PROMONTORY
an IBM Company

Sightlines
INFOCUS

promontory.com APRIL 4, 2017

BY JIM GREGOIRE AND LINDA GALLAGHER

Strategies to Modernize and Increase the Effectiveness of Compliance Training

Jim Gregoire is a senior principal and advises clients from various sectors on compliance, privacy and data security, and issues pertaining to staffing, management, strategy, governance, and risk management.

Linda Gallagher is a managing director at Promontory and global head of its consumer protection practice. She has three decades of consulting experience and expertise in all aspects of consumer-oriented regulation, compliance, and risk management.

Companies are under great pressure to carry out effective employee training in regulatory compliance. Inadequate training can lead to regulatory breaches, which in turn can lead to enforcement actions, large fines, and severe reputational damage. New regulations have only added to requirements — and raised existing standards — for corporate due diligence and training.

Yet any company designing, implementing, or even updating its training program confronts formidable complexities and challenges. Not only are requirements and regulatory expectations for training constantly changing, but the most effective ways to reach your audience are evolving because of changing technologies, communication norms, and workplace demographics. What has worked in the past may not work in the future.

Organizations can make employee education more relevant and engaging by adopting strategies to modernize and invigorate their traditional training approaches. A fundamental shift in communications and philosophy for employee education can enhance employee perception of its importance and, ultimately, the training program's effectiveness. Stronger regulatory-compliance training also increases the knowledge (and value) of employees, provides customers with higher-quality products and services, and meaningfully reduces an organization's risk levels.

Regulatory Requirements, Expectations, and Consequences

Regulators have long recognized training as an essential component of a robust compliance program. The Federal Financial Institutions Examination Council's manual on Bank Secrecy Act/anti-money-laundering compliance, for example, includes appropriate personnel training among its four major requirements.[1] Recent failures by financial institutions to establish or maintain an effective BSA/AML compliance program have resulted in major regulatory enforcement actions accompanied by billions of dollars in fines. These enforcement actions (and, similarly, enforcement actions for non-BSA/AML violations) often include the requirement that management improve employee compliance training. In 2015, a Federal Deposit Insurance Corp. official noted that the agency was "seeing instances of insufficient resources/training dedicated to BSA compliance."[2] Such deficiencies may relate to the

[1] "BSA/AML Compliance Program — Overview," Federal Financial Institutions Examination Council: https://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_007.htm.

[2] Federal Deposit Insurance Corp. Deputy Regional Director John Conneely, "BSA Today — Regulatory Tips, Trends, and Hot Topics," (March 3, 2015): https://www.fdic.gov/news/conferences/NY/2015-03-03-transcript.pdf.

scope of the individuals given training, the frequency of the training, and, in some cases, the content of the training itself. In January 2017, the U.K.'s Financial Conduct Authority fined a major global bank more than $200 million — the largest penalty assessed by the regulator — for inadequate AML controls, with several of the alleged violations stemming from personnel issues, including insufficient time for training.[3]

In 2016, the Consumer Financial Protection Bureau issued a compliance bulletin — on "Detecting and Preventing Consumer Harm from Production Incentives" — which included recommendations for providing comprehensive training for employees, among other topics. The CFPB noted that this training should "foster greater awareness of primary risk areas."[4]

Training is now being more formally articulated and integrated into the regulatory framework. The Financial Industry Regulatory Authority recently wrote that financial institutions could use FINRA's annual letter on regulatory and examination priorities "to help identify applicable priorities and then to define their training program requirements for the coming year, assess programs they may need to strengthen or update, and frame issues that they will address in their annual compliance conferences and other internal communications."[5] In addition, the New York State Department of Financial Services' recently finalized cybersecurity regulation became effective on March 1, 2017, and requires financial services institutions under the agency's regulatory authority to establish and maintain a cybersecurity program for consumer protection.[6] The regulation includes the requirement that covered entities must "provide cybersecurity personnel with cybersecurity updates and training sufficient to address relevant cybersecurity risks."[7]

Although the NYDFS training mandate seems both broad and reasonably achievable, it may nonetheless represent a shift for many organizations unaccustomed to compliance with explicit requirements for training. Ponemon Institute, a leading research company on privacy, data protection, and information security, published a 2016 survey on training and culture.[8] Ponemon gathered responses from professionals working in information technology, compliance, IT security, privacy, and human resources in more than a dozen industries, and found that only 45% of organizations make data protection and privacy training mandatory for all employees.[9] Training in this area will assume even greater importance for organizations processing data of individuals in the European Union under the new General Data Protection Regulation, taking effect on May 25, 2018. The GDPR requires that designated data protection officers be responsible for awareness-raising and training of staff involved in data processing, which will provide additional safeguards for data protection. Infringements of the GDPR will carry fines of up to 4% of a firm's worldwide turnover (revenue).

