partners, but this has resulted in significantly more responsibilities.

THE CHANGING ROLE OF THE CHIEF PRIVACY OFFICER

The Evolving Role of the Chief Privacy Officer
Illustrative



Source: CEB analysis.

A combination of internal and external trends will make privacy risk even more difficult to manage in the future.

KEY MAGNIFIERS OF PRIVACY RISK

1

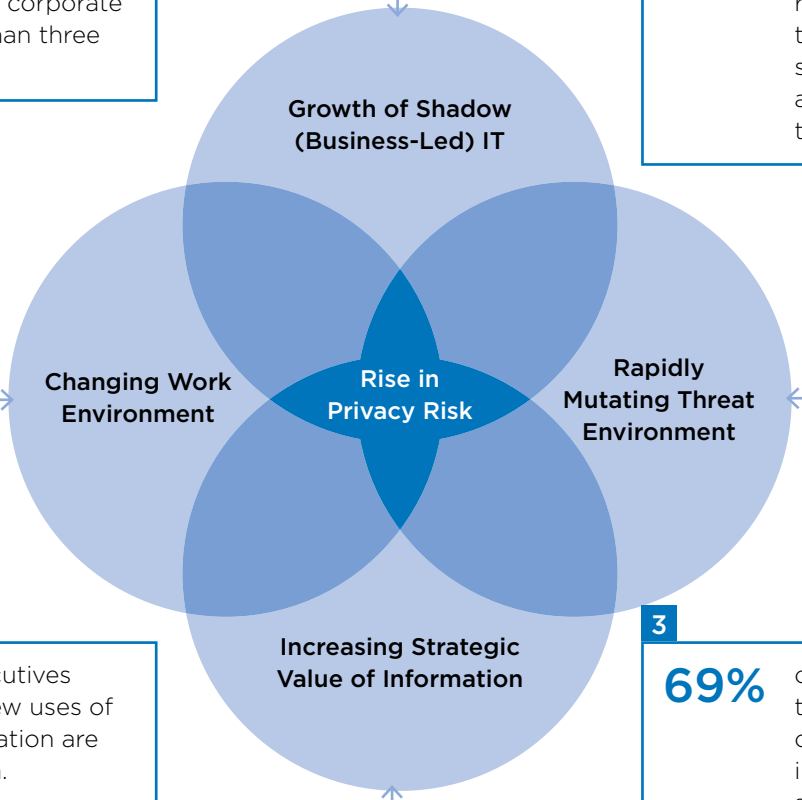
64% of employees regularly use personal technologies for work.

76% of employees now spend more time accessing and reviewing corporate information than three years ago.

2

37% of technology budgets are now controlled outside of the IT department.

68% of IT executives claim responsibility for technology use and security but lack the authority to manage these effectively.



4

79% of senior executives report that new uses of digital information are key to growth.

60% increase in operating margins is possible through better use of information.

3

69% of executives believe that their companies can't keep up with the increasing pace and sophistication of attacks.

23% of successful attacks are now attributable to third-party negligence.

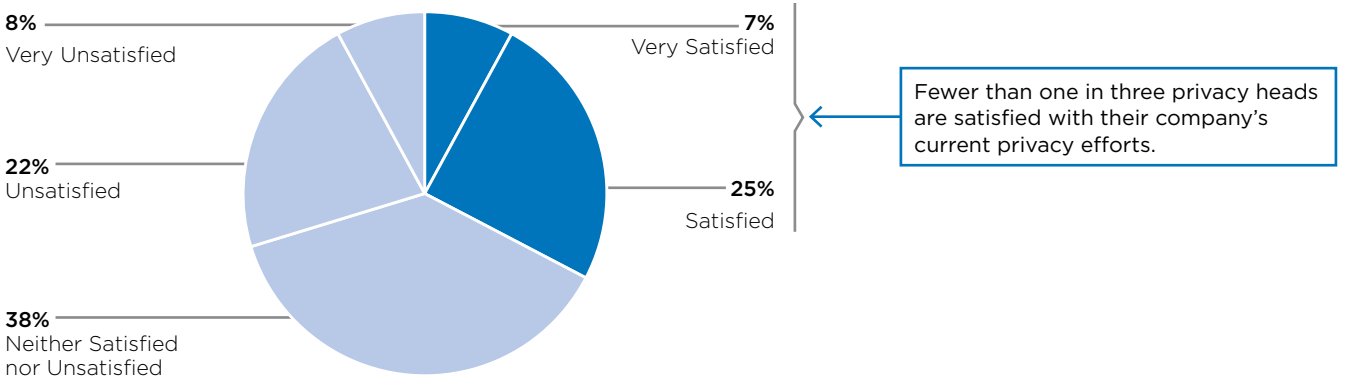
Source: CEB 2012 High Performance Survey; CEB 2012 Employee Technology Value Survey; Ponemon Institute, "2013 Cost of Data Breach: Global Analysis," 28 May 2013, http://www.ponemon.org/library/2013-cost-of-data-breach-global-analysis; McKinsey & Company, *Big Data: The Next Frontier for Innovation, Competition, and Productivity,* May 2011; Avanade, *Global Survey: What's Creating Tension Between IT and Business Leaders?,* 2014; World Economic Forum and McKinsey & Company, *Risk and Responsibility in a Hyperconnected World,* January 2014.

Given the expansion of roles and responsibilities, it is not surprising that chief privacy officers report less satisfaction with their program efforts.

THREE CHALLENGES TO SUCCESSFUL DEVELOPMENT

Satisfaction with Privacy Efforts

Percentage of Respondents



n = 65.

Source: CEB 2014 State of the Privacy Function Survey.

Challenges to Developing Effective Privacy Programs

Inconsistent (and Limited) Mandate

Inconsistent reporting structures and limited resources hamper the chief privacy officer's ability to lay the foundation for an effective privacy program.

"We have operations in 60-plus countries, but there are just two of us dedicated to privacy full-time. How are we supposed to roll out a program across the entire firm?"

Chief Privacy Officer
Fortune 100 Company

Unclear Governance of Activities

Lack of ownership from an enterprise-wide standpoint and no clear goals create confusion among functions.

"What have we already done? I think HR and IT are complying with certain privacy requirements, but is it enough?"

Chief Compliance Officer
Retail Company

Lack of Employee Awareness

Employees lack realistic policies and applicable training to comply with corporate privacy principles.

"The majority of what needs to be done…involves being thoughtful about the human beings involved, training, 'laying the pipe' for the kind of behavior you want, and modeling that behavior at the senior levels."

