


Effective Privacy Training & Communications

Key Principles & High-Risk Employee Segmentation

Preview Report

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

- More than half of privacy departments are not satisfied with their training.
- Fifty percent of organizations combine privacy training with annual code of conduct training.
- Fourteen percent of organizations conduct no privacy-related training at all.

 The majority of companies in excess of \$5 billion in revenue conduct data privacy training in the following ways:

- General employee training as part of new employee onboarding
- As part of annual code of conduct training
- Targeted regulatory training (HIPAA, PCI, etc.)

TRAINING REQUIREMENTS

Hours of Privacy Training

Number of Hours Required Annually of All Employees

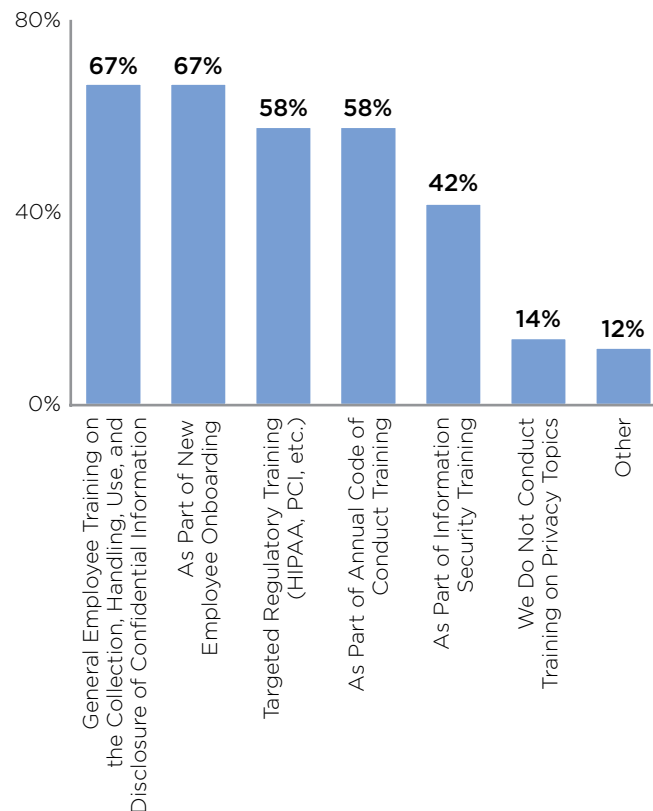
Mean	25th Percentile	Median	75th Percentile
2.91	0.00	1.00	2.00

n = 69.

Source: CEB 2014 State of the Privacy Function Survey.

How Privacy Training Is Incorporated

Percentage of Respondents, Multiple Responses Permitted

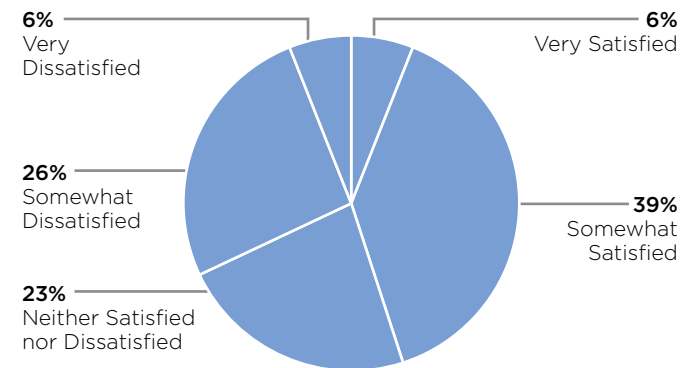


n = 69.

Source: CEB 2014 State of the Privacy Function Survey.

Satisfaction with Training Efforts

Percentage of Respondents



n = 69.

Source: CEB 2014 State of the Privacy Function Survey.

CEB GUIDANCE: KEY PRINCIPLES FOR DESIGNING AN EFFECTIVE PRIVACY TRAINING AND COMMUNICATIONS PROGRAM

1 Focus on the Do's and Don'ts

The single most impactful driver of behavior is training content that tells employees how to be secure in a way that is relevant to their day-to-day activities.

2 Provide More Training Hours

Although fears about employees receiving too many compliance trainings or messages may seem reasonable, an employee's behavior becomes more secure with additional training.

3 Keep Communications Frequent

Most employees receive fewer than three direct and indirect communications each month; however, each extra communication is helpful at reminding employees what they should and should not do.

4 Brand Your Privacy Campaign

When privacy and security training and communications programs are branded and given a consistent look and feel, the overall impact of the program increases.

5 Segment Employees Based on the Characteristics That Matter

Three key demographic attributes—role, level within the organization, and geographic region—affect an employee's compliance with privacy and security policies. Segmenting employees according to these attributes and developing unique training for each group improves rates of compliance.

Source: CEB analysis.

