NAVEX GLOBAL®
The Ethics and Compliance Experts

WHITE PAPER

Top 10 Ethics & Compliance Predictions and Recommendations for 2017

By NAVEX Global's Advisory Services Team

Once again it's time for our annual review of trends and events that will impact your Ethics and Compliance (E&C) program in the year ahead.

This year presents a unique challenge. We are preparing our predictions before the dust has settled from the recent U.S. election. It's likely that the election will have an impact on regulatory and enforcement efforts in the coming year and beyond, but at this time it is difficult to know what the impact may be and how it will affect the work of ethics and compliance officers.

While changes are likely, many of the challenges we face are unlikely to be affected at least in the near term. For this reason we are confident in our predictions and recommendations. We've talked with industry experts, our colleagues at NAVEX Global, and ethics and compliance professionals from our more than 12,500 client organizations and based on their input, we've selected the Top 10 Predictions and Recommendations for 2017.

1) DELIVERING A RETURN ON COMPLIANCE (ROC)

How do you prove a negative? How can you estimate the value to your organization of misbehavior that was prevented, or the value of compliance failures that, because of your efforts, didn't happen? That is the thorny question Legal, Compliance and other non-revenue business units have grappled with for years. In spite of this difficulty, we nevertheless push for resources to create or improve our E&C programs in accordance with guidance such as the U.S. Federal Sentencing Guidelines for Organizations (FSGO) and others. In return, leadership quite understandably wants to know what they are getting for their money. This is especially true as E&C departments have grown and matured over the years – along with their costs.

To make matters more difficult, other business units have become adept at modeling return on investment: "If we spend X on marketing, we improve sales by Y." To level the predictive and resource playing field, ethics and compliance officers must demonstrate that what we are doing is effective, and delivers business value.

The first step is to reach agreement on what constitutes ROC. Examples of ROC may include legal and regulatory expenditures that are avoided or reduced; employee satisfaction and retention; and improved organizational culture in areas such as fear of retaliation and cynicism, which can in turn improve productivity.

While these examples of ROC are difficult to quantify, fortunately, as compliance has matured as a profession it has also become more data driven. This data can assist in helping to make the case that resources spent on compliance can yield solid, discernible returns.

Data indicates one program investment that correlates very well with delivering ROC is automation (see Trend #3). In the 2016 NAVEX Global Benchmark Report on Third Party Risk Management, 32 percent of respondents reported that in the last three years they faced a legal or regulatory action involving third parties. Seventeen percent of organizations faced 5-10 actions with almost 33 percent of those respondents placing the costs of each action at $10,000-$99,000. Now, with the right benchmarking data, we can start to see ROC taking shape.

Furthermore, many respondents who utilized an automated third-party due diligence system indicated that legal and regulatory actions decreased significantly. Similarly, when asked to rate their third-party risk management programs on 10 "effectiveness" elements, those programs using automated third-party systems rated all 10 elements higher than those not using automation. Some elements were rated more than 100 percent better, including "Overall Program" and "Accurately Scoring Third-Party Risk."

This same correlation is also present in NAVEX Global's 2016 Policy Management Benchmark Report. Programs using dedicated, automated policy management systems reported greater satisfaction than those not using automation or software.

As this data indicates, in the year ahead, a commitment to automating elements of your ethics and compliance program may be the best investment you can make to deliver ROC.

KEY STEPS FOR ORGANIZATIONS TO TAKE:

- **Benchmark and Measure**
  The important thing is to find benchmarks or develop key performance indicators (KPIs) which are meaningful to your organization based on its risks, industry, geography or other factors.
- **Solicit Input**
  When defining ROC, solicit input and feedback from your organization's leadership about what is critical for them and how your benchmarks and KPIs relate to the overall strategic goals of the organization.
- **Measure and Assess**
  After identifying the benchmarks or KPIs, track and report on the impact of changes to FTEs or expenditures on program elements or other KPIs. Remember, this is not a one-way street. Some data may suggest value in reducing or reallocating expenditures from one risk area to another.

2) THRIVING IN A FIVE GENERATION WORKPLACE

An unprecedented change is happening in our workplaces. In many organizations, up to five generations are currently working together creating a situation that is both full of opportunities and challenges for E&C.