Chief Privacy Officer
Technology Company

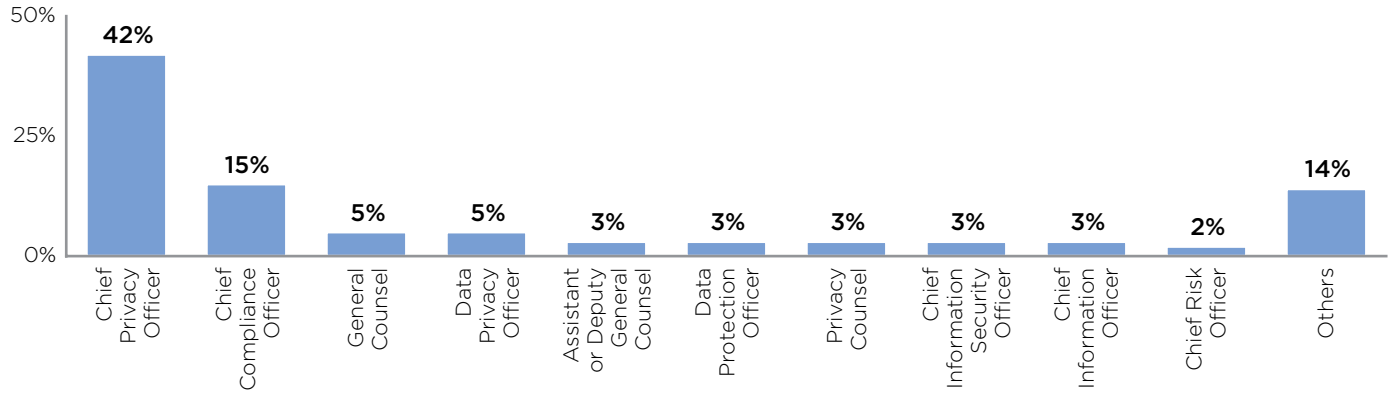
Approximately 42% of companies have a Chief Privacy Officer, while almost half of privacy functions reside in the Compliance Department.

- Companies that do have a chief privacy officer report that they are satisfied with their program more than twice as often as those that do not.
- In addition to the functions mentioned, seniormost privacy officers also report into Human Resources or in some cases, a Privacy Committee.

PORTRAIT OF THE CHIEF PRIVACY OFFICER

Title of the Seniormost Privacy Officer

Percentage of Respondents

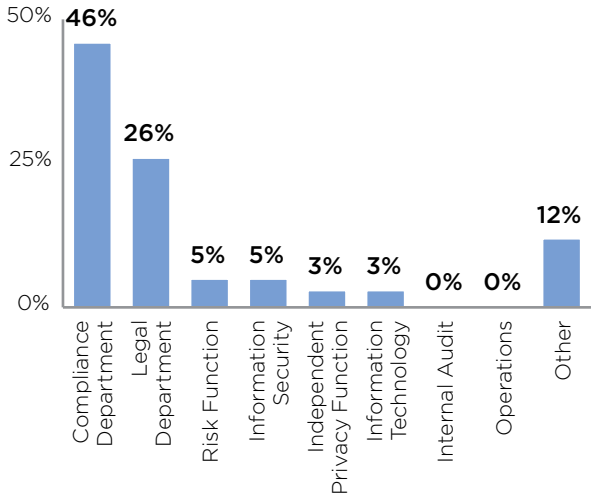


n = 65.

Source: CEB 2014 State of the Privacy Function Survey.

Location of the Privacy Function

Percentage of Respondents

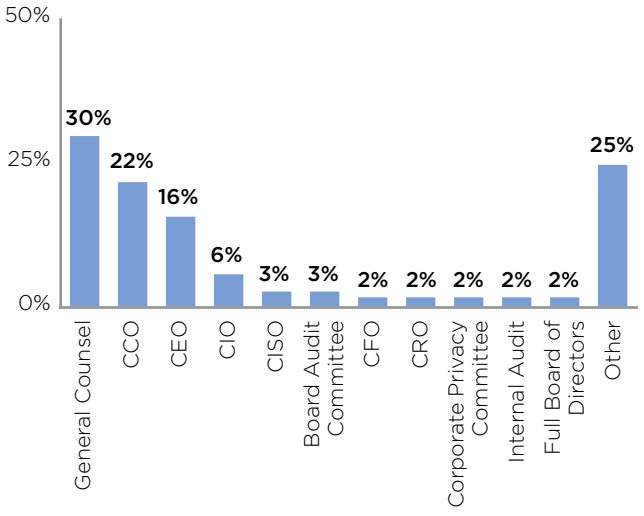


n = 65.

Source: CEB 2014 State of the Privacy Function Survey.

Primary Reporting Relationship of the Seniormost Privacy Officer

Percentage of Respondents



n = 64.

Source: CEB 2014 State of the Privacy Function Survey.

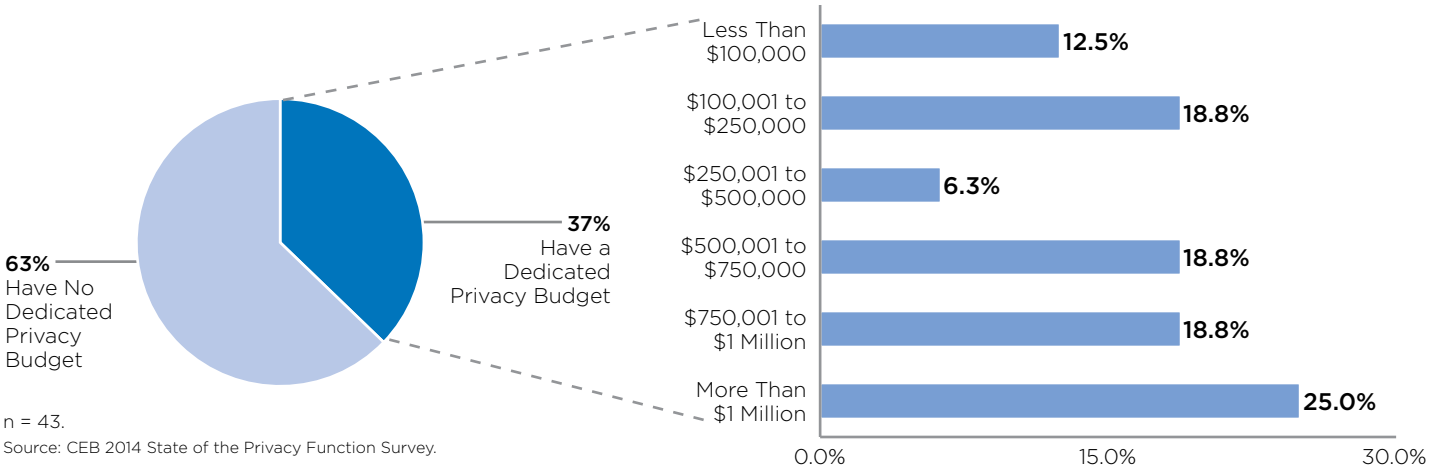
The average privacy budget was $366,884 with a projected increase of 32% in 2015.

- Half of privacy heads expect to increase their budgets on staff training and internal compliance measurement and monitoring.

LIMITED RESOURCES FOR PRIVACY FUNCTIONS

Estimate of Current Privacy Program Budget

US Dollars, 2014



n = 43.

