NAVEX GLOBAL®
The Ethics and Compliance Experts

WHITEPAPER

Top Ten Ethics & Compliance Predictions and Recommendations for 2015

By Ed Petry, Ph.D., with contributions from NAVEX Global's Advisory Services Team

Are you—and your ethics and compliance program—prepared to meet the challenges 2015 holds?

To help, we've asked industry experts, our colleagues at NAVEX Global and ethics and compliance professionals from across our more than 8,000 clients what trends they believe will have an impact on our industry in the months ahead—and share practical steps we can take to prepare.

1 Increasing pressure to maximize the ROI of ethics and compliance

In a time of tight budgets and increasing scrutiny, ethics and compliance programs are not immune from the expectation that time and resources be well spent, and that organizations will see a tangible return on investment. All indications are that pressure to maximize the ROI of ethics and compliance is increasing—and there is no reason to think the trend will change in the coming year.

Key Steps For Organizations To Take:

Ensure you have a clear and complete picture of the size of your budget. To maximize the ROI of your ethics and compliance program, the first step is to ensure that you have a clear and complete picture of the size of your current budget. This may seem obvious, but an analysis of data published over the last year indicates that many organizations actually underestimate the size of their ethics and compliance budgets and oversimplify their allocations. An independent study commissioned by NAVEX Global in 2014 found:

- Compliance officers lack adequate and accurate information about their current and historical spend. In part this is because ethics and compliance expenditures originate from an average of 2.7 departmental budgets in addition to the Compliance department budget. These departments often include: Audit and Finance, Risk Management, Training and Professional Development and Legal.
- Only 60% of organizations' ethics and compliance spending is accounted for in annual, fixed budgets—the rest is in "special budget allocations."
- When compliance professionals share incomplete budget information, one consequence is that budget trends and benchmarking among peer organizations can also be misleading.
- Our 2014 study indicates that the ethics and compliance budget story is better than most people realize. Budgets are increasing. Nearly half of the respondents to our study expect budget increases in 2015 and virtually none expect budget cuts.

Account for "non-quantified expenditures." Non-quantified expenditures are too often left out of budget calculations. One significant non-quantified spend is the hours that employees devote to training. For example, one hour of training for all employees plus the time that managers or in-house trainers spend preparing can quickly add up to thousands of hours. Another major non-quantified spend is the amount of time organizations spend tracking and analyzing regulatory changes. A recent study noted that over one-third of organizations globally spend an entire working day every week on this activity. Business leaders who are eating this time will often be the first to remind compliance officers of these hidden costs.

Assess your program's effectiveness. Of course, getting a handle on expenditures is only half of the story. To maximize ROI you also need to assess effectiveness—what is your organization's return on its ethics and compliance investment? Unfortunately, according to a 2014 survey by Deloitte, 68% of compliance officers try to measure program effectiveness but only half have a high degree of confidence in the metrics they track.

Maximize operational efficiencies. There are major efficiencies—and major ROI improvements—to be gained in a well-run ethics and compliance program. An organizational structure that enables planning and coordination across functions is critical to efficiency and success. In addition, outdated, manual, time-intensive approaches are under heightened scrutiny and no longer make sense—particularly related to policy management and third party risk management. Scalable, automated technology, combined with access to integrated data, is key to program effectiveness and an improved ROI for ethics and compliance.

Use advanced ethics and compliance measurement tools. In recent years, we have seen significant progress toward integrated ethics and compliance dashboards that can provide compliance officers with useful, robust, data on training, code acknowledgements and third-party due diligence which can in turn can enable them to be proactive in predicting risks and problem areas. And, more and more resources are being deployed in a "smarter" more integrated way.

RELATED RESOURCES:

Webinar: Proactive vs. Reactive: The Dollar Value of A Strong Ethics and Compliance Program

2 Dealing with conflicting legal requirements: guns, drugs and marriage in the USA

It may sound like a description of a new reality-based TV show, but we're actually referring to the very real issue of how you address hot-button risk areas when legal requirements are in conflict. Of course this issue is not completely new. Global companies have always needed to reconcile conflicting laws and cultural norms. But now a compliance matrix of overlapping and conflicting laws is impacting far more companies—especially in the U.S.

Consider the legalization of marijuana. Under U.S. federal law, the use, distribution and manufacturing of marijuana is illegal. But some states now permit recreational use, and many more allow medical use.

Similarly, over the past two years, there has been a sea change in the treatment of same-sex spouses under both federal and state law. Now that federal law and the laws in 35 states and the District of Columbia recognize marriage equality for same-sex spouses, employers must review and possibly change their policies and practices especially as they pertain to their leave policies and employer-provided benefits.