More detail provided in this preview report. To access principles #3 and #4, [contact us](#) for more information.

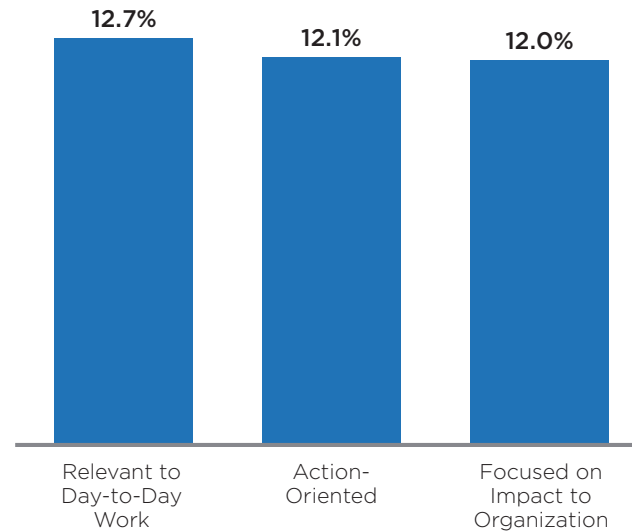


The most effective message content identifies exactly what employees should or should not do to protect their organization.

KEY PRINCIPLE 1: FOCUS ON THE DO'S AND DON'TS

Impact of Message Content

Secure Behavior Index (Maximum Impact)



Company Case Profile: Virtual Suggestions Drop Box (Delta Company¹)

- Delta Company's CISO creates a security suggestions e-mail address to which users can send questions, concerns, or possible improvements to information security policies.
- The address is included in all awareness and training materials pushed out to the user population.
- An automated response acknowledging suggestion and thanking the user for submission is key to ensuring ongoing utilization.
- User suggestions provide insight into the frontline workflows and processes competing for user attention to security policies.

¹ Pseudonym.

Source: Information Risk Executive Council research.

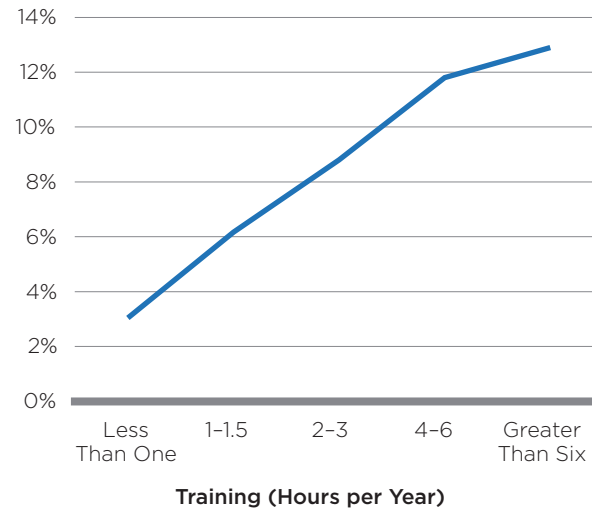


Diminishing returns on training don't set in until after six hours per year, but most employees receive far less than that.

KEY PRINCIPLE 2: PROVIDE MORE TRAINING HOURS

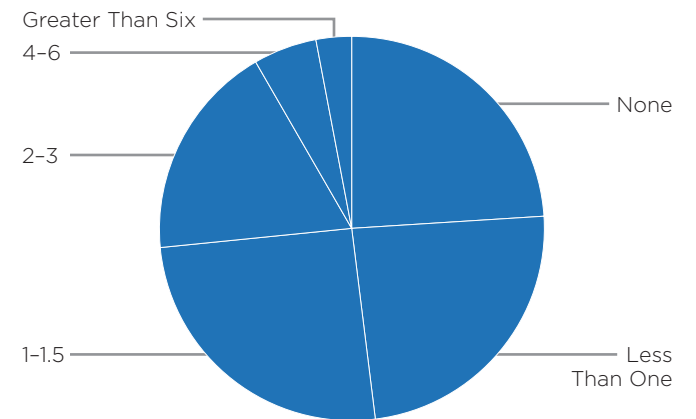
Impact of Training

Secure Behavior Index (Maximum Impact)



Annual Hours of Training

Percentage of Responses



Company Case Profile: Security Training for Laptop Users (Bank of Scotland)

- Mindful of special risks posed by laptop users, Bank of Scotland requires all staff with laptops to attend live training on secure laptop use.
- In-room training allows instructors to provide users with immediate feedback and to provide answers to particular user concerns. Such exchange allows users to learn from one another's mistakes.
- Beyond merely communicating policies, risks, standards, and procedures related to laptop use, the training sessions allow users to learn the necessary concepts in an interactive, risk-free environment. The experiential learning garnered from in-room training leads to better understanding and retention.