Source: CEB 2014 State of the Privacy Function Survey.

n = 16.

Source: CEB 2014 State of the Privacy Function Survey.

Allocation of Privacy Program Budget

	Average Percent Allocation	Percent Who Expect This Number to Increase in 2015	Percent Who Expect This Number to Decrease in 2015
Privacy training and communication vendors	8%	27%	7%
Internal compliance training and communication development	11%	40%	0%
Staff salaries, bonuses, and benefits	43%	41%	3%
Outside consultants/counsel	14%	35%	16%
Travel	5%	30%	7%
Privacy staff training (conferences, associations, licenses, certifications)	5%	45%	3%
Internal compliance measurement and monitoring	6%	46%	0%
Other	8%	30%	10%

n = 24–30.

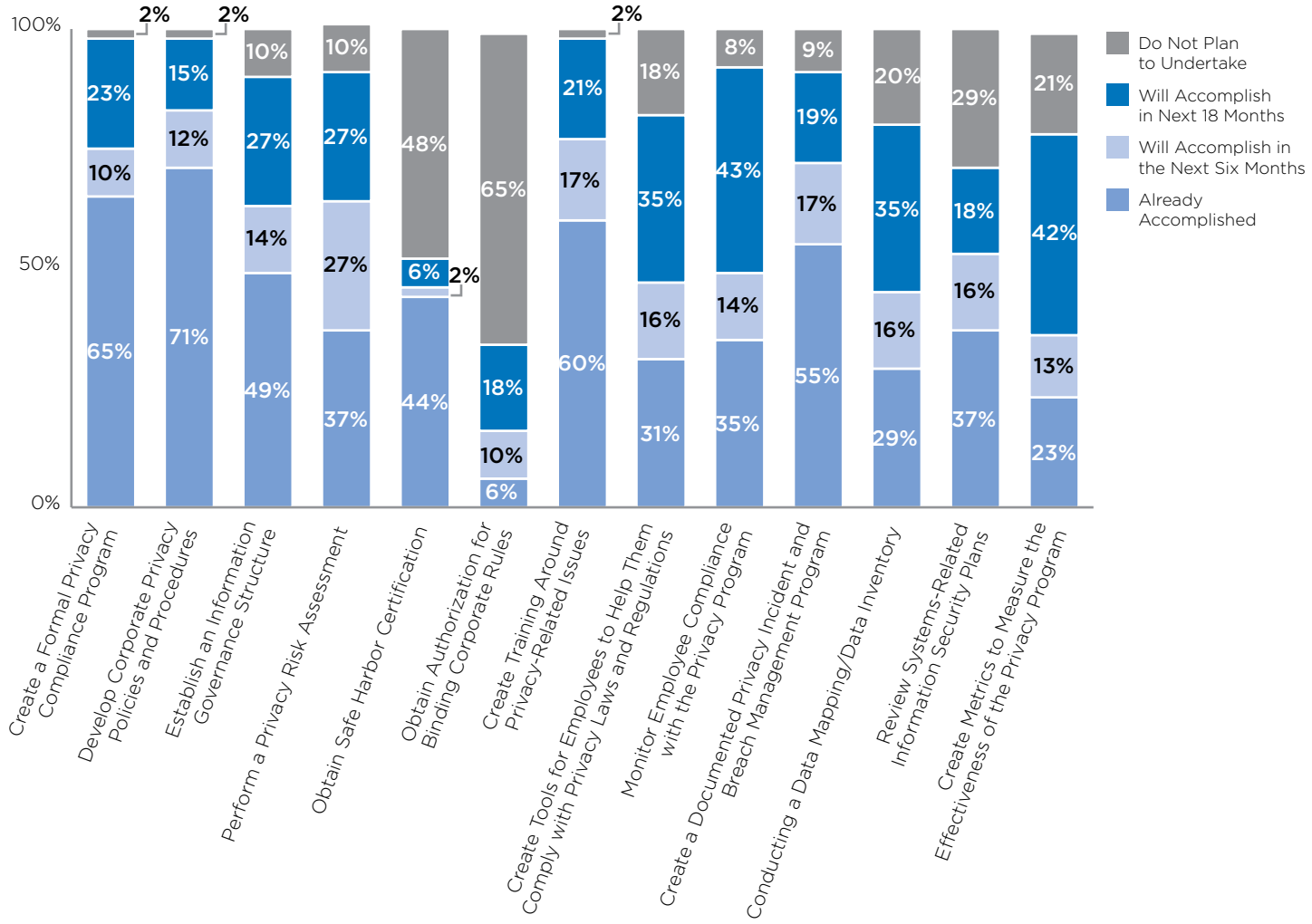
Source: CEB 2014 State of the Privacy Function Survey.

The majority of privacy functions have already created policies, training, and breach management programs.

- In the next six months, many privacy functions plan to perform a privacy risk assessment.
- Across the next 18 months, privacy functions plan to establish metrics to track program effectiveness, and monitor employee compliance.

MORE WORK TO BE DONE

Intent to Take on Initiatives in the Near Future
Percentage of Respondents



n = 49–53.
Source: CEB 2014 State of the Privacy Function Survey.
Note: Bars may not total 100% due to rounding.