Gun laws also vary state to state. An increasing number of states have passed laws that limit property owners' ability to ban firearms. Under such laws, companies can ban firearms in the office or on the factory floor, but they can't always ban guns that are stored in vehicles in the parking lot. Whether these laws escalate or help prevent workplace violence has become a point of contention and sometimes mark a cultural and political divide within organizations.

Given the conflicts, employees and managers need guidance. Organizations that operate in multiple jurisdictions must balance safety risks, legal exposure and possibly do some soul searching to ask critical questions about their organization's values and culture.

Global companies facing jurisdictional conflicts most often create one, high-level, company-wide standard, usually included in their code of conduct, with a caveat that in some instances local or regional laws may take precedent. A statement is usually included in the code that places the responsibility on employees and managers to be familiar with local laws that may apply, and to ask questions when in doubt. These companies also rely on country-specific communications, policies and training to clarify expectations.

Key Steps For Organizations To Take:

- **Stay informed.** The legal landscape is changing rapidly. Make sure you fully understand the law in the jurisdictions where you operate. Enlist the help of local legal liaisons to keep you up-to-date.
- **Be clear on your organization's obligations.** For instance, are you required to follow federal law? Does your industry dictate a strict policy?
- **Take into consideration your organization's values and culture.** For instance, what is your organization's position on marijuana use (even if it is legal)? Does your corporate culture or values statement already lend itself to a position on marriage equality?
- **Don't assume that your views on these matters or the views of your close colleagues represent all of your organization's employees**. You may be surprised. When assessing employee opinion, include key stakeholders who must implement the policy and keep in mind that some employees likely will have a different point of view than yours. While this may not have an impact on policy development, it can affect culture. Some may not feel comfortable speaking up and sharing their opinions with management, but your actions may have a significant impact on their morale and behavior.
- **Develop targeted communications and training for those impacted by jurisdictional conflicts.** Often the most successful way to implement such training is to have local managers give the training—both to ensure cultural clarity and local relevance as well as to enforce that these policies are priorities of the business team, not just the ethics and compliance team.
- **Identify exceptions.** For example, should you enforce a zero-tolerance drug policy for safety reasons? What about an employee's drug use during off-work hours?
- **Update outdated policies and identify unauthorized policies.** Implement a policy management system that allows you to:
  - » Control permissions and authority levels on drafting, redlining and distributing policies.
  - » Track, report and archive policies
  - » Inspect and audit policies
  - » Mine your data to find deviations from policies
  - » Take corrective action for misconduct, including updating policies
  - » Document that these steps have been taken

RELATED RESOURCES:

Reference Guide: The Definitive Guide to Policy Management

Webinar: Emerging Workplace Behavior Risks: Legal Implications for Your Organization

Legal Brief: Does Your Company's Drug-Free Workplace Policy Pass Muster in Today's Legal Climate?

3 Culture (still) trumps compliance

The past year has added to our growing list of examples that prove the wisdom of the maxim: "Culture trumps compliance." In 2014 culture problems were cited as the root cause of ethics and compliance failures at a diverse sample of organizations including:

- **General Motors:** In the wake of recalls of 2.6 million vehicles and at least 30 deaths linked to defective switches, studies pointed to the lack of a speak-up culture and leadership that lost track of the importance of listening to employees.
- **The "Bro" or "Brogrammer" culture in high tech firms:** Whether they are in Silicon Valley, New York, Paris, New Delhi or Berlin, high tech firms continue to struggle to address allegations that the male-dominated industry too often embraces a sexist culture.
- **Sports spotlight:** The sports world seemed particularly susceptible to culture breakdowns in 2014. From conduct issues in football to basketball to investigations of corruption at the Zurich-based Fédération Internationale de Football Association (FIFA), the sports world was rocked by lapses in ethics.
- **Government and higher education institutions:** A "corrosive culture" was blamed for the failures at the U.S. Department of Veterans Affairs while a culture of silence contributed to embarrassing security breaches at the U.S. Secret Service. And now attention is focusing on the culture of several elite colleges and universities following charges of sexual assault and a failure of officials to take appropriate action.

Unfortunately the culture-related cases from 2014 are in many ways all too similar to examples we have seen in the past. But this year's case studies do call attention to two relatively new factors that we suspect will continue to be important:

- **The role of video and social media in exposing broken cultures:** The video of a football player punching his girlfriend in an elevator and its immediate circulation via social media completely changed the narrative in this case and altered the way discipline was handled. Without the viral video it is doubtful the case would have created such a public outcry, or would have had such a reputational impact on the sports' governing body.

