

The Danger Within

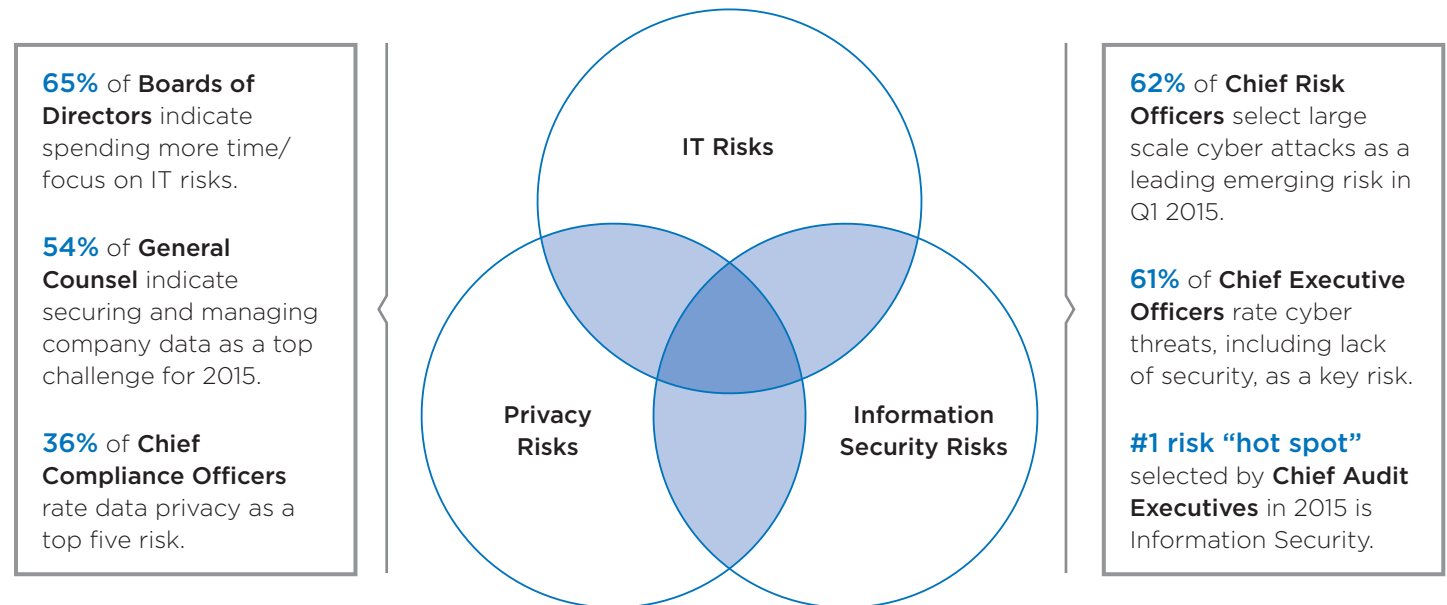
Addressing the Internal Risks of Privacy Failures

Preview Report

Privacy- and technology-related risks increasingly surface as top-level concerns for both senior executives and boards of directors.

PRIVACY AND TECHNOLOGY CONCERNS CONVERGE

Leadership Perceptions of Privacy and Technology Risks



Source: PwC 2014 Annual Corporate Directors Survey; PwC 2015 Annual Global CEO Survey; CEB 2015 Legal Department Priorities; CEB 2014 State of the Compliance Function Survey; CEB 2015 Audit Plan Hot Spots; CEB Q1 2015 Emerging Risks Report and Monitor.