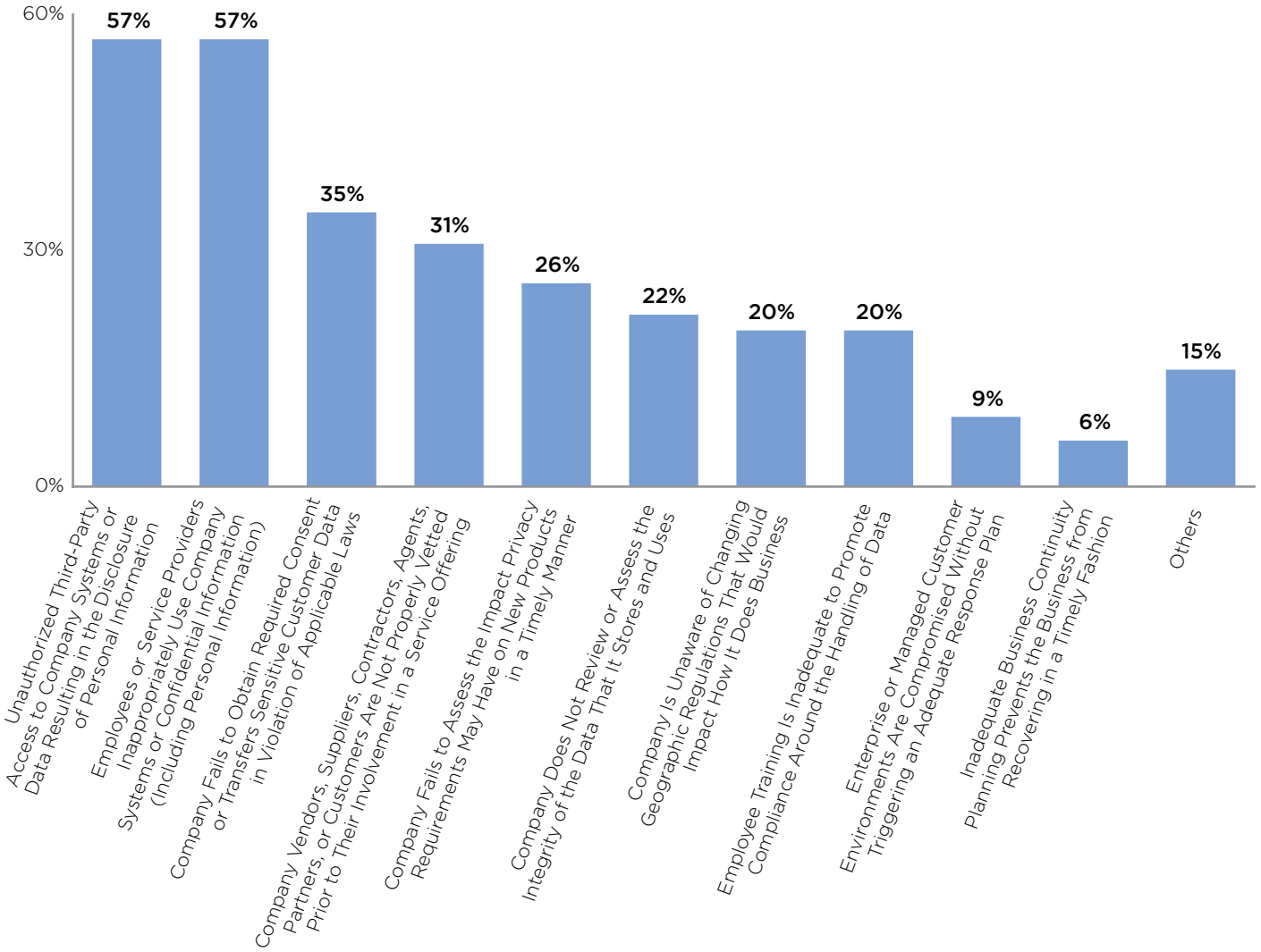
Chief privacy officers rank unauthorized access and use of data by both external and internal parties as the biggest risks to privacy.

- More than one-third of chief privacy officers reported improper third-party access to company systems as their top privacy risk.
- Half of chief privacy officers consider inappropriate use of data by employees as one of their top two risks.

IDENTIFYING THE MOST SIGNIFICANT PRIVACY RISKS

Most Significant Privacy-Related Risks to Organizations

Percentage of Respondents Indicating Risk Is in Top Three



n = 54.

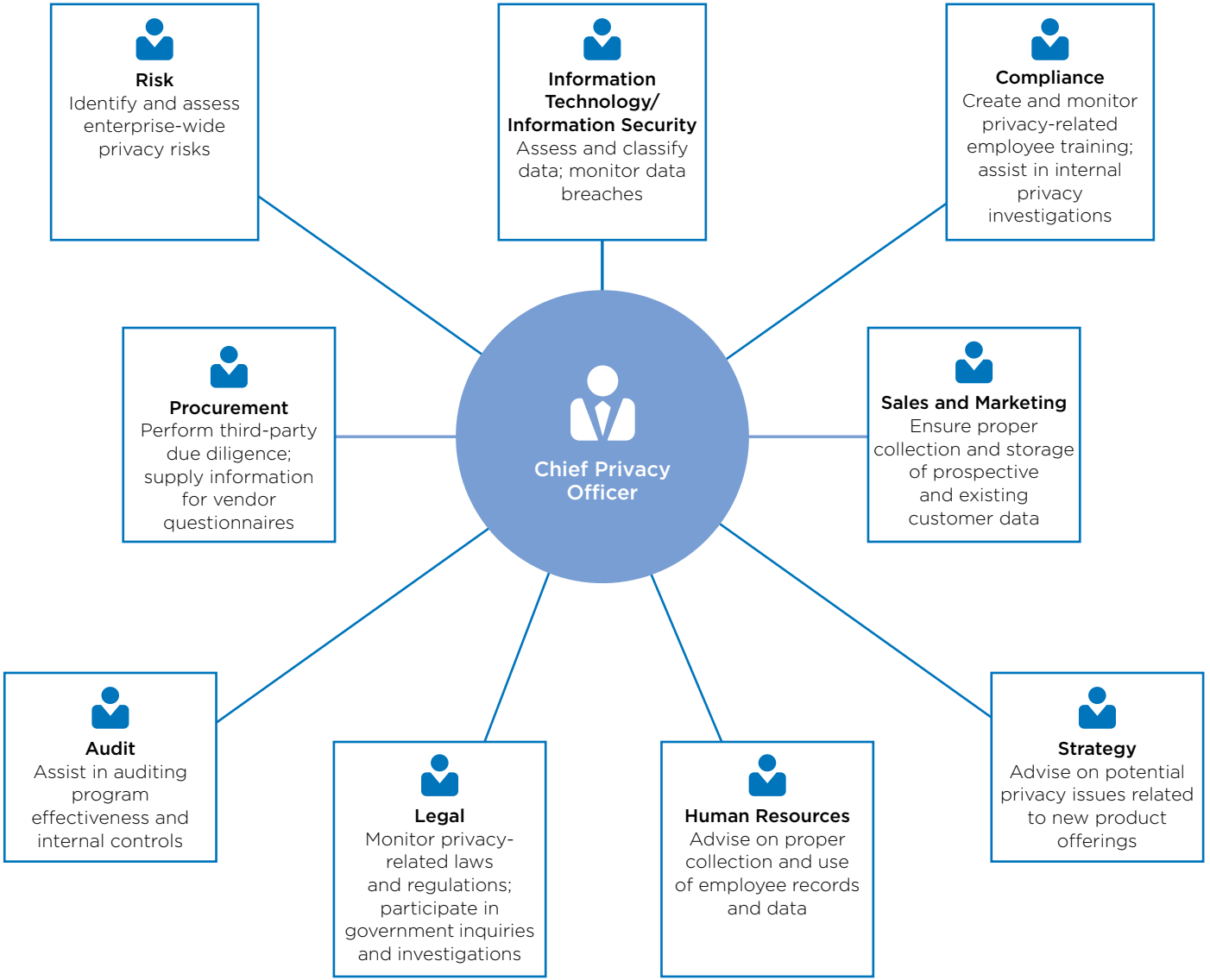
Source: CEB 2014 State of the Privacy Function Survey.

Chief privacy officers increasingly work with other functions to ensure that data is properly categorized and protected.

- Although the head of privacy is ultimately accountable for the program, his or her success depends on working closely with key stakeholders across the organization, including leaders from IT/IS, HR, Internal Audit, Sales, Legal, Compliance, and the business.