  While social media has been with us for years, this case highlights the impact of video, made possible by the omni-presence of security and cell phone cameras. There is literally no place to hide. While a picture is worth a thousand words there is no calculation for the power of a video that goes viral. Of course viral video can also be a tool for good: consider the remarkable success in 2014 of the ALS Ice Bucket Challenge.
- **Many of the 2014 cases involved organizations and industries that have lagged behind in adopting rigorous ethics and compliance programs:** Often these industries have claimed that they are too different from others and so unique that they alone can properly address their compliance and culture challenges. These industries—including high-tech, academia and sports—will continue to be vulnerable until they catch up and more fully participate in the ethics and compliance community.

RELATED RESOURCES:

Blog Posts:

» Speak Up or Pay Up: Lessons from GM
» You've Got a Problem, Bro: Tinder, Silicon Valley and Resolution 62
» California AB 2053 Training Regulation On Abusive Conduct at Work: What You Need to Know
» Five Strategies For Addressing Social Media Risks (Without Breaking the Bank or Using Up Valuable Seat Time)

White Paper: Creating a Culture of Ethics, Integrity & Compliance: Seven Steps to Success

4 Maybe one size does fit all: Moving toward a uniform, global model for compliance

A few years ago it was common to remark on the two very different approaches to business ethics—one that was common in the U.S. and based on the eight-part compliance model promulgated by the U.S. Sentencing Guidelines for Organizations in 1991 (and the Defense Industry Initiative before that). The other approach, more common in Europe, was based on the principles of Corporate Social Responsibility (CSR). There was overlap and many organizations managed to incorporate the best elements from both camps, but there was no question that the two approaches were largely distinct.

While CSR is still an enormously important force—especially in academia, non-governmental organizations and among social investors—within corporations the compliance model is now the dominant approach and, with some variation, defines corporate ethics and compliance programs worldwide. The new ISO Compliance Management System Standard (ISO 19600) is another example of the consequences of this movement toward uniformity.

As anti-corruption programs have taken root worldwide, so too has this compliance model. One result of the spread of a uniform, global approach has been the increasing cooperation among regulatory bodies. Most notably the U.K. Serious Fraud Office (SFO) has increased its cooperation with other governments to prosecute financial crimes. Cooperation has led to greater access to evidence of wrongdoing that previously may have only been available to local authorities. Such cooperation would not have been as likely prior to the alignment of compliance models and the general acceptance of a uniform compliance philosophy. Given the underfunded status of some government regulatory authorities, and increased cross-border sharing, we should expect more such cooperation in the future.

Key Steps For Organizations To Take:

For compliance officers looking ahead to 2015, this trend means that in some respects, they now have an easier row to hoe. Senior executives no matter where they're located are much more likely to understand the details and importance of an ethics and compliance program. Also, training, communications, auditing, documentation and reporting systems can be streamlined and better coordinated.

At the same time, it would be premature to think that we are truly at the point of one uniform global model. Important differences still remain and need to be accounted for:

- Strong differences of opinion continue, especially between the U.S. and the E.U. on issues of privacy and information sharing.
- Attitudes towards whistleblowing also differ. Evidence of the remaining differences includes the U.K.'s rejection of U.S.-style "bounties" for whistleblowers. The U.K. Financial Conduct Authority (FCA) rejected the approach on the grounds that "bounties" act as an incentive for employees to bypass company sponsored reporting systems and report straight to the government. The U.S. Securities and Exchange Commission had considered the same argument and though it made some concessions, it still came down on the side of "bounties."
- And finally, even where laws and the compliance models are in sync, communications and training still must take into consideration cultural differences and norms.

RELATED RESOURCES:

Blog Posts:

» Creating a Speak-Up Culture in the E.U.: Five Key Challenges Compliance Professionals Are Tackling

» Reflecting on the E.U. Ethics & Compliance Landscape

Ebook: Bribery & Anti-Corruption Compliance in the U.K. & Europe

5 Regulatory enforcement moves down market

While ethics and compliance scandals that implicate brand name companies tend to grab the headlines, smaller organizations have always borne the brunt of regulatory enforcement. Over the years, U.S. Sentencing Commission data has consistently shown that a significant percentage of organizations sentenced under elements of the Organizational Guidelines have had fewer than 1,000 employees, and the majority have had less than 50. This has been true since the Organizational Guidelines were first promulgated in 1991.

In part, this is simply a matter of numbers: small to mid-sized organizations vastly out-number the Fortune 500. But another piece of the explanation is that small and mid-sized companies have also been more at-risk because they have lagged behind in the creation of ethics and compliance programs. The vulnerability of smaller companies was highlighted in two important cases from 2014.