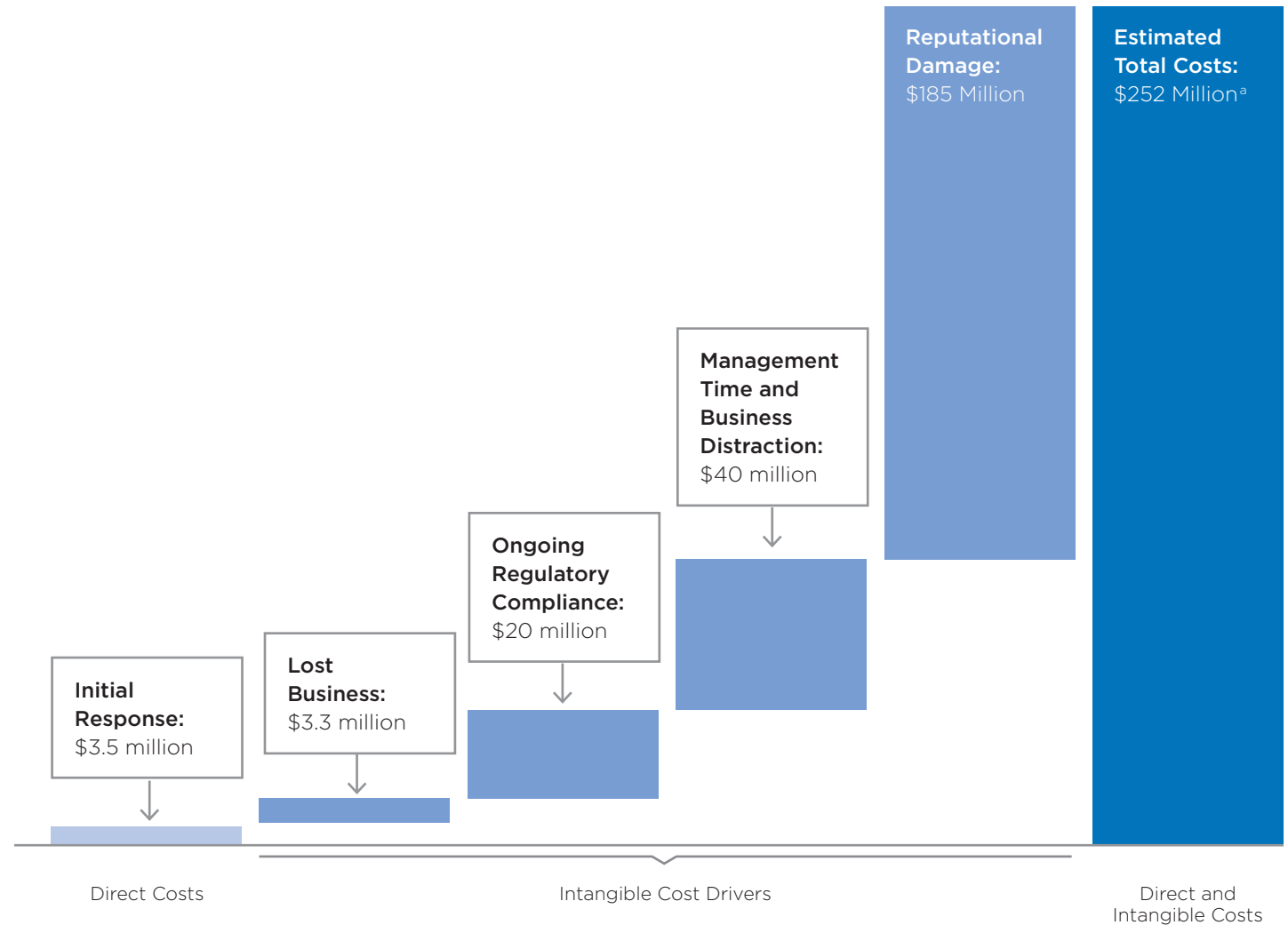
The total costs of privacy failures far surpass initial expenditures, and these costs can compound as new issues arise before others fully resolve.

- Many times companies will experience subsequent privacy failures before fully resolving older incidents, multiplying the impact of privacy failures and costs over time.

THE TRUE COST OF A PRIVACY FAILURE

Costs Associated with Privacy Failures

Estimated



Source: Ponemon, 2015 Cost of a Data Breach Study: Global Analysis; CEB analysis.