The changing demographics may be surprising:

- The Silent Generation (born 1900-1945) currently makes up only about 3 percent[1] of the global work force.
- Millennials (1981-2000) are now the most prevalent generation in the workplace (25 percent), surpassing the number of Baby Boomers (1946-1964) in 2014, and Generation X (1965-1980) in 2015.
- Millennials are on track to comprise 50 percent of the workforce worldwide by 2020.[2,3]
- "Nexters" or Generation Z (born after 2000) comprised another 3 percent of the global workforce, but they make up more of the global population (25 percent) than any other generation.[4] By 2020, they will be out of school, making up 20 percent of the global workforce[5] right behind Millennials.

In sum, the two youngest generations together will comprise nearly 70 percent of global employees within the next four years, while the older three generations will still be in the workplace. For a successful work environment, it is important for generations to understand each other and work well together, but perhaps more to the point, this is a rare opportunity to build a dynamic multi-generational workforce.

Many ethics and compliance officers report that while they can certainly identify broad differences between generations, what is most striking is the blending and mixing of generational attitudes and beliefs. Some employees, who according to their age may be categorized as the Silent Generation, nevertheless use information technologies in ways more similar to Millennials. And some Nexters have work habits and worldviews that are similar to Baby Boomers.

This blending of traits and habits underscores the importance of identifying where there are alignments and positive engagement among generations and how the interplay between generations can create a dynamic, thriving culture. At the same time, prudent ethics and compliance officers must also be on the lookout for points of tension that can create ethics and compliance problems or risk areas.

While some of the most critical insights emerge from an examination of how generations are blending and merging, it is important to clarify how – in general terms – generations differ. With that in mind, the following is a summary of common generational differences as identified by various researchers on the topic:

The Silent Generation is often identified by the importance they place on duty and loyalty. They are the last generation to likely spend an entire career at one company. They are inclined to follow the rules, but their experience encourages them to sometimes overestimate their abilities to handle whatever comes their way. Their embrace of self-reliance and pragmatism means they are the least likely to report issues to management or to the helpline. Many may struggle with technology, but they are the most engaged generation and want opportunities to develop and learn. They like teamwork. They also expect their experience to be respected.

Baby Boomers often see their self-worth tied to career and consequently are seen by others as "workaholics" who are driven by material acquisitions, titles and personal success. Their optimistic outlook and youth orientation – which remains unshaken even as they age – have helped many of them embrace the latest technology, though direct person-to-person communication is still their preference. Like the Silent Generation, they are also team-oriented.

Generation X'ers include many of the first "latchkey kids." The popular image of Gen X'ers is a product of change and unrest in their families and the broader society. This often contributes to their independence and self-direction, while at the same time resulting in skepticism toward authority. They tend to be adaptable, focused on results and motivated by a need for security. Their self-sufficiency causes them to ask for feedback only when they need it, and they would rather work alone. They are very technologically literate.

Millennials are the first generation to grow up using the internet and information technology from a very young age. They are typically confident (and sometimes over confident) due to highly involved, affirming parents. In the U.S. and affluent nations, their early lives were overscheduled making them comfortable with multitasking. Millennials expect lots of feedback and rewards in the workplace and are considered to be idealistic. They work to live, not live to work. Work/life balance is more important to them than salary and they want to do work that improves society, putting emphasis on corporate social responsibility, sustainability and diversity. They crave more frequent learning and advancement opportunities. They are technology experts.

Nexters are digital natives and, though time will tell, at this early stage they seem to have shorter attention spans and limited interpersonal skills. As a group they are creative – especially with respect to application of technology – and open-minded with a desire for opportunities to use their many skills. Like Millennials, they expect feedback and rewards and they are not principally motivated by money but by a flexible lifestyle. Also like Millennials, they have strong commitments to social responsibility. Though immersed in technology, they prefer face-to-face communications. They enjoy working in structured, small teams.

KEY STEPS FOR ORGANIZATIONS TO TAKE:

» **Focus on Strengths and Generational Overlaps Instead of Differences**
Understand the skills, knowledge and other benefits offered by the different generations in your workplace and leverage them. Look for ways to combine the strengths of each generation to develop stronger teams. For example:

- The Silent Generation may need and want help with technology from Nexters. Millennials can learn about detail-orientation and efficiency from Boomers. Mix up the generations on teams to cross pollinate valuable skills.
- Create mentor relationships. The two younger generations expect lots of feedback and opportunities to grow. Connecting these workers with mentors from the older generations can increase engagement and retention of employees in all groups.