Lawson vs. FMR: On March 4, 2014, the U.S. Supreme Court issued its first decision interpreting whistleblower protection under the Sarbanes-Oxley Act of 2002 (SOX). In *Lawson vs. FMR*, the Court greatly extended the scope of SOX when it ruled that the whistleblower provisions of SOX apply not just to public companies, but also to employees of private contractors and subcontractors. The ruling expanded the reach of SOX to cover an estimated six million contractors including smaller private companies, many of which may have thought they were beyond the reach of SOX.

SEC's Smith & Wesson Settlement: The second important case from 2014 focusses on one risk area in particular—bribery and anti-corruption. In July, the U.S. Securities and Exchange Commission charged Smith & Wesson Holding Corporation with violating the U.S. Foreign Corrupt Practices Act. In contrast to the multi-million dollar bribery cases the SEC and DOJ have focused on in recent years, the Smith & Wesson charges involved a few small contracts in the Middle East where the profit was barely $100,000. The eventual settlement was described by the SEC's chief of FCPA Enforcement as a "wake up call for small and medium businesses."

Key Steps For Organizations To Take:

For companies, an important take-away is that ethics and compliance programs are not just for the big guys. They too would be wise to create codes, policies, reporting case management systems and online training and awareness programs. Of course they needn't have ethics and compliance programs on the same scale or complexity as larger organizations, though they still should be designed to address identified risk areas.

Large companies also need to pay attention to these down market regulatory trends. For larger organizations this matters because it can impact their supply chain. Given the pressures placed on organizations to know and understand the risks posed by all their various—often thousands—of third parties, it's prudent for companies to consider implementing a system with standardized questions for third parties together with automated systems for processing responses, generating auditable reports and flagging third parties that require follow up attention.

In addition, in order to help their smaller business partners that may not currently have sufficient ethics and compliance programs, companies should also consider the following steps:

- Ensure you have an accurate and complete record of all your third parties.
- Assign managers within your organization with the responsibility to ensure that third parties are aware of their ethics and compliance responsibilities, enforcement trends and your expectations.
- Make your code of conduct available to business partners and third parties and consider ways that you can assist them in developing or accessing relevant training and other ethics and compliance resources.

- Some organizations host quarterly training calls for business partners and have reported excellent participation. Their experience is a good indicator that business partners are often eager for this type of information.

RELATED RESOURCES:

Blog Posts:

» Retaliation Exposure Tipping Point? Lawson vs. FMR Extends SOX Whistleblower Protections to Private Company Employees

» Does Your Company's "Inadequate Compliance Program" Violate Securities Laws? Lessons from the Smith & Wesson Settlement

6 Gender diversity—are quotas the answer?

In last year's annual report, we suggested that perhaps a corner had been turned on perceptions about gender and corporate leadership. After all, in 2013 we saw stories about newsmakers including Janet Yellin at the U.S. Federal Reserve, Christine Lagarde at the IMF, Mary Jo White at the SEC, as well as CEOs Mary Barra at GM, Meg Whitman at HP, Virginia Rometty at IBM, Patricia Woertz at ADM and Marissa Mayer at Yahoo. While these stories were not always positive, the important point was that, for the most part, the stories were about these executives' policy decisions, experience, mistakes and achievements—and not about their gender. It was a subtle change, but one we thought might indicate more positive changes to come.

Unfortunately, if changes are coming, they're coming all too slowly—despite the fact that research shows that organizations with women represented on the board and at senior management levels often yield higher results for stakeholders.

To address the disparity, a growing number of nations are creating quota systems and other measures to accelerate the number of women at the top of organizations. Norway was the first. In 2008, they introduced a 40% quota for female directors of listed companies. The penalty for non-compliance could be as severe as forcibly dissolving the company. Following Norway, Malaysia, Brazil, Belgium, Iceland, Italy, the Netherlands and Spain have also imposed gender quotas for boards and the European Commission is considering imposing quotas across the E.U. Australia, Britain and Sweden have threatened to impose quotas if firms do not appoint more female directors voluntarily.

If this approach gains more traction in 2014, look for it to spark considerable debate. Advocates for quotas argue that it may be the best way to force change and that once the numbers increase, the public and stakeholders will become more comfortable with female leaders and any stigma that still exits will dissolve more quickly. Opponents argue that quotas are anti-meritocratic and inevitably result in women leapfrogging over more qualified men resulting in a backlash against the process, suspicion of those who benefit and a culture and morale problem for all parties.