COLLABORATING WITH MULTIPLE STAKEHOLDERS

Select Joint Initiatives Between the Chief Privacy Officer and Other Functional Heads
Illustrative



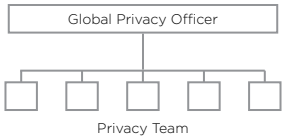
Successful privacy programs vary in structure, including reporting lines, resource commitment, and business unit ownership of program activities.

- Regardless of the type of structure, privacy heads report the complexity of business operations as one of the biggest barriers to effectiveness.

ORGANIZATIONAL MODELS FOR PRIVACY PROGRAMS

Representative Organizational Structures, Listed by Degree of Centralization

Model 1: Centralized Privacy Program — 43%



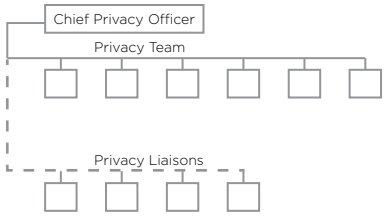
Highest Priority Activities
- Create metrics to measure effectiveness
- Safe Harbor certification
- Monitor employee compliance with privacy program

Typical Adopters
- Transportation, Banking, Pharmaceuticals, B2B Companies

Biggest Barrier to Effectiveness
- Complexity of business operations; lack of predictive metrics; technology constraints

Satisfaction Level[a] : 2.80

Model 2: Hybrid Privacy Program — 21%



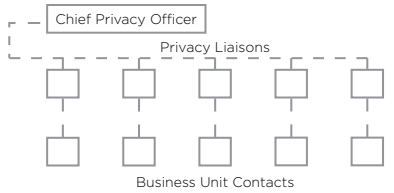
Highest Priority Activities
- Create metrics to measure effectiveness
- Conduct data inventory
- Review systems-related information security plans

Typical Adopters
- Construction, Utilities, Professional Services

Biggest Barrier to Effectiveness
- Complexity of business operations; corporate culture; resistance from the business

Satisfaction Level[a] : 3.25

Model 3: Decentralized "Virtual" Privacy Program — 36%



Highest Priority Activities
- Conduct data inventory
- Create tools for employees to comply with privacy policy

Typical Adopters
- Insurance, Health Care, Energy, B2C Companies

Biggest Barrier to Effectiveness
- Complexity of business operations; staff skills; regulatory requirements

Satisfaction Level[a] : 3.21

Source: CEB 2014 State of the Privacy Function Survey.

[a] Satisfaction levels were scored from 1–5 (1 = Very Unsatisfied, 5 = Very Satisfied).

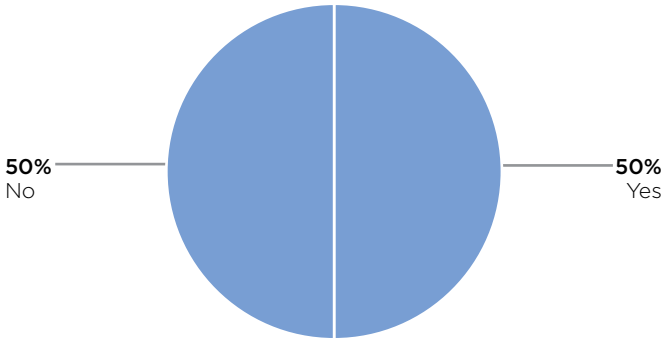
Half of privacy functions have a corporate privacy committee.

- The average committee has three participants.
- Other participants in privacy committees include business unit heads, Assistant or Deputy General Counsel, privacy liaisons, and research heads.

PORTRAIT OF A CORPORATE PRIVACY COMMITTEE

Existence of a Corporate Privacy Committee

Percentage of Respondents

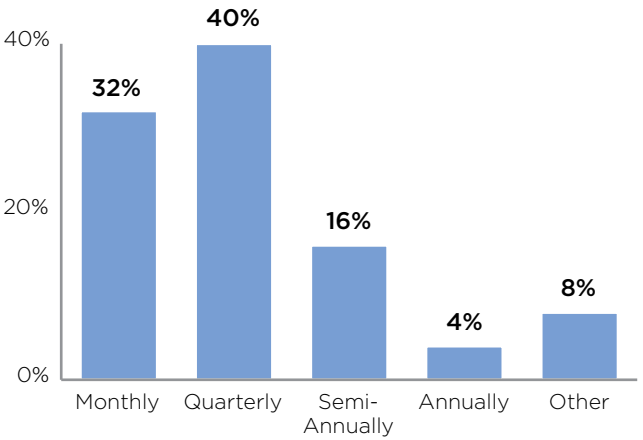


n = 64.

Source: CEB 2014 State of the Privacy Function Survey.

Frequency of Corporate Privacy Committee Meetings

Percentage of Respondents

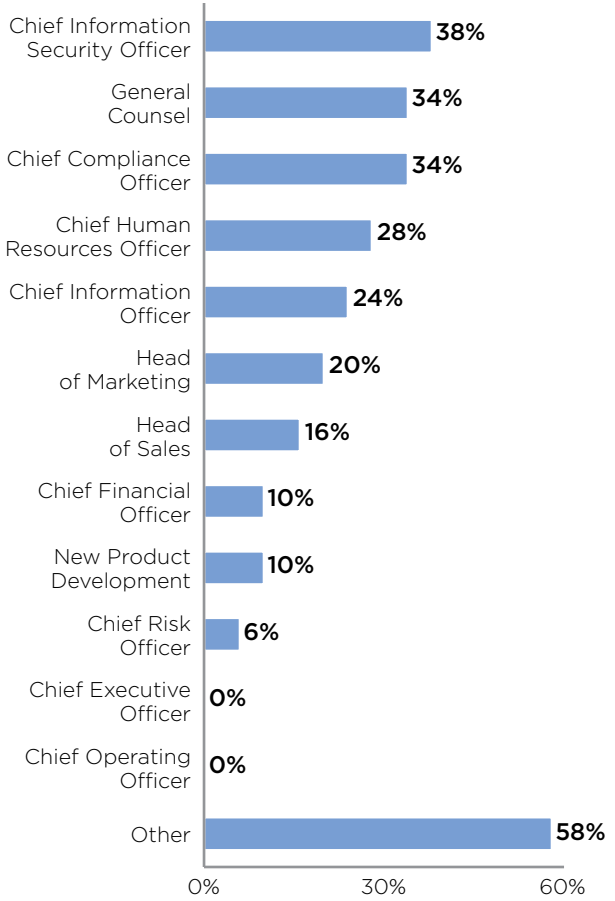


n = 63.

Source: CEB 2014 State of the Privacy Function Survey.

Members of the Corporate Privacy Committee

Percentage of Respondents



n = 58.

Source: CEB 2014 State of the Privacy Function Survey.