Source: Information Risk Executive Council research.

Companies should segment employees based on their demographics.

- An employee's role is the strongest predictor of how he or she will respond to various categories of training and communications methods.

KEY PRINCIPLE 5: SEGMENT EMPLOYEES BASED ON THE CHARACTERISTICS THAT MATTER

User Characteristics Tested for Effect on Secure Behavior

Characteristics	Ease of Targeting	Effect on Behavior
Role	Easy	✓
Geographic Region	Easy	✓
Level Within Organization	Easy	✓
Computer Savvy	Medium	✗
Amount of Travel	Easy	✗
Tenure	Hard	✗
Age	Medium	✗

Target based on these characteristics which affect behavior and allow for easy segmentation

Do not target—no effect on behavior

Effectiveness of Awareness Tactic, by Role

Role	Incentives			Message Characteristics				
	Positive	Negative	Empowerment	Frequency	Content	Source	Medium	Saliency
Sales and Marketing	XX	✓✓		XX		X	✓	✓
Corporate Administration, Legal, and Strategy	X	✓✓	XX	✓	XX	X	✓✓	XX
R&D		✓						
Finance, Accounting, and Purchasing		✓	✓	✓✓		X	XX	
HR		XX			✓✓	✓	XX	✓✓
Administration Assistant and Clerical	✓✓	✓✓	✓	✓	XX	✓✓	XX	XX
Customer Service					✓		✓ ¹	
Application Development		XX	X		✓		✓✓	
Other IT	X	X		✓	✓		X	✓
Manufacturing	✓							

¹ Best context for training was IT-focused training.

Source: Information Risk Executive Council research.

✓✓ Focus Efforts on These Approaches
 ✗✗ Less Effective Than Typical
 ✓ More Effective Than Typical
 ✗ Much Less Effective Than Typical

CASE STUDY: SEGMENT HIGH-RISK EMPLOYEES

OVERVIEW

While trying to address the business' desire for greater balance between security and utility of information, the company recognized that assurance should be focused on those employees who pose the greatest risk of becoming malicious insiders. They used employee risk assessments to identify high-risk employee groups and targeted awareness efforts toward them.

SOLUTION HIGHLIGHTS

- **Employee Risk Assessment:** An employee risk assessment was conducted to identify staff whose roles, functions, and information access make them more risky in terms of information security.
- **Scenario Testing:** Test the security awareness of high-risk employees using real-life information security scenarios.

COMPANY SNAPSHOT

Ferrovial S.A.

Industry: Transportation
 Infrastructure

2013 Income: US\$11.2 Billion

Employees: 57,000

Ferrovial is the world's leading private investor in transportation infrastructures, with a workforce of approximately 57,000 employees and operations in more than 25 countries. The company manages key assets such as Canada's 407 ETR highway and London's Heathrow Airport. It also provides municipal services to more than 800 cities and towns in Spain and to the millions who use the Madrid metro system, and the hundreds of kilometers of streets and highways where they perform maintenance services in the United Kingdom.



To drive balance between information security and utility, Ferrovial identified high-risk employees and prioritized assurance over this segment of staff.

- High-risk employees may be subject to updated and sometimes stricter technical controls, although it is believed this should be complementary to a strong security culture and training.