The potential consequences of inadequate training in data protection are easy to observe: 25% of data breaches are caused by the so-called "human factor," involving negligent employees or contractors;

3 https://www.fca.org.uk/publication/final-notices/deutsche-bank-2017.pdf

4 "CFPB Compliance Bulletin 2016-03," Consumer Financial Protection Bureau (Nov. 28, 2016): https://s3.amazonaws.com/files.consumerfinance.gov/f/documents/201611_cfpb_Production_Incentives_Bulletin.pdf.

5 "2017 Annual Regulatory and Examination Priorities Letter," Financial Industry Regulatory Authority (Jan. 4, 2017): http://www.finra.org/sites/default/files/2017-regulatory-and-examination-priorities-letter.pdf.

6 "Cybersecurity Requirements for Financial Services Companies," New York State Department of Financial Services: http://www.dfs.ny.gov/legal/regulations/adoptions/rf23-nycrr-500_cybersecurity.pdf.

7 Ibid., Page 7.

8 "Managing Insider Risk through Training & Culture," Ponemon Institute (May 2016): http://www.experian.com/assets/data-breach/white-papers/experian-2016-ponemon-insider-risk-report.pdf.

9 Ibid., Page 2.

another 27% of breaches involve system issues that include both IT and business-process failures.[10] Many of these data breaches occur as the result of hacking schemes that use social engineering and phishing. In a recent study, 30% of phishing messages were opened by the target across all campaigns, and more than 10% of recipients clicked the malicious attachment or link, enabling the attack to succeed.[11] Effective training can dramatically lower the risk to companies, however. A study on the security training at companies from nearly two dozen industries found that, after their employees completed three training exercises, only 13% of them clicked through to phishing messages, while the click-through rate fell to 0.2% for employees who went through five training sessions.[12]

The average per-record cost of a data breach resulting from human error was recently estimated to be $133,[13] which can aggregate to millions of dollars for even small to midsize data-intensive organizations. These incidents may also cost companies indirectly, through lost sales due to reputational impact and/or decreases in share price. Significant investment in an effective training program is therefore essential as a preventive measure for data security and other areas of regulatory compliance.

Challenges to Effective Training

Training in regulatory compliance poses major challenges that firms can easily overlook or underestimate. As you think about how to best deploy training at your organization, it is essential to keep in mind the pitfalls most likely to limit training effectiveness. Companies often encounter several common challenges when carrying out regulatory-compliance training:

TRAINING FATIGUE

New and stricter regulatory requirements to provide regular, comprehensive training have increased the time employees spend completing mandatory training courses. In calendar year 2015, employees at the average company received almost 54 hours of training, 13 hours more than in the previous year.[14] The average was even higher for midsize companies (67 hours) and much higher for government/military organizations (82 hours).[15]

COMPETING DEMANDS FOR TIME

The stress workers already feel when completing their day-to-day responsibilities can be exacerbated by requirements to put those activities on hold to complete training. Employees may therefore postpone or fail to meet important training obligations. The common employee frustration about a lack of time for training reflects — and arguably perpetuates — the lower priority given training vis-à-vis other responsibilities.

CONTENT IS UNINTERESTING AND DULL

Designing compliance training that holds employees' attention — and thereby helps firms avoid major regulatory lapses — is far from easy. Many existing training programs take the form of long, text-heavy courses that might make for excellent bedtime reading at home, but lead to low user engagement and poor retention of the subject matter in the workplace.

[10] "2016 Cost of a Data Breach Report," Ponemon Institute (June 2016): https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN, Page 11.
[11] "2016 Data Breach Investigations Report," Verizon (April 29, 2016): Page 18.
[12] "Enterprise Phishing Susceptibility Analysis," PhishMe (Dec. 21, 2015).
[13] "2016 Cost of a Data Breach Study: Global Analysis," Ponemon Institute: Page 2.
[14] "2015 Training Industry Report," *Training* (November 2015): https://trainingmag.com/trgmag-article/2015-training-industry-report.
[15] Ibid.