RELATED RESOURCES:

Blog Posts:

» More Progress for Gender Equity in the Boardroom: Germany Moves to Mandate a 30 Percent Quota for Women on Corporate Boards

» Doing Deals like a Girl (and the Rewards of Open Corporate Culture)

7

Crime and punishment

On the accountability and punishment front, three trends bear watching:

1. Expanded use of Deferred Prosecution Agreements
2. The prospect of jail time for executives
3. Legal exposure faced by compliance officers

Deferred Prosecution Agreements (DPAs): DPAs and Non-Prosecution Agreements (NPAs) allow prosecutors to require corporate reforms and penalties in exchange for avoiding or delaying the filing of charges if there is satisfactory completion of the requirements. As we noted in last year's review, the use of these and similar agreements has continued to be an important enforcement tool for the U.S. Department of Justice (which first used DPAs in 2000) and the SEC. And in in healthcare, the Corporate Integrity Agreement (CIA) has been a similar enforcement tool used by the Office of the Inspector General of the U.S. Department of Health and Human Services since the late 1990s.

Now it appears that DPAs will become a more common enforcement tool in the U.K. Recent legislation authorizing U.K. authorities to use DPAs has provided an important new tool for the U.K.'s SFO and other U.K. authorities. Most importantly, the Code of Practice guidance that governs the use of DPAs sets up significant incentives for companies to "self-report" potential violations of the law and to cooperate fully with the government if investigated—including future cooperation in prosecution of individuals.

DPAs can allow authorities to utilize scarce resources more efficiently by deferring prosecution instead of bringing a case and taking it through a lengthy (and expensive) trial. DPAs also can result in significant fines, which then can be used to help fund further enforcement activities. Given the potential benefits to governments, it seems only a matter of time before DPAs become a common feature of the U.K. enforcement landscape—and perhaps elsewhere.

Jail Time for Executives: With the exception of punishments imposed under repressive regimes, jail time has rarely been used as a deterrent for corporate wrongdoing. In fact in recent years the public and many commentators have been increasingly frustrated that no individuals have been sent to jail for the abuses that sparked the financial crisis. There may be signs that this is about to change.

In August, 2014, three former U.K.-based executives of a specialty chemicals company were sentenced to jail for their part in a bribery scheme. The U.K. SFO settled the criminal case against the company resulting in a relatively modest $12.7 million in fines, but went on to prosecute individual executives and senior managers. Testimony in the case showed that the bribery was a calculated business decision.

In his sentencing statement, the U.K. judge summarized the rationale for jail time: "The corruption was endemic, ingrained and institutional," and he also noted that companies are not automated machines, rather that, "decisions are made by human minds. It follows that those high up in the company should bear a heavy responsibility under the criminal law."

Time will tell whether this argument resonates with other judges and enforcement agencies outside the U.K.

Compliance Officers in the Crosshairs: Since the role was first created in the 1980s, compliance officers have always harbored some worries about personal liability. Recent regulatory actions like the following have brought this to a fuller and more open discussion:

- Total Wealth Management: In an on-going case, the chief compliance officer (CCO) along with an investment advisor, were charged with failing to disclose conflicts of interest and concealing kickbacks for investment recommendations to clients.

- GunnAllen Financial: The former CCO was fined $15,000 in 2011 for failure to set policies "reasonably designed" to protect customer financial information.
- Brown Brothers Harriman: The former global anti-money laundering compliance officer for the organization was fined $25,000 for the company's related compliance failures.

Key Steps For Organizations To Take:

When compliance officers have been held liable it has primarily been for intentional violations of the law. The simplest way to minimize escalating risk for compliance professionals is to scrupulously avoid legal wrongdoing and not assist others who are breaking the law, as well as:

- Document important decisions and formal advice that you provide.
- Be sure that policies and procedures that govern your work are in writing and have been reviewed and approved. In particular, to avoid the possibility of supervisory liability, when misconduct occurs, make sure the company documents which supervisor is responsible for handling it.
- Committees on which you serve should also document in their charters that your role is only advisory. And, have a formal charter in place that clearly addresses your position's duties and responsibilities.
- Have a board-approved, formal escalation policy and escalate when appropriate.
- Check your organization's directors and officer's liability insurance to ensure that adequate coverage extends to the compliance role.
- Don't go it alone. Share compliance responsibilities with others.

RELATED RESOURCES:

Webinar: CCOs in the Crosshairs: Addressing Escalating Risk

Blog Posts:

» Deferred Prosecution Agreements in the U.K.: The New Frontier for Employers

» Jail Time & Multi-National Cooperation in Investigations: Clues to Future Enforcement of U.K. Financial Crimes

8 Key trends from the U.S. Dodd-Frank Whistleblowing Program annual report

On November 17, the U.S. Securities and Exchange Commission issued its 2014 Annual Report to Congress on the Dodd-Frank Whistleblower Program. It is clear that the program is going strong. Following are six key takeaways and trends ethics and compliance professionals should learn from the report:

1. Last year was momentous for the Office of the Whistleblower, both in terms of the number and dollar amount of whistleblower awards. In fiscal year 2014, the Office of the Whistleblower received 3,620 whistleblower tips, a more than 20% increase in just two years. Corporate executives and boards should take note that, in the case of this particular government agency, they should not count on the wheels of government turning slowly (note the annual report was issued less than 60 days after the end of the fiscal year) nor should they assume they are dealing with "less business savvy" government personnel who they believe they can "out-lawyer."
2. Compliance officers should also take heed and ensure that they can track and measure the progress, timeliness, quality and outcomes of their internal cases. And, as the SEC does, organizations should maintain an open channel of communications with employees and consultant reporters throughout the process—even with those who are anonymous. In addition, as we found and reported in our 2014 NAVEX Global Hotline Benchmarking Report (representing data from thousands of internal hotline

reporting systems), the median numbers of days to close a case has recently jumped from 30 to 36 days, which is a red flag that delays in investigations could lead to more reports going to the government.

3. The SEC report states that, to date, more than 40% of the individuals who received awards were current or former company employees. This seems low as most expected that reports of original information which would likely qualify for an award would come from insiders with specific knowledge of wrongdoing. What is not surprising is that, of the award recipients who were current or former employees, most had raised their concerns internally to their supervisors or compliance personnel before reporting their information to the SEC. In our culture assessment work, we often hear from employees that they would much rather raise the issue internally to their manager than take it outside. And, our 2014 benchmarking data showed that 40% of all reports received by our clients internally were substantiated either all or in part. This confirms that companies generally do get the opportunity to resolve issues internally—the question is whether they will take this opportunity or miss it.

4. There isn't an employee in your organization who doesn't gauge the potential for retaliation when considering raising an issue. The Office of the Whistleblower is taking this issue head on. In 2014, the Commission brought its first anti-retaliation case. Of course addressing fears of retaliation—and training managers and supervisors on recognizing and avoiding it—should be a top priority for any compliance program whether the SEC is focused on it or not.

5. Both in recent remarks and in the report, Sean McKessy, the Chief of the Office of the Whistleblower highlighted that they have been "working to identify employee confidentiality, severance, and other kinds of agreements that may interfere with an employee's ability to report potential wrongdoing to the SEC." The report references Rule 21F-17(a) under the Exchange Act that provides that "[n]o person may take any action to impede an individual from communicating directly with the Commission staff about a possible securities law violation, including enforcing, or threatening to enforce, a confidentiality agreement…with respect to such communications." While it may only be a paragraph in the report, Mr. McKessy has said that the agency is "looking for the first big case here" and "we will continue to focus on agreements that attempt to silence employees from reporting securities violations to the Commission by threatening liability or other kinds of punishment."

6. Finally, the report offers some interesting demographics on who is reporting and their geographic locations. The report notes that during 2014, the Commission received submissions from individuals in all fifty states, as well as from individuals in 60 countries. The highest numbers of international reports are coming from the U.K., Canada, Australia, China, and India with the most coming from the U.K. (70 reports). As noted above, after a lengthy study by a commission formed by the Bank of England and the U.K. Financial Conduct Authority (FCA), the commission rejected U.S.-style "bounties" for individuals who report financial crimes to government authorities. We will see if this decision is revisited based on the U.S. Office of the Whistleblower report.

RELATED RESOURCES:

Blog Posts:

» SEC's 2014 Report on Dodd-Frank Whistleblowing Program: Key Takeaways and Trends Companies Should Expect for 2015

» Hear it From Employees First: Why Managers Should Encourage Whistleblowers

9 Technology-enabled ethics and compliance is ready for takeoff

By every indication we are about to witness a dramatic leap in technology-enabled ethics and compliance. Trends and our own client experiences are demonstrating that we are likely to see advances in each of the following areas:

Codes of Conduct: Last year we saw a significant increase in the number of organizations considering ways to better use technology to revamp how they develop, design and distribute their codes of conduct and manage associated policies. The driving force in code improvements was recognition that the code is primarily a communication and reference tool for employees. With that in mind, enhancing the ease of use, readability and access to information becomes a priority. In that light, lengthy, wordy codes that repeat what is already in policies and employee handbooks are understood to be counterproductive. And so, to enhance usability, organizations are exploring ways to create web-based versions of their codes and/or adding technology features to codes including embedded video, and links to FAQs and to more in-depth policies.

Policy Management: Even more progress is occurring on the policy management front. Policy management tools are now available to significantly streamline what is too often a manual process. Maintaining updated policies and documenting and tracking their delivery—as well as linking policy information to training and helpline data—can greatly improve ethics and compliance efficiency. This is a step that compliance officers should include on their to-do list for 2015.