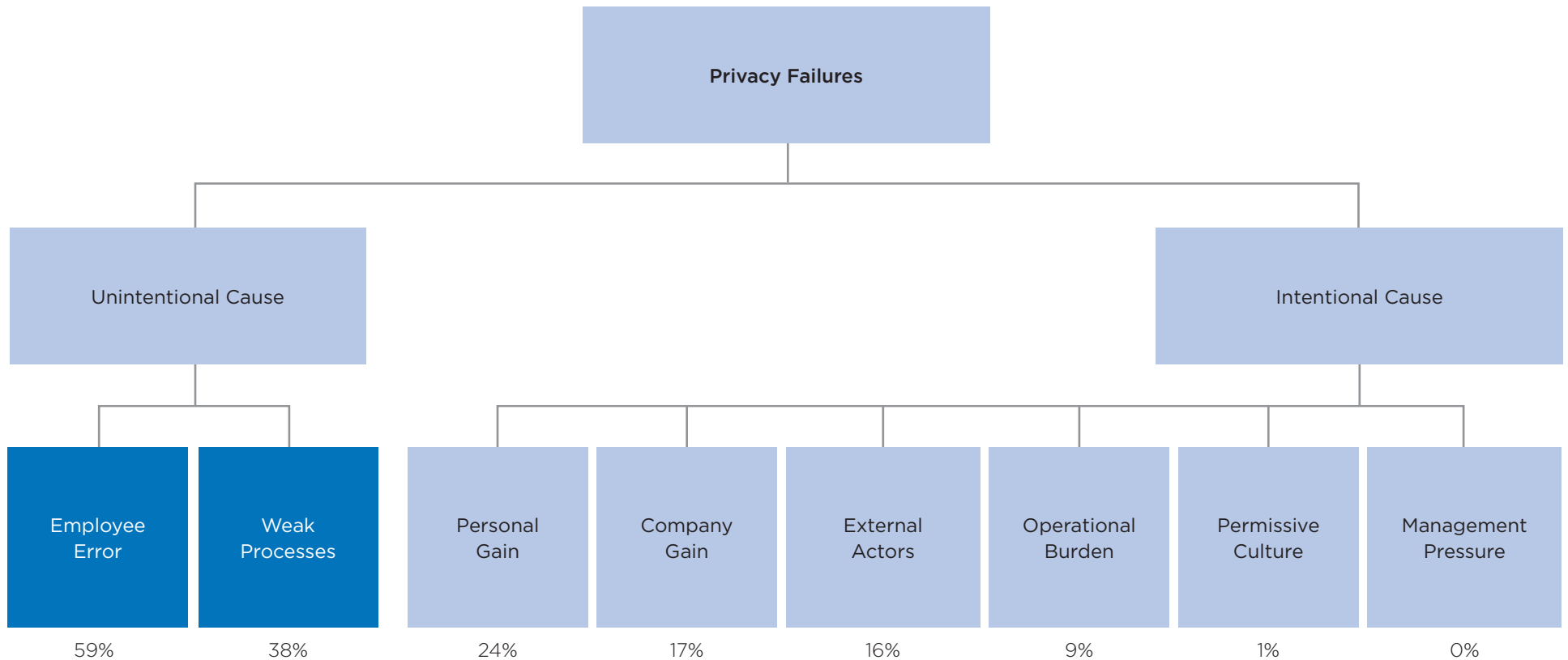
^a Excludes settlements and fines, which usually amount to < 1% of total revenue.

WHY DO PRIVACY FAILURES HAPPEN?

Root Causes of Privacy Failures

Percentage of Privacy Failures^a

Privacy failures disproportionately result from employee errors and weak processes, even compared to intentional, malicious outsiders.



n = 82.

Source: CEB 2015 Compliance Failures Analysis.

^a Percentages sum to more than 100 to account for privacy failures deriving from more than one root cause.