LIMITED TRAINING ACCESSIBILITY

Different workers in different industries have access to vastly different levels of connectivity. According to one industry observer's estimate, 80% of workers are "deskless" — such as salespeople out in the field and delivery drivers.[16] The most appropriate method for delivering training varies for each person. Current training options may limit accessibility (e.g., offering access only via networked office computer), which further restricts the time during which employees can complete the training.

REPETITIVE LOOK AND FEEL

Uniformity in the look, feel, and delivery method of an organization's training courses can provide a more consistent experience for the user. Yet it also increases the risk that the courses blend together in the employee's mind, making distinct topics and lessons more difficult to recall.

CONTENT DOES NOT RESONATE

There are compelling arguments to purchasing an off-the-shelf training product. Notably, the upfront cost is typically lower, and the time and effort required to make the course "ready" for employees are minimal. However, the importance of tailoring a course to the company cannot be overstated. A course that reflects your company's terminology and contains real-world scenarios faced by your employees will be far more effective at reaching your employees and effecting certain desired behaviors.

COMPANY CULTURE DOES NOT EMPHASIZE TRAINING

Employees can tell when training is not perceived as particularly important by the organization. Senior managers need to set the right tone, communicating why the training is important and attending the required sessions themselves. A company that takes training seriously holds employees accountable for completing it. An organization that fails to promote training is not just missing an opportunity, but contributing to a bad compliance culture.

Current Trends in Training Design

Many organizations recognize these challenges and are exploring potential solutions. To combat training fatigue, companies are looking for opportunities to consolidate overlapping courses — shortening total training time by, for example, combining two 45-minute courses into a single course with an expected duration of one hour. Some companies have begun distributing training more evenly throughout the year. Rather than a one-hour course completed in one sitting, the course is broken into 15-minute increments and completed once per quarter. This training schedule not only lessens the time commitment required for any one session, but keeps the training material more front-of-mind due to regular exposure throughout the year. Companies are also considering the use of mobile devices for more on-the-go training, though the training industry remains at a relatively early stage of developing and delivering mobile-compatible content.

Two other trends help address the training challenges companies face.

[16] Carol Leaman, "The Deskless Worker: The Next Big Opportunity in Corporate Learning," *Training* (Jan. 2, 2017): http://www.trainingindustry.com/e-learning/articles/the-deskless-worker-the-next-big-opportunity-in-corporate-learning.aspx.

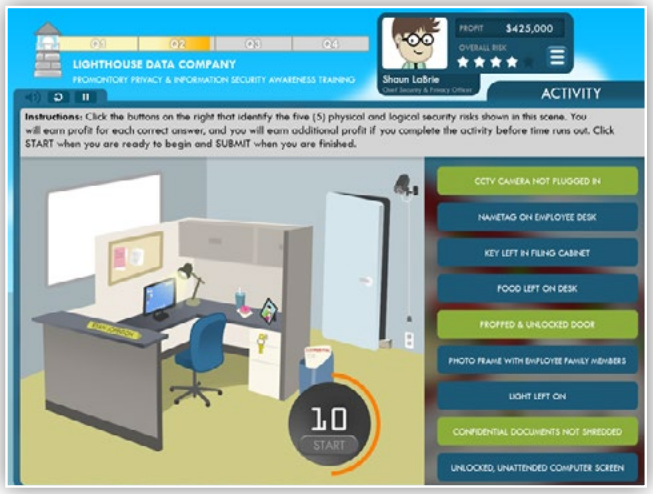
THE BENEFITS OF GAME-BASED TRAINING

A review of 65 studies and data from 6,476 trainees showed that video-game training is more effective than comparison groups.

11% HIGHER FACTUAL KNOWLEDGE LEVEL

14% HIGHER SKILL-BASED KNOWLEDGE LEVEL

9% HIGHER INFORMATION RETENTION RATE



Source: Traci Sitzmann, "A Meta-Analytic Examination of the Instructional Effectiveness of Computer-Based Simulation Games," *Personnel Psychology* (summer 2011): Pages 489-528.