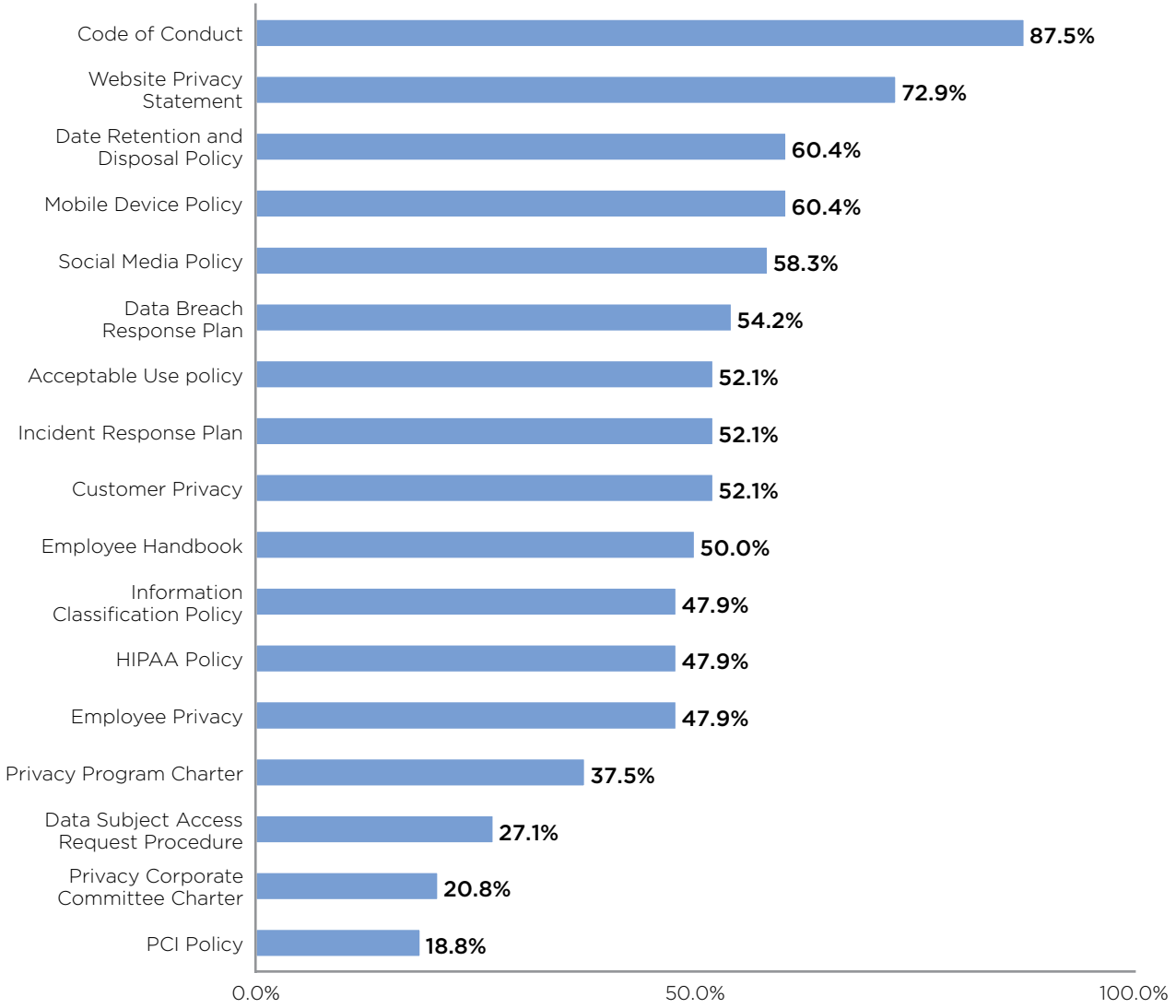
Most privacy departments underappreciate the value of cross-functional collaboration when creating privacy-related policies.

- The average privacy department maintains more than eight privacy-related policies.

CASE IN POINT: DRAFTING INFORMATION POLICIES

Policies Addressing Privacy Issues

Percentage of Company Policies Addressing Privacy Issues



n = 48.

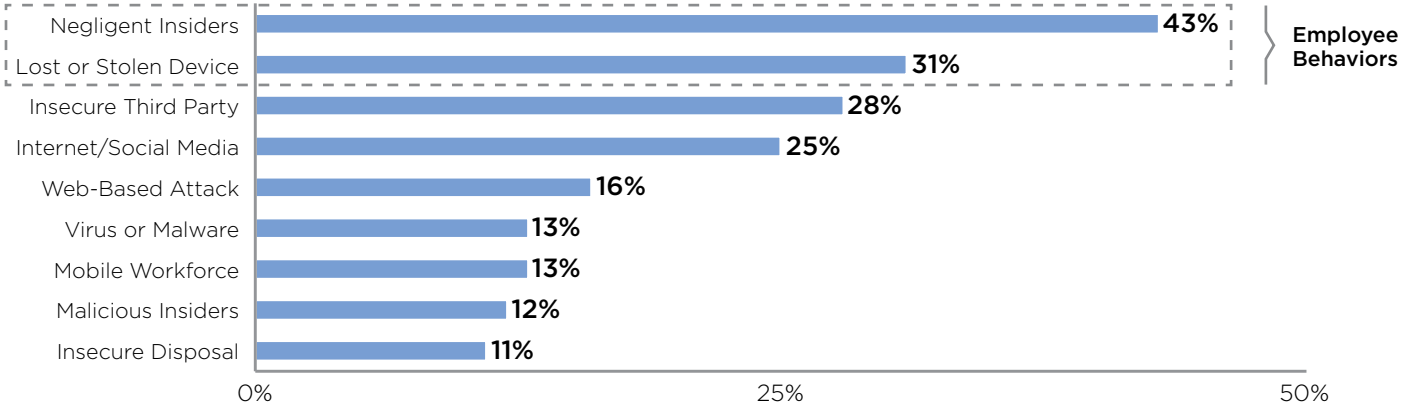
Source: CEB 2014 State of the Privacy Function Survey.

The greatest risks associated with the use of sensitive data are related to employee negligence.

- Data privacy violations are three times more likely to be unintentional than fraud violations and 20 times more likely than antitrust violations.
- In 42% of cases, unintentional violations occurred because the employee was unaware of the requirements.