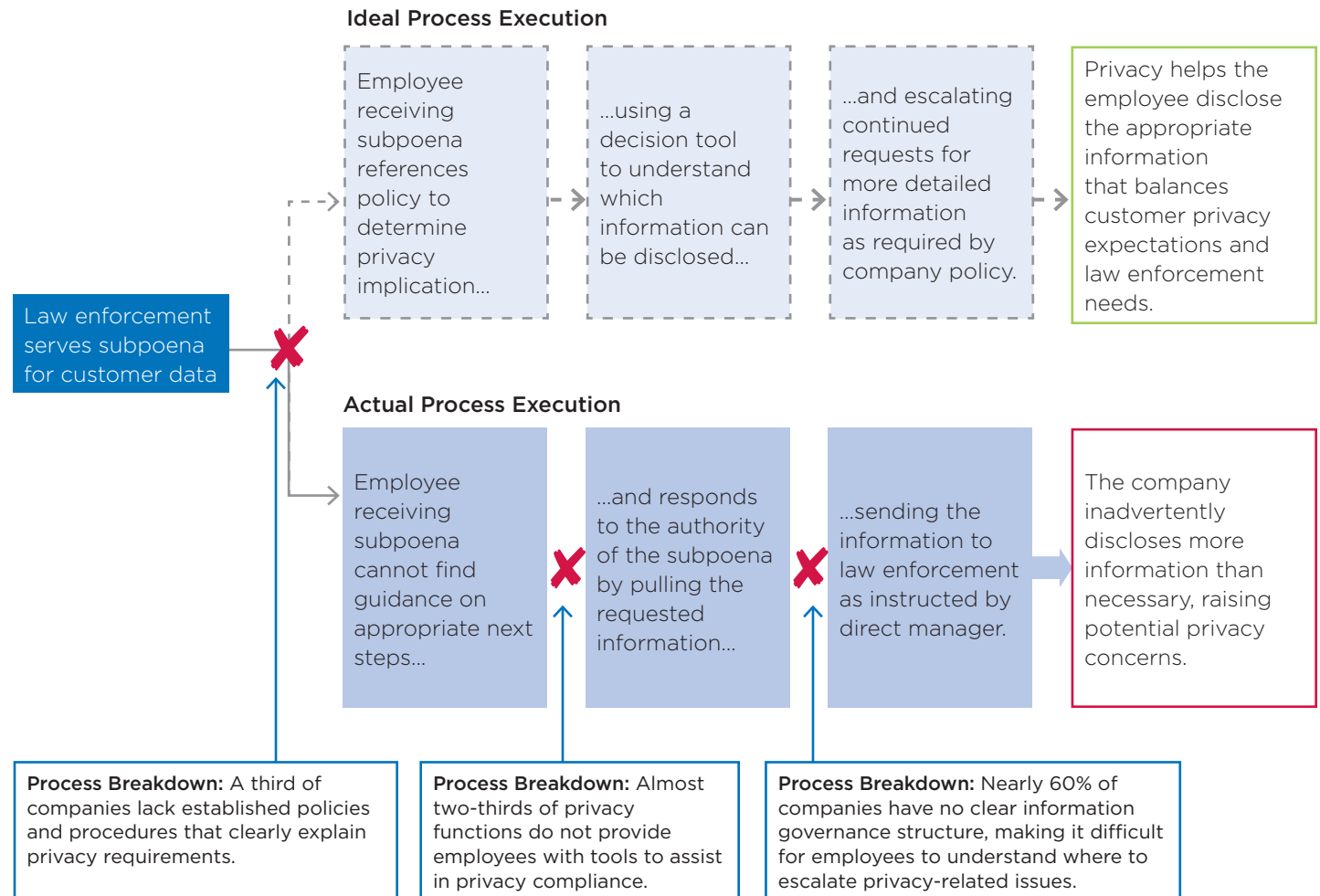
Many companies struggle with developing cohesive privacy frameworks, including clear tools and process guidance, that enable employees to easily make decisions about data and information.

- Without clearly defined parameters, privacy functions struggle to establish consistent approaches to addressing privacy concerns, leading to disjointed management and frequent process breakdowns.
- Employees commonly contribute to process failures in an attempt to meet seemingly innocent business demands and needs.

MISTAKE 1: WEAK PROCESSES LACKING GUIDANCE

Ideal Versus Actual Process Execution

Illustrative



n = 53-57.

Source: CEB 2014 State of the Data Privacy Function Survey; CEB analysis.

Companies with leading education efforts experience drastically reduced occurrences of inappropriate employee behaviors, but most privacy functions provide only limited training each year.

MISTAKE 2: EMPLOYEE ERROR DUE TO LIMITED TRAINING

Average Secure Behavior by Organization

Secure Behavior Index

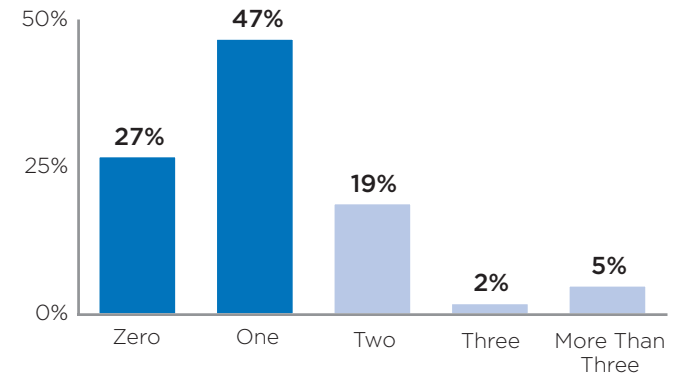


CEB research shows that the average propensity for insecure employee behavior is approximately 22%; however, companies with best-in-class education efforts see secure behavior scores approaching 90%.

Source: CEB Employee Awareness/CISO Survey; CEB analysis.