GAMIFICATION

Organizations are increasingly turning to games to achieve a higher level of engagement in their training. Gamification makes "use of game theory and game mechanics in non-game contexts" — e.g., common work situations and scenarios — "to engage users in solving problems," a recent industry report said.[17] Studies show that gamification helps trainees reach higher levels of factual knowledge, skill-based knowledge, and information retention. In 2016, worldwide revenues for game-based learning products reached $2.6 billion, which is expected to grow at a compound annual rate of 22% to $7.3 billion by 2021.[18] Historically, many companies have perceived game-based learning as incompatible with their corporate culture; but this perception has changed significantly in recent years, as companies use gamification in their main training courses or for supplemental learning to enforce key messages and evaluate employees' retention of those messages.[19] Game-based training also allows companies to hold internal competitions that increase employee engagement, to celebrate professional milestones (e.g., department anniversaries), and to promote awareness of a particular subject as part of a company campaign.

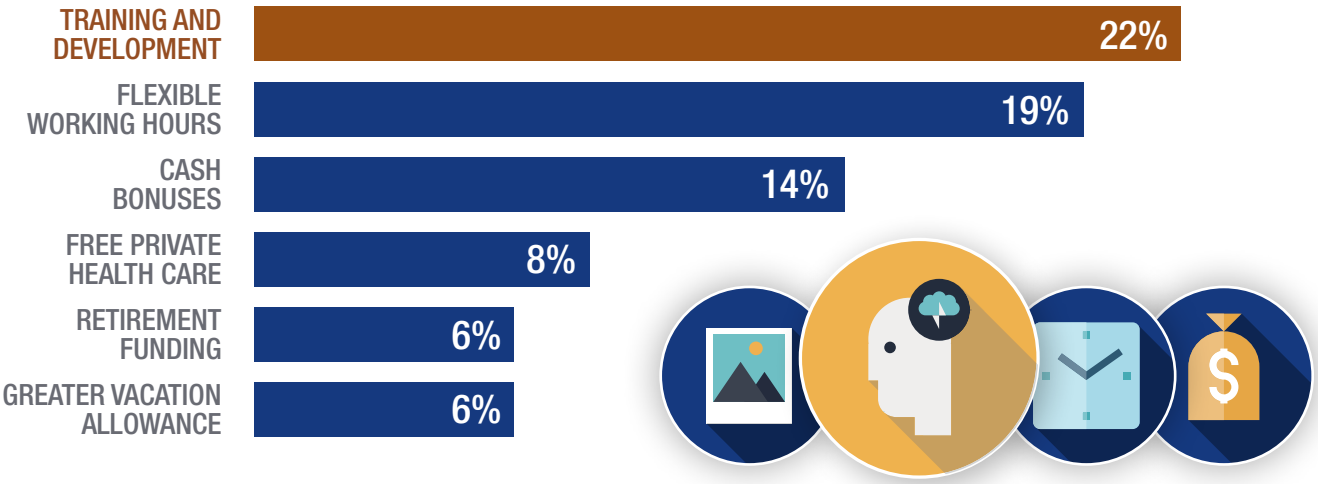
MICROLEARNING

Some organizations are pursuing so-called "microlearning," which provides training condensed into three to five minutes and designed to meet a specific outcome. Companies typically use this more informal type of learning as a supplement to primary training courses. The shorter nature of this training makes it easier to deliver via multiple channels, including mobile devices.[20] Microlearning is also an effective means of delivering just-in-time training — in which employees receive personalized information based on their job responsibilities and performance and timed for the moment when the information is needed.

[17] "Elearning Market Trends and Forecast 2017-2021," Docebo (Dec. 8, 2016): Page 35.
[18] "Key Findings from Ambient Insight's 'The 2016-2021 Global Game-based Learning Market' Report," Ambient Insight (Sept. 22, 2016): http://www.ambientinsight.com/Resources/Documents/Ambient_Insight_2016_2021_Game-based_Learning_SeriousGamesClusterHelsinki.pdf.
[19] "Elearning Market Trends and Forecast 2017-2021," Docebo: Page 35.
[20] Ibid., Page 30.

MILLENNIALS IN THE WORKFORCE

For millennials, "Training and Development" is the most coveted job benefit.



Source: "Elearning Market Trends and Forecast 2017-2021," Docebo.