Training: Along with the development, management and distribution of codes and policies, training is also undergoing a transformation added by advances in technology. Employees are sophisticated consumers of technology and they expect on-line training to meet their standards. Fortunately, new formats and short, burst learning vignettes are proving to be very effective, not only for general training but also for targeted training on specific risk topics and audiences—particularly senior executives, boards and third parties.

Third Party Risk Management: As we have noted in past annual reviews, third party risk is still the Achilles' heel for many organizations. Companies with global supply and distribution networks are especially at risk. Unfortunately, many organizations are inconsistent in their application of standards or they rely on manual processes that are time consuming, difficult to audit and lack the ability to be benchmarked for industry comparisons.

In 2015, we expect to see a continuation in the number of organizations that are automating their third party risk management process. The benefits of doing so are clear. An automated third party risk management system can:

- Help identify your universe of third-party relationships and prioritize it by risk.
- Conduct due diligence on a risk-adjusted basis and uncover and assess risks that require additional attention.
- Clarify, communicate and document mitigate steps that are required to address risks that are uncovered.
- Assist in continually monitoring and periodically re-screening third parties to flag risk-related changes that may occur, and to ensure follow through that mitigation steps are occurring.
- Provide an auditable documentation trail.

BIG DATA AND PREDICTIVE ANALYSIS

Ethics and compliance programs gather a huge amount of information from a variety of sources including: helpline and case management reports, surveys, training records, code attestations, program audits and assessments, regulatory actions, financial performance and more. This data can serve as the "canary in the coal mine," an early warning system that trouble is brewing. And further, the data can provide a diagnostic measure to help you identify where steps can be taken and how to better deploy your assets to improve your organizational culture and the effectiveness of your ethics and compliance efforts.

It's worth noting that other departments in your organizations (such as sales and marketing) are probably already using big data to understand their customers and assign resources. It won't be long before compliance officers can tap into the power of the total data available in their cross-organizational systems. But we aren't quite there yet. We tend to look at (and share) our data only at a high-level summary rather than conducting a deeper, more granular trend analysis. Therefore, we are more reactive than predictive. And, ethics and compliance faces a lot of fragmentation. Some of our most powerful data sources (HR, financial reporting and quality systems) are not yet connected to us.

Though we haven't fully pulled together all of our relevant data sources, that doesn't mean we can't do more with the data we have. And, at the same time, we can take steps toward laying the groundwork for a more robust data mining and predictive capability.

Key Steps For Organizations To Take:

- Begin integrating data from multiple departments.
  - » Consolidate helpline, open-door, mobile and web-based incident reports into a single location for secure review, investigation, resolution, reporting and analysis.
  - » Allow multiple departments to manage cases and roll up for data analytics to provide more comprehensive insights across the organization.
- Learn from your ethics and compliance training and learning management systems (LMS), including drilling down into information pertaining to specific employee populations and risk areas. The findings can help you gauge whether training is effective and whether additional targeted efforts may be needed.
- Learn from your hotline/helpline data. Look for trends and red flags related to:
  - » Types of reports/call categories
  - » Allegations versus inquiries
  - » Anonymous versus named reporters
  - » Sources and allegation types by groups, locations, businesses or services
  - » Substantiation rates, for both named and anonymous reports
  - » Discipline/remediation actions
  - » Case cycle time
  - » The number of online vs. telephone reports
  - » Follow-up contacts from anonymous calls

RELATED RESOURCES:

Reference Guides:

- » The Definitive Guide to Policy Management
- » 2014 Ethics & Compliance Online Training Benchmark Report
- » 2014 Hotline Benchmarking Report

Webinars:

- » Big Data in Compliance: Making Your E&C Data Actionable
- » Inspiring Ethical Behavior: Code of Conduct Best Practices

10 Cybersecurity: A risk that needs to be on your ethics and compliance to-do list

The starting point for every ethics and compliance program must always be an analysis of the ethics and compliance risks faced by the organization. In that light, it's important to listen to James Comey, Director, U.S. Federal Bureau of Investigation, who said at a 2014 conference: "There are two types of companies when it comes to cybersecurity. Those that have been hacked and those that do not know they've been hacked." The risk is real and it is growing every day. The "connectedness" of our digital world makes reaching across the globe a lot easier—for those with good and bad intentions.

In spite of these risks, many compliance officers still see cybersecurity as solely an IT concern. While it's true that the primary responsibility for cybersecurity is shared across departments, and that IT must provide subject matter expertise, compliance officers must have a seat at the table. Cybersecurity is both an ethics matter—we have a responsibility to protect our organization's information as well as that which is entrusted to us—and it is a compliance matter as well. Regulatory drivers including Sarbanes Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI) all require controls to prevent unauthorized access to data.