» **Don’t Fall into the Trap of Age Bias when Awarding Growth Opportunities**
In a 2015 study[6], many managers said workers over 50 years old are less interested than younger workers in learning and advancing themselves. However, those older workers ranked themselves more eager to learn and develop than any other generation. Use these five steps to better understand employees across generations:

1. **Find out What They Need**
The generations have different expectations for feedback and different motivators for engagement and retention. Understand these differences and address them in developing E&C training and ongoing communications.

2. **Find Common Ground**
Mission and making a difference is important for four of the five generations. These are also good motivators for doing the right thing. Use them to focus on common goals and drive home the importance of ethical conduct within the broader framework of societal good.

3. **Adapt E&C Programs to Workforce**
With the increasing numbers of tech-savvy employees, add more digital solutions to your program. Increase automation for policies, training, communications, reporting, case management and third-party due diligence. Implement mobile solutions where it makes sense to meet employee needs for flexibility.

4. **Broaden the Scope of E&C**
Millennials and Nexters are likely to view business ethics in terms of corporate social responsibility, human rights and environmental sustainability. If your ethics and compliance program is too narrowly focused, you may see an increasing disconnect between your efforts and their expectations.

5. **Reach out to Your Marketing Department for Help with “Big Data”**
It’s likely that your organization’s marketing and advertising professionals have been leading the way in crunching “big data” and analyzing generational traits. Use this resource to better understand your employees with an eye toward identifying emerging ethics and compliance risks and opportunities.

3) PUTTING THE "E" IN ETHICS AND COMPLIANCE

Developments in information technology are creating more and more opportunities for the automation of E&C programs. Automation and integration can benefit programs in many ways, including increasing effectiveness, efficiency and consistency. We've seen this trend begin to develop over the last few years, and we believe this is the year in which building an 'e' program should be a priority for every organization.

There are four key areas of E&C programs where we believe automation will make the biggest difference: Incident Management, Training, Policy Management and Code of Conduct.

KEY STEPS FOR ORGANIZATIONS TO TAKE:

» **Incident Management:** The Helpline in most cases is the central element of a successful E&C program, it allows for all employees to have a safe and protected voice. Each organization has a responsibility to respond to reports of wrongdoing in a clear and consistent manner. Without one central incident management system designed specifically to manage and analyze reported issues, this can be nearly impossible. The days of Excel workbooks and clumsy tracking tools are over – a modern E&C program needs a tool capable of advanced reporting, consistent process and defined workflow. These elements can help organizations become more aware of potential trends, improve their investigation efficiencies and also create a consistent workflow which allows for predictable and repeatable investigation timelines.

» **Training:** For most organizations, it's already likely that a significant component of their training is delivered via electronic means, but with a diverse workforce (see Trend #2) it is important that organizations continue to update how training is delivered. Short-form learning vignettes can be used to refresh on specific topics, or address a localized problem. Since short-form learnings are quick and direct, they are also quite effective at training executives and boards of directors. Additionally, administering training from a learning management system will aid in confirming attestation, allow for employees to take the training from multiple devices and help in creating an auditable documentation trail.

» **Policy Management:** Policy Management may strike fear in the hearts of those who have had to maintain policies by hand. Fortunately, automating your policy management process gives you the ability to write, update, distribute and garner attestations all within one platform. This allows for organizations to automate their workflow related to policy management from legal review to employee attestations. A well-designed policy management tool will allow for organizations to be audit-ready. This includes easily mapping E&C policies to the relevant standards, allowing auditors to quickly find what they are looking for.