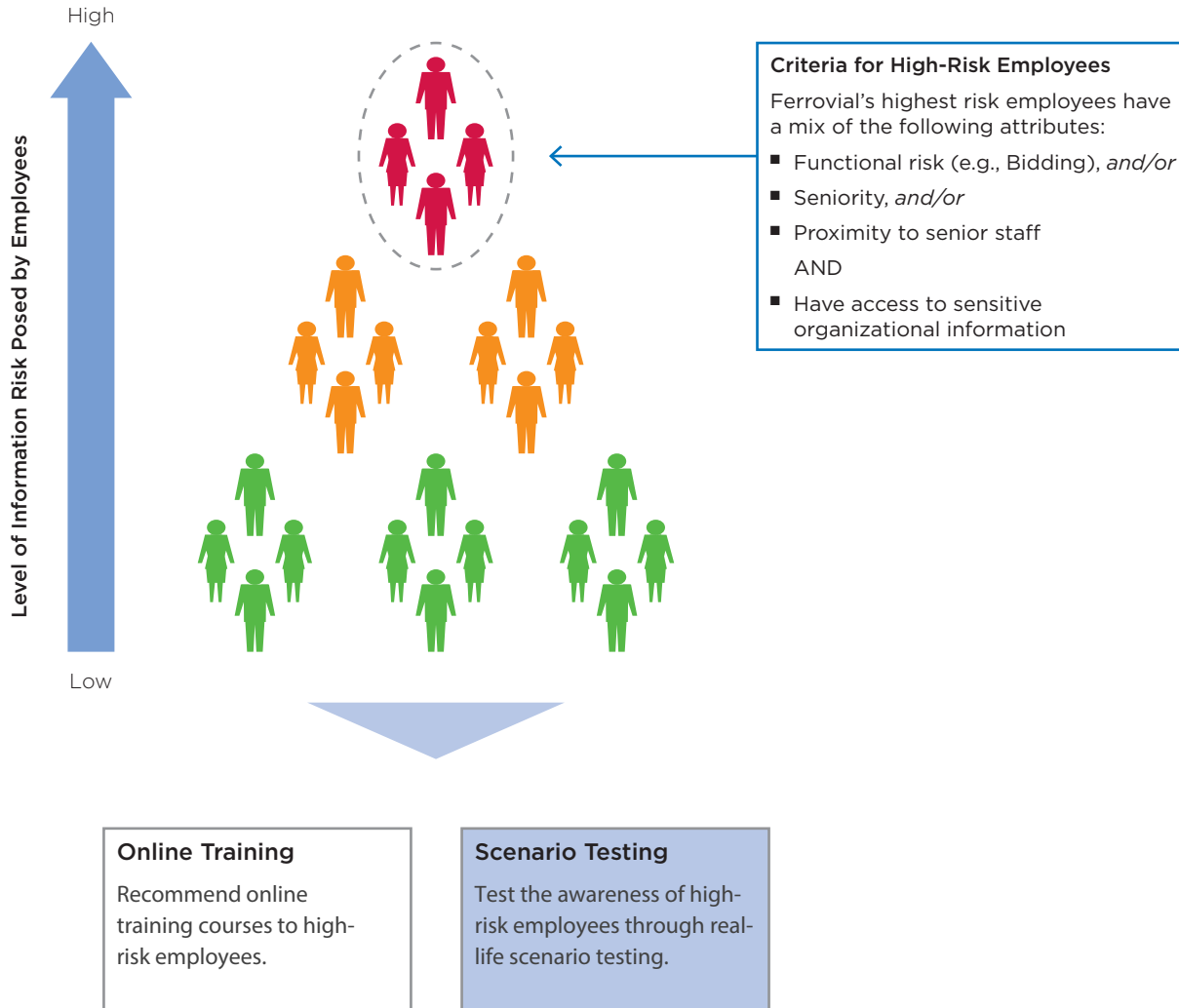


“We are very concerned about internal parties leaking sensitive information. We wanted to identify which people posed the greatest danger based on their responsibilities, seniority, and information access.”

Alberto Ferreira
Chief Audit Executive
Ferrovial S.A.

IDENTIFY HIGH-RISK EMPLOYEES

Ferrovial’s Employee Security Risk Assessment



Source: Ferrovial S.A.; CEB analysis.

Ferrovial tests the awareness of high risk employees using real-life information security scenarios.

- The IT team records all information security incidents that occur at the company, and scenarios are based on these incidents.
- Scenarios based on real incidents demonstrate the reality of information security risk to more skeptical employees.

TEST THE AWARENESS OF HIGH-RISK EMPLOYEES

Ferrovial's Information Security Scenario Testing Process
Illustrative



Incident 1: Malware was uploaded onto isolated network via phishing e-mail.

How Discovered
Employee reported that his laptop was operating extremely slowly.

Root Cause
Awareness: Employee had opened a link in an e-mail from an unknown, malicious source.

Remediation
Computer scrubbed, employee given information on phishing and recommended for online training course

Incident 2: Intruder accessed company networks by "piggy-backing" on employee access via an unsecured Wi-Fi network in a hotel lobby.

How Discovered
Detective controls were triggered by unusual access to networks.

Root Cause
Awareness, Technical: Employee used unsecured public Wi-Fi in hotel. Controls preventing company hardware access to unsecured Internet were circumvented.

Remediation
Highlighted policy on use of unsecure Wi-Fi to access company networks to employee. Updated technical controls organization-wide on company hardware to prevent access to unsecure Wi-Fi.



Implementation Tips

- Develop scenario questions that will pressure test employee awareness of appropriate security behaviors.
- Use open-ended questions, multiple correct answers, and misleading scenarios to avoid questions with obvious answers.

Example Scenario Tests

1. When traveling for work, how would you access the company networks?
2. Which of these are acceptable ways to connect to the Internet using company devices, or to access company networks (including e-mail)?
 - Personal 4G network
 - Company-issued hot spot
 - Public Wi-Fi
 - Password-secured Wi-Fi
 - Public hot spot
3. What is the safest way to work around controls that prevent you from accessing unsecure Wi-Fi?

Effective Privacy Training & Communications

Key Principles & High-Risk Employee Segmentation

Contact us directly to dive deeper into the full report and learn how CEB can help your privacy team implement leading assessments and training practices to reduce business risks.