Key Steps For Organizations To Take:

- **Take a step-by-step approach to address the cybersecurity threats facing your organization.** If your organization lacks the in-house expertise to tackle cybersecurity, get help now. This is not an issue that can be left for later. If senior leadership is not convinced of the threat, marshal your in-house resource and allies and make the case. You probably do not need to look far for a peer company that has suffered a public breach, along with the reputational and financial consequences. Educate your board and employees on the risks to the organization's infrastructure and inform them of the steps you are taking and the role they must play in keeping the organization safe. Teach stakeholders about phishing emails and the importance of only visiting "safe" websites from work devices.
- **Evaluate your organization's exposure on an ongoing basis.** Make sure cyber-risks are included in your compliance and enterprise-wide risk assessments. In addition, focus immediately on high priority data and records that need to be secured. Include in your appraisal of the risk level of particular data a calculation of the reputational as well as the legal and operational hit that your organization would take if a cyber-attack occurred. At a minimum your high priority list should include customer and employee Personally Identifiable Information, as well as intellectual property—both yours and your business partners.
- **Assess the adequacy of your policies, oversight and training related to cybersecurity.** Most organizations have not kept pace with the development of new technology. The use of tablets, smartphones and social media provide additional entryways to critical organization information. Strong IT usage policies and procedures are critical to mitigating your cyber risks.
- **Ensure that you have strong alert protocols and breach response plan.** The plan is essential, but it must be practiced to be effective. Breach response time is critical to your organization's ability to recover from an attack. Your plan and processes should allow for quick scanning of your networks to determine the intrusion points. As this risk continues to garner worldwide attention, expect to hear more news on the formation of additional, designated bodies of government dedicated to addressing this risk area. As a matter of fact, as we write this we were notified that the senate approved the formation of a separate committee within the Department of Homeland Security dedicated to governing the sharing of cybersecurity information, an act that was anticipated to take place in 2015 but was expedited due to the urgency of this emerging risk area.

RELATED RESOURCES:

Webinar: Cybersecurity for Ethics and Compliance Pros: The New E&C Frontier

CONCLUSION

Organizations that focus on doing what's right reap enormous benefits—including reduced legal and business risks, higher employee morale and a strong corporate culture of ethics and respect. At NAVEX Global, we rely on the insights we gain from research and ongoing discussions with our 8,000 clients—the largest ethics and compliance community in the world—to help them do just that.

We will continue to provide thought leadership, facilitate open dialog and encourage the sharing of best practices to grow and strengthen the ethics and compliance function. Our experience tells us the best insight and the most valuable advice comes from working with clients to solve their day-to-day challenges.

In the year ahead, we encourage you to join the NAVEX Global conversation. Subscribe to our blog, *Ethics & Compliance Matters,* participate in our webinars, visit with us at conferences, join our email and newsletter lists and let us know what you see as emerging trends and challenges—and how we can help.

ABOUT THE AUTHOR

Lead Author: Ed Petry, Ph.D.

Ed Petry, Ph.D. joined NAVEX Global's Advisory Services team in 2004 after almost ten years as executive director of the Ethics and Compliance Officer Association (ECOA). Ed also previously served on the Advisory Panel to the U.S. Sentencing Commission, which was responsible for the 2004 revisions, and on the Ethics Oversight Committee for the U.S. Olympics. Earlier in his career, Ed was a tenured professor of philosophy and a prolific author and researcher. Ed's work with the ECOA and the Sentencing Commission helped establish industry best practices as well as the standards by which they are measured. In his current role, Ed applies his more than 25 years of experience to help companies assess their ethics and compliance programs. He has also written many of the most admired codes of conduct for companies worldwide and representing nearly every industry.

Contributing Authors: Shanti Atkins, founder and executive chairman of NAVEX Global, and Mary Bennett, Diane Brown, Andy Foose, Ingrid Fredeen and Carrie Penman from NAVEX Global's Advisory Services Team.

Stay up to date with the Advisory Services Team's latest insights on industry trends and best practices at Ethics & Compliance Matters, the official blog of NAVEX Global.

ABOUT NAVEX GLOBAL'S ADVISORY SERVICES TEAM

NAVEX Global's Advisory Services Team members have more combined in-house ethics and compliance experience to clients than any other advisory team in the industry. They use that expertise as they serve as the trusted business partners for ethics and compliance professionals at organizations around the world. Their proven approach helps businesses create strong cultures of ethics and respect while protecting their people, reputation and bottom lines.

ABOUT NAVEX GLOBAL

NAVEX Global helps protect your people, reputation and bottom line through a comprehensive suite of ethics and compliance software, content and services. The trusted global expert for 8,000 clients, our solutions are informed by the largest ethics and compliance community in the world.

+1 866 297 0224 INFO@NAVEXGLOBAL.COM WWW.NAVEXGLOBAL.COM