A New Training Philosophy

Companies take a variety of approaches to regulatory-compliance training, but too often view training as a check-the-box exercise where the sole objectives are to provide evidence they comply with applicable regulatory requirements and/or transfer liability to the employee. Training instead provides a great opportunity to increase the knowledge and value of your employees. Many employees — especially younger employees — seek a strong sense of purpose in their employment. Having greater understanding and knowledge, and thus being able to effect greater change within an organization and for its customers, can promote employee satisfaction. As shown above, millennials view training and development as their most coveted job benefit.

Properly executed training garners positive reactions from employees, offers customers the benefits of higher-quality service and protections, and achieves a meaningful reduction in an organization's risk levels. Companies have several additional ways to maximize the impact of training.

Tying employee performance evaluations, compensation, and advancement to training completion, knowledge and skill levels, and application of training principles: The more knowledgeable employees become, the more valuable they are to their organization. The recent Ponemon survey found that only 19% of respondents say their organizations provide a financial reward for protecting sensitive information and reporting potential issues, while only 29% of respondents said their organizations included such information in performance reviews.[21]

[21] "Managing Insider Risk through Training & Culture," Ponemon Institute: Page 3.

Investing in training and education: How companies fund and talk about employee education affects employee perception of its importance and effectiveness. Training isn't cheap — companies spent an average of $702 per learner in 2015[22] — but the investment can pay long-term dividends. And internal messaging that emphasizes training as an opportunity to enhance employee knowledge, improve the services provided to customers, and increase the value of your brand can alter employee perceptions that training is a merely check-the-box activity.

Providing a combination of general and role-based training: When companies forget or neglect to provide role-based training, which presents employees with tailored examples and scenarios that they are likely to face on a day-to-day basis, the information will be less pertinent, relatable, and memorable.

Leveraging subject-matter experts and tailoring the content to your organization: Training content should be prepared by subject-matter experts and reflect a company's specific terminology, challenges, and people. The content should also reflect the latest market trends. Scenarios that mirror what employees see in media reports will resonate more. For instance, a hypothetical situation where your company is hacked by a nation-state seeking to influence the sales of your leading product may be particularly relatable. Similarly, ensuring that content reflects your policies and procedures will help yield employee behavior consistent with desired norms.

Making key takeaways clear: Given the limits of human memory, training programs must provide carefully and clearly structured content and emphasize the top three to five lessons and action items you want employees to remember, even if they forget everything else.

Tracking performance to determine training effectiveness: Companies can develop metrics and monitor operational trends to discern whether training is having the desired effect. Only 25% of organizations surveyed by Ponemon measure the success of their data protection and privacy training programs by using pre- and post-training tests to determine the amount learned and retained, and only 11% measure success by gauging the reduction in noncompliant behaviors and practices.[23]

Conclusion

Educating employees is an essential component of every compliance program. New and existing regulations will continue to stress the importance of training, and regulators expect to see an appropriate level of resource dedication when they conduct risk and compliance examinations. Investing additional time and resources in the development of a modern regulatory-compliance training program yields positive benefits for your employees and customers, while reducing your company's overall risk.

[22] "2015 Training Industry Report," *Training*.
[23] "Managing Insider Risk through Training & Culture," Ponemon Institute: Page 22.

Contact Promontory

For more information, please call or email your usual Promontory contact or:

Linda Gallagher
Managing Director and Global Head of the
Consumer Protection Practice, Washington, DC
lgallagher@promontory.com
+1 202 370 0411

James Gregoire
Senior Principal, San Francisco
jgregoire@promontory.com
+1 424 225 1015

Robert Grosvenor
Managing Director, London
rgrosvenor@promontory.com
+44 207 997 3407

Michael Spadea
Director, San Francisco
mspadea@promontory.com
+1 415 291 2671

To subscribe to Promontory's publications, please visit promontory.com/subscribe.aspx

Follow Promontory on Twitter @PromontoryFG

PROMONTORY
an IBM Company

Promontory Financial Group, an IBM Company, excels at helping clients resolve critical issues, particularly those with a regulatory dimension. Promontory professionals have unparalleled regulatory experience and insight, and provide our clients with frank, proactive advice informed by best practices and regulatory expectations. Founded in 2001 by Chief Executive Officer Eugene A. Ludwig, former U.S. comptroller of the currency, Promontory became a wholly owned subsidiary of IBM in 2016.

801 17th Street, NW, Suite 1100, Washington, DC 20006 Telephone +1 202 384 1200 Fax +1 202 783 2924 promontory.com