Annual Privacy Training

Hours of Annual Training, by Percentage of Companies



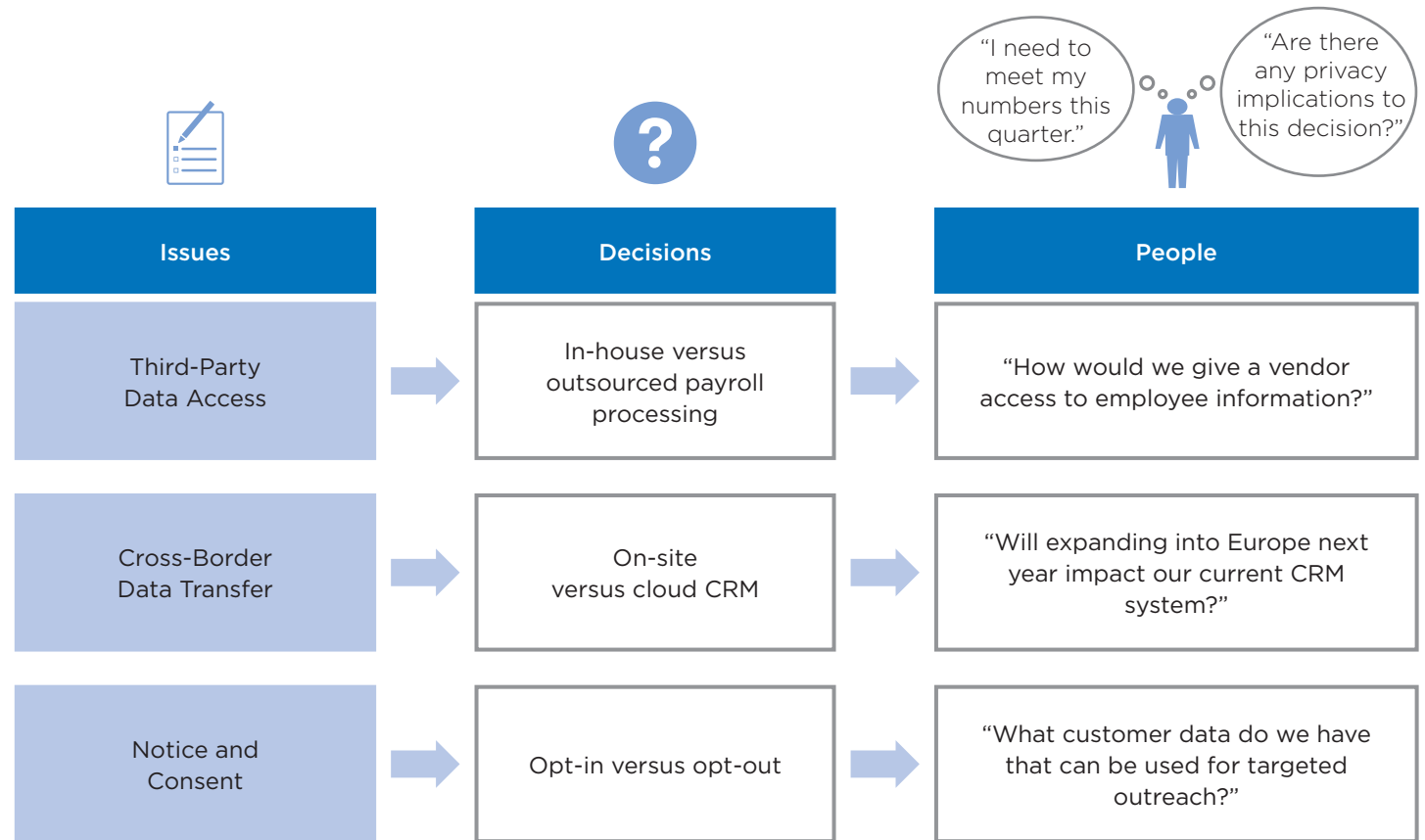
Roughly 50% of companies incorporate privacy training into other training courses, and the brief time spent on privacy content makes it difficult for employees to understand and correctly apply appropriate behaviors.

$n = 59$.

Source: CEB 2014 State of the Data Privacy Function Survey.

A singular focus on privacy issues may fail to capture the personal context in which employees create risk.