EMPLOYEES ARE THE GREATEST SECURITY THREAT

Source of Greatest Risk of Sensitive Data

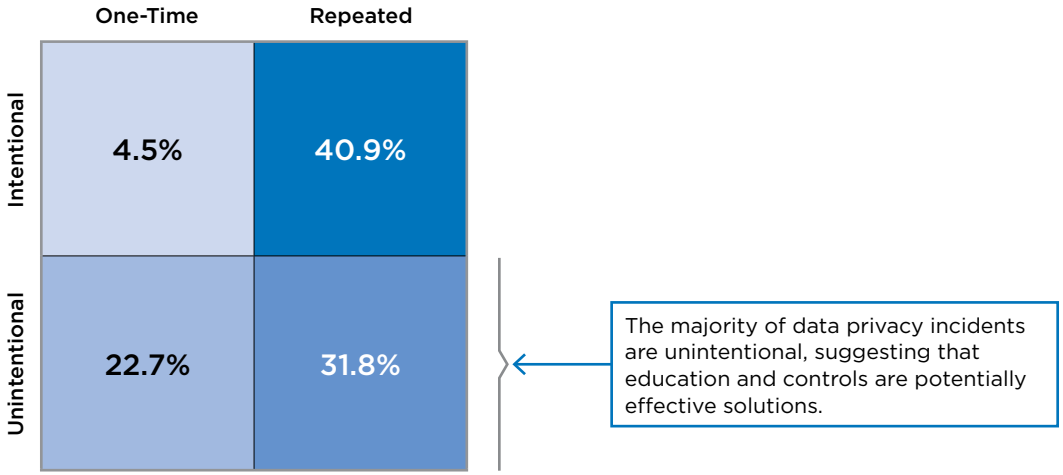


n = 265 senior executives. Two responses allowed.

Source: Ponemon Institute, Business Case for Data Protection, March 2012.

Breakdown of Data Privacy Incidents

Percentage of Incidents, by Intentionality and Occurrence



n = 66.

Source: CEB 2014 Compliance Failures Analysis.

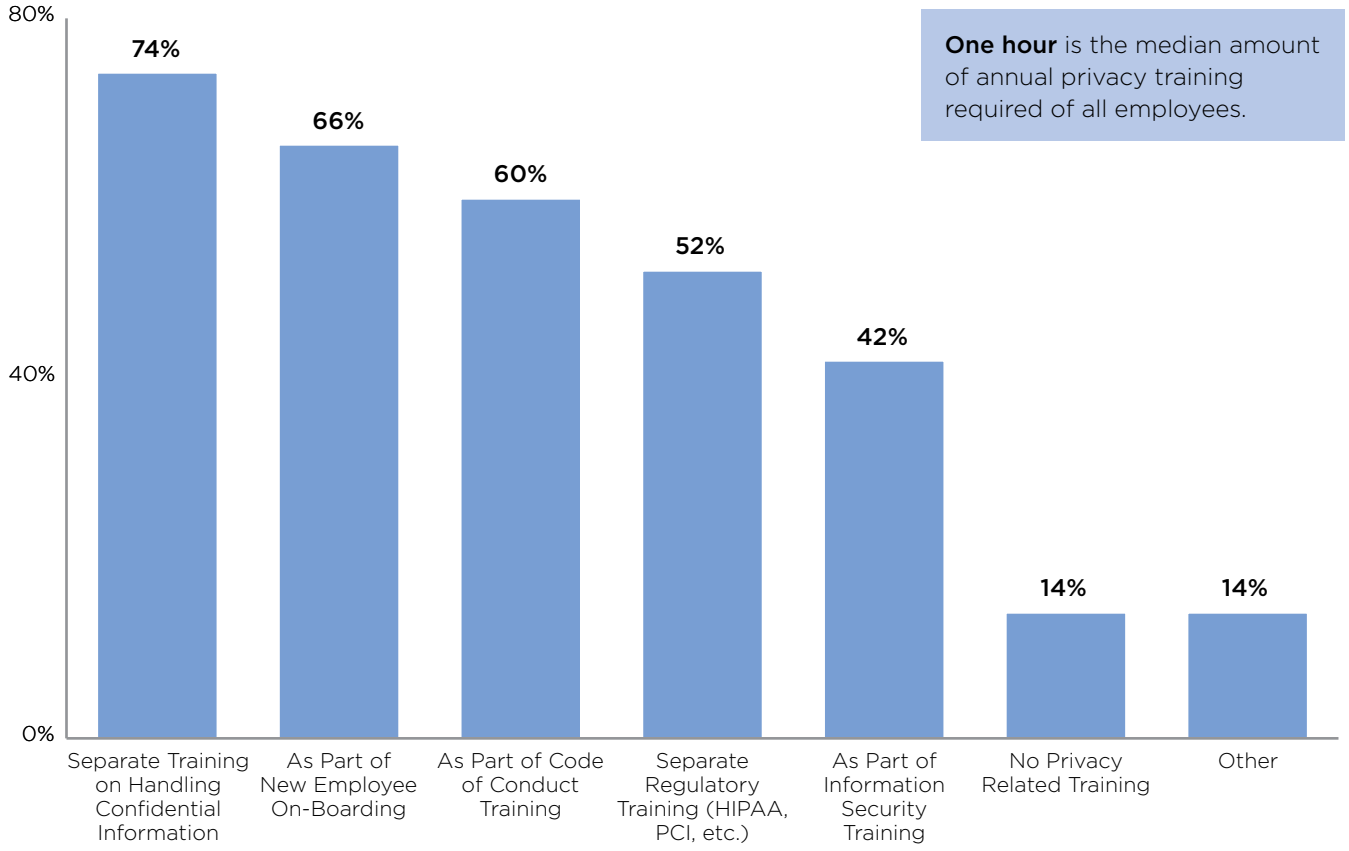
Privacy programs use a variety of means to conduct privacy training for their employees.

- More than half of privacy departments are not satisfied with their training.
- Forty-six percent of privacy departments indicate their budget allocation for training will increase in 2015.

FORMATS FOR DATA PRIVACY TRAINING

Employee Training Methods

Means of Training Employees on Privacy-Related Issues



One hour is the median amount of annual privacy training required of all employees.

n = 50.

Source: CEB 2014 State of the Privacy Function Survey.

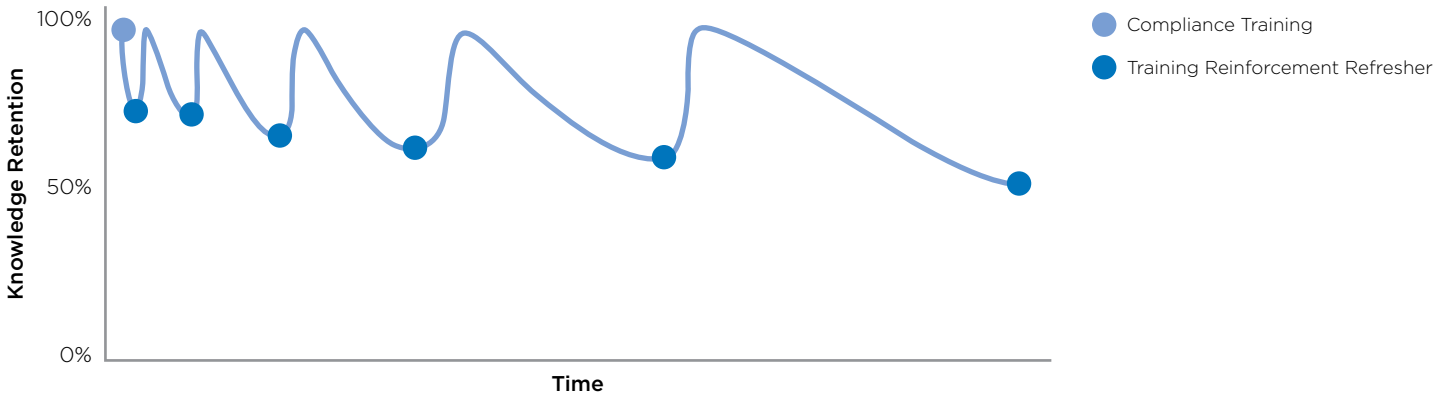
Even effective privacy training quickly loses its impact unless reinforced by accessible support and decision-making guidance.