» **Code of Conduct:** In simple terms, the Code of Conduct is the face of the E&C program. It is the central guiding document for all employees, and is that to which the public and third parties will hold you accountable. Since the Code of Conduct is so vital to the success of E&C programs, transforming the document into an interactive format will improve the readability and understanding of the content. A few ways to help improve your Code are:

- Update the design to include compelling graphics and ensure it is aligned to the organization's brand guidelines
- Include navigation tools and icons within the document
- Embed Videos and short-form trainings
- Incorporate internal policy links so that employees may learn more if they desire
- Establish a unified format displayable on multiple device types

4) SORTING THROUGH THE ALPHABET SOUP OF GLOBAL STANDARDS

The publication of new anti-bribery and corruption compliance program guidance, ISO 37001 (The International Standards Organization's Anti-bribery management systems – Requirements with guidance for use), in October, 2016 is a reminder that the list of what is "required" of an effective E&C program is not yet settled. Professionals and scholars working in this field continue to produce new guidelines and tweak existing ones. The regulatory alphabet soup is a heavy burden for ethics and compliance professionals and their organizations and the coming year shows no signs that the burden will be lessened.

In addition to the most widely known guidelines, such as FSGO (the U.S. Sentencing Commission's Federal Sentencing Guidelines for Organizations), ISO 19600 (The International Standards Organization's Compliance Management Systems – Guidelines), the COSO Framework (The Committee of Sponsoring Organizations of the Treadway Commission's Internal Control – Integrated Framework), and OECD, (The Organisation for Economic Co-operation and Development's Good Practice Guidance on Internal Controls, Ethics and Compliance) there are also numerous other guidelines focused on specific risk areas such as privacy or anti-bribery and corruption, for example the FCPA (U.S. Foreign Corrupt Practices Act Guidelines 2012), and the U.K. Bribery Act.

If this wasn't complicated enough, there are also industry specific guidelines including: The Payment Card Industry Data Security Standard (PCI DSS), Compliance Guidance of the Office of Inspector General (OIG) of the U.S. Department of Health and Human Services (HHS), and the U.S. Federal Acquisition Regulation (FAR). We lack the space to even begin to cite the relevant compliance requirements for banking, insurance, energy and financial industry organizations.

If your organization has global reach, there may be another level of complexity to consider and your program must deal with the plethora of country specific guidance as well as varying cultural considerations. The list is extensive and goes well beyond provisions of ISO and the OECD including, for example the Russian Federal Act on Data Protection, and a dizzying number of data protection regulations from the European Union, Argentina, Canada, Costa Rica, Hong Kong, India, Israel, Japan, Malaysia, Mexico, Peru, South Korea, Taiwan and Uruguay.

To add an additional layer of difficulty when deciding what guidance applies, there are some instances when standards conflict (e.g., in the U.S., state requirements differ with U.S. federal requirements pertaining to guns, drugs and marriage – see 2016 Top 10)

The good news is that this alphabet soup of guidelines is broadly consistent and addresses virtually the same E&C program elements: Written Standards; Oversight; Training and Communication; Remediation; Monitoring; Risk; and Culture. So an effective program under one guideline will likely pass muster under the others.

The bad news is that it is now well understood by regulators that "one size doesn't fit all," so to meet the various requirements, every organizations' program must be tailored for each unique organization, its resources, risks and other factors which can change over time.

How do we wade through all of this?

KEY STEPS FOR ORGANIZATIONS TO TAKE:

» **Assess and Document**

- Conduct a documented E&C program assessment and document current program strengths and gaps.
- Conduct a documented E&C program risk assessment to identify high-risk areas and implement short-and long-term mitigation steps and strategic goals.
- Review client contract and industry requirements regarding E&C program expectations for programs to be designated "effective."
- Collect all E&C program documentation in a way that is easy to archive and access, such as utilizing a policy management system that can handle many types of documents beyond policies.

» **Utilize Best Practices**

Follow developments in new standards or guidance and consider utilizing best practices such as program automation.

5) BEING MORE THAN JUST THE PEOPLE WHO SAY 'NO'

As part of our culture assessments, NAVEX Global's Advisory Services team has led more than 1,300 in-person focus groups with employees at all levels, in many countries and from every industry. We've heard candid comments about what employees really think about their organization's E&C program, and the personnel who run it.

Unfortunately, in many organizations, the E&C department is viewed as "the people who say no." By this, employees mean that E&C is viewed as enforcers of rules or "policy wonks." E&C is seen as not aligned with the organization's business goals but instead as a "necessary evil" or "CYA" function.

Rebranding your office as a positive contributor to the business and a key part of the management team may be a long-term goal, but moving in that direction will pay immediate dividends.