FOCUS ON PEOPLE, NOT ISSUES



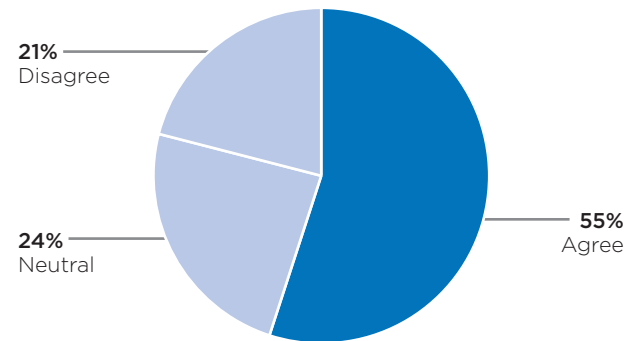
Source: CEB analysis.

Over half of employees making privacy-related decisions believe policies and procedures slow down business execution, with the majority of employees preferring manager or peer guidance over tools, training, and policies.

- The perceived burden of compliance results in a 42% negative impact on employee compliance.

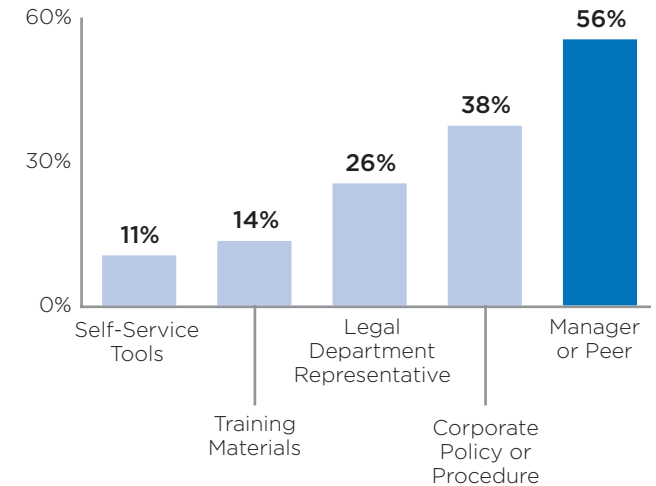
PROCESS EXECUTION IS NOT MADE EASY

Employee Agreement That Policies and Procedures Slow Business Execution
Percentage of Respondents Making Privacy-Related Decisions



n = 1,033.
Source: CEB 2014 Corporate Legal Decision-Making Survey.

Employee Use of Resources When Making Privacy-Related Decisions
Percentage of Respondents



n = 1,033.
Source: CEB 2014 Corporate Legal Decision-Making Survey.

Rather than take a rules-based approach to policy development and privacy guidance, Eli Lilly creates self-service tools that encourage employee ownership of privacy decisions.

SAMPLE CASE PREVIEW: FROM PRIVACY RULES TO BUSINESS JUDGMENT



Typical Rules-Based Approach

- ✗ To adequately mandate unacceptable behaviors or decisions to effectively minimize risk, Privacy must gain a comprehensive knowledge of employee workflows across the company.
- ✗ Detailed policies attempt to define appropriate employee behavior for every possible circumstance but fail to provide flexibility to adapt to new or unforeseen circumstances.



Lilly's Judgment-Based Approach

- ✓ Lilly assigns accountability for privacy risks to the business, allowing those who best understand specific processes to make judgment-based decisions.
- ✓ Privacy creates tools to support employees as they weigh the privacy risks inherent in a particular process.

Result

A rules-based approach increases the burden of compliance on employees while requiring an extensive resource investment from Privacy, both in terms of developing such comprehensive rules and monitoring compliance.

Result

Enabling employee judgment streamlines the decision-making process and ensures that employees can own privacy risks within defined but flexible parameters while maintaining adherence to privacy laws and regulations.

Elements of Process-Embedded Privacy Guidance

Prioritize High-Risk Processes

Privacy determines which processes would benefit from guidance by using risk factors such as likelihood, impact, and velocity as filters.

Create Easy-to-Use Guidance

Tools embedded into existing workflows provide accessible guidance without disrupting processes, discouraging employees from circumventing privacy controls.

Promote Consistent Adoption

Lilly tracks employee use of privacy tools to revise guidance when business processes change.