- Reinforcement is as important as the training event itself and critical to building long-term memory and securing desired behavior.

REINFORCEMENT IS KEY TO RETENTION

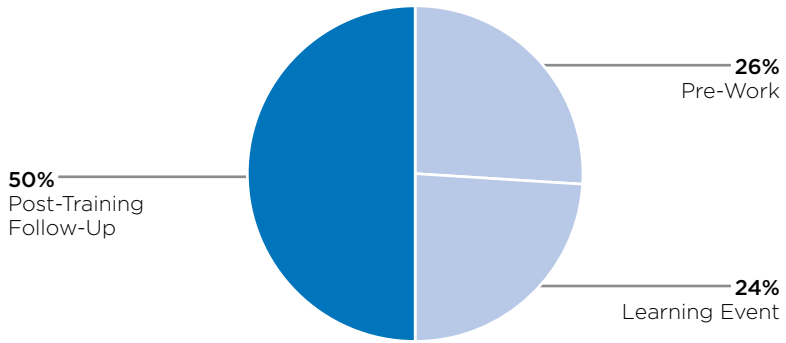
Knowledge Retention Curve

Illustrative



Source: Based on Hermann Ebbinghaus's "Forgetting Curve" and subsequent research on memory and cognition.

Activities Contributing to Learning Effectiveness



Source: "The Promise of Phase 3," T+D Magazine, The American Society of Training and Development, January 2005.

Infrequent Communications

- Only 7% of compliance programs provide post-training refreshers (two to five minute refreshers of training theme).
- Only 36% of employees remember key lessons from training.
- Only 45% of employees receive any post-training communication.

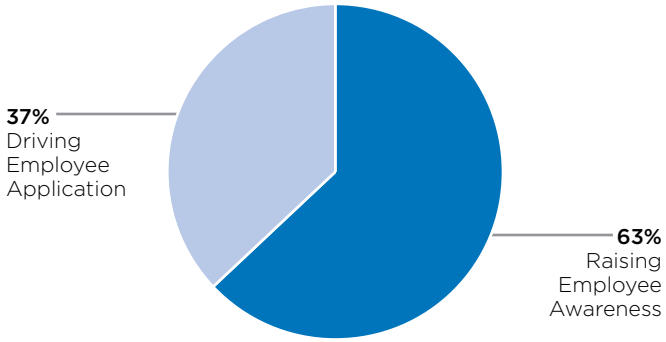
Compliance programs must shift the focus of their training from awareness to application.

- The majority of compliance executives design their training around raising employee awareness; as a result, employees possess less comfort applying concepts to their job.

MISPLACED FOCUS

Primary Desired Outcome of Current Compliance Training

Percentage of Respondents

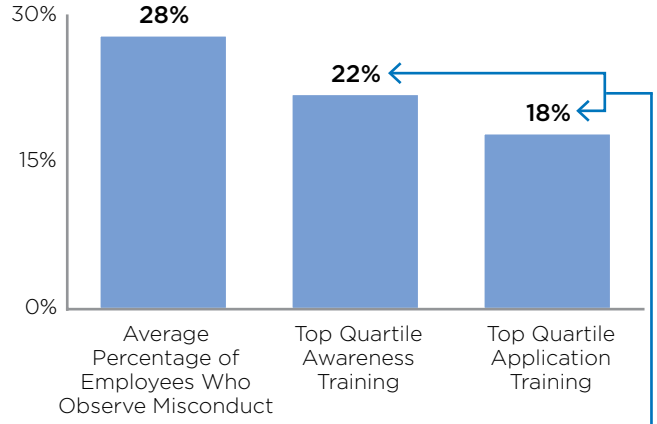


n = 104.

Source: CEB analysis.

Employee Observations of Misconduct

Percentage of Employees Observing Misconduct by Type of Compliance Training



n = 3,019.

Source: CEB analysis.

In an organization of 20,000 employees, the movement from awareness to application training translates to 800 fewer employees observing misconduct.

"We feel pressure not to add several additional hours of training to the calendar for data privacy, but we know it must be a priority. How do we build something that is digestible? How can we create trainings to respond to specific occurrences, like after a data breach?"

General Counsel
Health Care Company

KEY TAKEAWAYS

Clarify Stakeholder Expectations and Prioritize Critical Activities Accordingly—Work with key senior stakeholders to clarify their expectations, and set clear goals for the program. In addition, once privacy department priorities are set, benchmark the department's staffing and resourcing to get a better understanding of where it may be under-resourced.

Leverage Other Functional Heads to Maximize the Effectiveness of Privacy Initiatives—Privacy functions that gather input from other functional leaders (and employees) often create more effective privacy policies, and obtain better senior management buy-in and employee adoption.

Maximize Training Effectiveness by Targeting High-Risk Employees and Delivering Actionable Training— Target training efforts towards high-risk employees (e.g., employees that handle large amounts of sensitive data, social media users) to manage the risk of data misuse or mishandling. In addition, create memorable training by linking it to real-life situations and tasks that are specific to the employee.

Contact Us to Dive Deeper into the Full Report and Learn More About CEB's Data Privacy Leadership Council.

UPCOMING INSIGHTS AND TOOLS FROM THE DATA PRIVACY LEADERSHIP COUNCIL:

Elements of a Highly Effective Privacy Program

Create a Formal Privacy Program

- Models for Privacy and Information Risk Governance
- Benchmarking Data on Resources, Structure and Staff

Understand the Location and Use of Data Assets

- Sample Data Classification Policies
- Information Classification Best Practices Checklist

Evaluate Existing Privacy Controls

- Database of Laws and Regulations for 50+ Countries
- Privacy Questionnaires for Other Corporate Functions

Prioritize Efforts Based on Organizational Risks

- Data Privacy and Information Security Hot Spots
- Mobile Device Toolkit

Develop Policies and Training

- Privacy Policy Database
- Best Practices on How to Develop Best-in-Class Training

Monitor and Report Program Performance

- Privacy Department Metrics Toolkit
- List of Most Commonly Used Metrics

Who We Are

CEB Data Privacy Leadership Council is a global network of heads of privacy and Chief Privacy Officers. We support leading companies and their privacy executives with our best practices, tools, templates, benchmarks, program maturity diagnostic and advisory support. It is our mission to bring science, standards and clarity to privacy programs.