KEY STEPS FOR ORGANIZATIONS TO TAKE:

» **Examine the Root Cause of Employee Opinions**

If your E&C department is viewed as the "people who say no," (and it probably is) your first step should be to determine the specific causes of this attitude. In many cases, the damage is self-inflicted and can be quickly corrected. Focus groups, interviews or informal discussions are all good ways to get to the bottom of the matter, and these steps themselves may help signal that your office is trying to change.

Some organizations have found that the root cause of the problem are what employees see as onerous or irrelevant requests from your office including overly complicated annual certification, complex and impractical gift registries or conflict disclosure processes; lengthy training that seems repetitive or not targeted to their actual responsibilities; and perhaps most often, lack of accessibility. In too many cases E&C officers are viewed as removed or impersonal. The consequence is that the E&C office becomes wholly defined by its emails and policies, which can contribute to the negative image. Remember that at its roots, ethics and corporate culture are personal and interpersonal matters. For this reason, direct access and "face time" can go a long way toward improving your brand.

» **Be Transparent and Respect Employees' Time**
From an employee's point of view, E&C requirements that seem irrelevant or consume an inordinate amount of time are seen as clear evidence that the E&C office doesn't "get it," which fuels the conclusion that E&C is marginal to the business and not aligned with business imperatives. In the coming year, if you do nothing else to address your E&C brand, vow to be more respectful of employees' valuable time, and be sure to include explanations of why the training or other E&C asks are needed. Develop a multiyear E&C communications and training plan that will ensure its relevancy and help you target your training and communications to specific roles and responsibilities. And remember: short and simple is always best.

» **Reposition the E&C Office as a Strategic Management Ally**
Meet with key managers and ask them how your office can help them meet their goals and solicit their suggestions on ways to collaborate and improve efficiency and effectiveness. Focus discussions on risk identification and management strategy. Talk less about the byzantine U.S. Sentencing Guidelines and other arcane requirements and more about operational effectiveness. Be practical, helpful and engaged. Act more like a strategic partner and less like a "compliance cop."

» **Don't Neglect Your Third Parties**
Risk identification and mitigation efforts should also include outreach to third parties. Positioning your office as a resource for third parties will not only change how you're perceived, but it can also go a long way toward improving supply chain compliance.

6) MEETING SOCIETY'S EXPECTATIONS FOR SOCIAL RESPONSIBILITY

As noted above in our second trend, "Thriving in a Five Generation Workplace," younger employees along with the public and media continue to apply pressure on organizations to address Corporate Social Responsibility (CSR) issues including human rights and environmental sustainability. For many consumers, a robust and transparent CSR program is a necessary condition before they are willing to buy.

How best to address society's expectations for social responsibility has become a challenge. How do you address these issues in meaningful ways and avoid accusations of "green washing"?

For many organizations, the approach has been to support philanthropy or community engagement, donating a portion of profits, offering employee volunteer time, pledging to provide certain products or services free of charge. For other organizations, the approach can be best described as CSR compliance – certifying supply chain behavior, meeting third-party standards for board diversity or conducting social audits.

A third approach is also beginning to gain momentum. This approach focuses on more strategic CSR programs that engage in activities that serve both the business and the community. More and more companies are finding ways to help their communities while simultaneously providing more value to employees, customers and improving operations. Here at NAVEX Global, our Outreach Program allows team members throughout the organization to develop and implement community outreach events. These projects both improve the communities in which we work as well as provide invaluable inter-personal and project management experience to the future leaders of the organization.

Examples of initiatives from other organizations of how to serve both the business and the community include:

Working with third parties to ensure they provide safe working environments and fair wages. By helping suppliers improve conditions for workers, CSR programs can limit the possibility that an organization's supply chain will run afoul of labor laws or be subjected to negative media attention.

Creating more environmentally-friendly industrial processes. By investing in environmentally-friendly innovation, CSR programs can help replace costly, polluting processes with cheaper, cleaner alternatives. This ensures the organization is protected from current and future regulations and can help reduce health risks for employees that may lead to litigation.