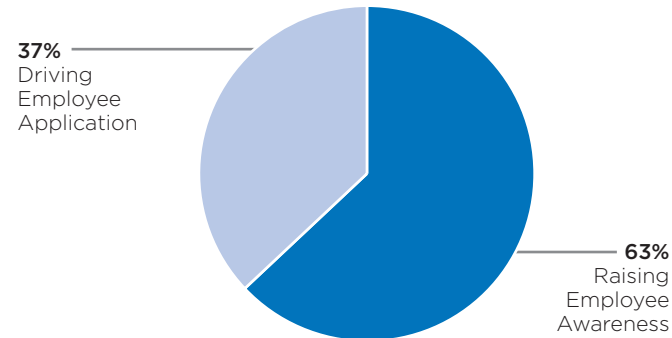
Source: Eli Lilly and Company; CEB analysis.

Most companies see increasing employee awareness as the primary objective of training; however, organizations that focus on teaching employees to apply training concepts experience greater returns on training efforts.

- Training that drives application contributes to higher levels of employee engagement and discretionary effort.

MISSING THE BENEFITS OF APPLICATION TRAINING

Members' Primary Desired Outcome of Current Training
Percentage of Members

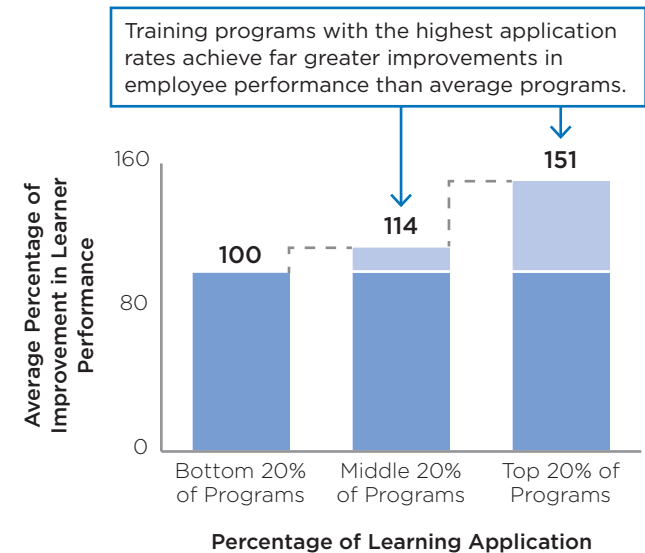


n = 104.
Source: CEB analysis.

Awareness Training: Conveys compliance expectations and risks conceptually without necessarily helping employees understand how to mitigate risk to the organization.

Application Training: Prompts mastery of learning concepts and overcoming obstacles to implementation by developing job-relevant skills and fostering motivation to apply training in all work contexts.

The Additional Impact from Achieving High Learning Application
Indexed^a



Source: CEB 2013 Learning and Development Effectiveness Survey.
^a For the purposes of illustration, improvements in learner performance were indexed to a scale on which 100 points indicates the improvements in learner performance of programs with the bottom 20% of application rates across programs.

Application Fuels Engagement


Employees who receive top quartile application training are 21% more engaged than the average employee and 39% more engaged than employees who receive bottom quartile application training.

Application Drives Discretionary Effort

Employees who receive top quartile application training display 12% more discretionary effort than the average employee and 22% more than employees who receive bottom quartile application training.

Privacy delivers messages to the right people at the right time, teaching employees how to apply privacy concepts to their particular circumstances.

- Western Union currently maintains a library of seven roughly two-minute privacy training reminder videos and continues to expand its library of training content.

 "The combination of videos, newsletters, and e-mail at various times across the year has increased privacy awareness."

Chief Privacy Officer

SAMPLE CASE PREVIEW: TARGET MESSAGES TO IMPROVE RETENTION



Privacy Message Targeting

Illustrative

Third-Party Agent



Video Reminder Training:
Security for Agents



Targeted Outreach

Privacy responds to new risks, regulations, and money services for Western Union agents with targeted external awareness efforts, improving agent's understanding of how to apply privacy and information governance concepts.

New Hire



Quarterly Newsletter:
Privacy 101



Consistent Messages

Targeted outreach through quarterly newsletters reminds employees to apply privacy practices to external activities.

HR Manager



New Project E-Mail:
Information Governance



Project-Specific Advice

Employees involved in information-related initiatives receive targeted communications that outline specific steps they must take as part of the initiative.

Source: Western Union; CEB analysis.

The Danger Within

Addressing the Internal Risks of Privacy Failures

Preview Report

Contact us directly to dive deeper into this report and learn how CEB can help you understand and implement the proven practices that drive employees to comply with privacy policies--ultimately reducing business risks.