KEY STEPS FOR ORGANIZATIONS TO TAKE:

- » **Identify and understand your organization's social responsibility image and what shapes it.**
  On a regular basis, gather and assess information about the impact of your organization's actions or lack of action from news reports, CEO statements, employee perceptions, customer experiences, social media, activists and other organizations in your industry.
- » **Reposition E&C as a broader social good.**
  Employees are rarely motivated by the call to "be compliant," however, they will respond more positively if they can see that their actions are advancing a broader, societal benefit. Most compliance efforts can be repositioned within the broader context of "values" and social good work – which are often more meaningful and motivational frameworks than strict compliance. For example, abiding by anti-corruption requirements in order to ensure ABC compliance is less motivating to employees than demonstrating the deleterious effect that corruption has on the lives of people in emerging economies and articulating the role they can play in eliminating corruption and its effects.

These, and similar efforts, also resonate well with employees who see it as a sign that the organization truly means what it says in its Code of Conduct and policies. Although many organizations are beginning to see the benefits of this new approach, only a few have fully capitalized on this change in the CSR space. We expect to see more examples in the coming year.

7) LATEST TRENDS IN HELPLINES AND WHISTLEBLOWING PROTECTION

Every year it's safe to assume that our list of Top 10 trends will include the latest developments pertaining to helplines, whistleblowers and retaliation, and this year is no exception. We begin by examining some hard data on the topics.

The NAVEX Global annual benchmarking reports review a variety of key metrics related to helpline reports, processes and outcomes. The data, along with our discussions with our clients and colleagues, help highlight several key trends that all ethics and compliance professionals should be aware of in the coming year.

1. **Case Closure Time Is Up**
   Over the last five years, the time it takes organizations to close a case has risen to risky levels – a median of 46 days in 2015 up from 32 days in 2011. Reasons given for the delays include insufficient resources and complexity of cases in the current regulatory environment. This may make perfect sense for Chief Compliance Officers, but for the employee who has raised a concern and is waiting for a response, every day can feel like an eternity and an opportunity for retaliation. Our data also shows that less than 1 percent of all reports in our database (of over 867,000 reports) are claims of retaliation. This suggests that employees who believe they have experienced retaliation are not reporting this back internally or that actual retaliation happens at a much lower rate than feared.
2. **E&C Groups Cannot Abdicate Responsibility**
   While the E&C office is not always the team that conducts the actual investigation, it is critically important to ensure that all issues raised through our helplines are properly investigated and that appropriate action is taken in a timely way. We see too many organizations use their reporting system as a clearing house to farm out reports to other organizations for action and then immediately close the case with no visibility into actions, timing or outcomes. If we abdicate responsibility with no follow-up, it is our credibility on the line and the potential for bad outcomes goes up.

3. **Managers Are First Line of Reporting and Need Training**
   E&C officers have long known that most employee concerns about misconduct don't come through the helpline. In most cases, employees bring their issues directly to their managers. When managers turn a deaf ear to those complaints, it is because they either don't know what to do with a complaint or don't want to take the necessary steps to address the concern. We, as business leaders, have an obligation to assist managers with this important responsibility. We need to provide them with training on how to respond and tools for them (and us) to enter and track issues they receive to an appropriate resolution and closure.
4. **Policies and Processes Deserve more Attention**
   The stakes a very high for getting this part of a whistleblower program wrong. Failures at this level telegraphs to employees, regulators, investors, customers and the public that your culture is wrong. That, in turn, can lead to steeper regulatory fines, loss of reputation, loss of good employees and even loss of business.
5. **Whistleblowing and Retaliation Needs to Be on the Board Agenda**
   The current regulatory focus, especially in the U.S., by numerous agencies on whistleblower reporting, incident management and retaliation is unprecedented. If this hasn't been a topic of discussion with your board and C-suite yet, it needs to become a priority.

An additional issue to consider is how investigation protocol may need to be changed due to recent published guidance from the U.S. Department of Justice (DOJ). This guidance is commonly referred to as the "Yates Memo."[7] The Yates Memo is the latest in a line of guidance which seeks to turn up the heat on culpable individuals in organizations being investigated for criminal or civil wrongdoing. It remains to be seen what the long-term impact will be, so it is necessary to read and address the plain language of the memo which requires organizations seeking cooperation credit from the DOJ to fully investigate individuals and share "all relevant facts" of the investigation. Cooperation credit is "all or nothing."

While the Yates Memo may focus on individual culpability, senior executives and in-house counsel must also be mindful of how organizations conducting "post-Yates" investigations can claim and utilize the attorney-client privilege in an era where the DOJ requires "all information." How does the organization maintain the privilege while disclosing sufficient information expected by the DOJ?

KEY STEPS FOR ORGANIZATIONS TO TAKE:

- First and foremost, accept that internal reporting is a good thing; that the majority of reporters do so with good intentions; and take all reports received seriously and investigate without bias. Treat your employees as reporters, not as whistleblowers or "snitches."
- Establish strong and consistent investigation and discipline processes and policies.
- Train investigators on proper techniques and required reporting. Evaluate legal involvement and sign-offs to protect organizations and individuals post-Yates.
- Train on retaliation at all levels of the organization including the front line, and test and assess the organizational culture and employee beliefs around speaking-up and fear of retaliation.
- Manage or oversee all reports to closure. Don't abdicate responsibility for reports by forwarding them to another department and closing the report without further review.

8) COMPLIANCE ROLE IN MITIGATING CYBER MAYHEM

In recent years, attention has been drawn to the impact of cyber and data breaches and the extent to which our organizations remain vulnerable to these threats. The cost of cyber and data security breaches is well known and most organizations are taking steps to address the problems. But while much is being done, too often E&C officers have remained on the sidelines wrongly assuming that cyber security is not their concern. While E&C departments may not be the appropriate lead function to address these risks, it is a serious mistake for E&C to be uninvolved. E&C can and should play a key supporting role in identifying and mitigating cyber and data-related risks.

One obstacle to more involvement is the assumption that these risks are technology problems and therefore are best mitigated by technology solutions. But the data clearly shows that human error is still the leading cause of cyber security breaches. For example, recent research "revealed that 69 percent of companies reporting serious data leaks reported that their data security breaches were the result of either malicious employee activities or non-malicious employee error."[8] The biggest cause of breaches was non-malicious employee error (39 percent). Interestingly, only 16 percent were due to hackers or external invasion.

In spite of this evidence, many organizations are missing this root cause and are focusing exclusively on infrastructure instead of making an investment in employee education and training, but here is where E&C can play a pivotal role.

KEY STEPS FOR ORGANIZATIONS TO TAKE:

» **Have Clear and Easy-to-read Cyber Standards**
Be sure your organization has up-to-date cyber security policies and that the topic is adequately covered in your Code of Conduct. But equally important, make sure the policy and the Code are understandable to employees. E&C officers have done well in recent years developing policies and codes that avoid legalese. In a similar manner, E&C officers need to ensure that their cyber standards are also free of tech-speak and are clear and easily understood by all.

» **Include Cyber Security in Your E&C Training**
Like all training, cyber and data security training should be targeted and tailored to the roles and responsibilities of employees – one size does not fit all. As an E&C officer, apply what you know and the work you've already done in developing your E&C training schedule to determine the best and most effective way to deliver cyber and data training so that it will be accepted and effective across your employee population. Information about cyber security can also be woven into case studies within existing E&C training.

» **Leverage Your Helpline**
If you are not already doing so, be sure to add cyber security and data breaches as examples of the type of issues that ought to be raised using your reporting system and Helpline. When you do so, make sure that appropriate escalation and resolution protocols are in place when technical questions are raised or threats are reported.

» **Avoid Turf Battles**
Remember that if you want a seat at the table when cyber security is discussed, you may need to give up valuable space or time that is currently devoted to more central E&C issues. This may include giving up time that is currently set aside for E&C training on other topics, or sacrificing space for posters and awareness campaigns on billboards in common areas, as well as virtual space on websites and the intranet. It may also include allowing cyber-related questions to be included in employee surveys in place of other E&C questions.

9) ETHICS AND COMPLIANCE CRISIS MANAGEMENT PLANS

When a major E&C mishap occurs, the consequences can be severe and long lasting. Beyond the penalties and related costs, reputation and brand value can take a hit, investors and customers can revolt and employees are too often left disheartened about the organization they work for. After an E&C failure, an organization must get to the costly and time-consuming task of developing a response, uncovering the root causes, rebuilding trust, restoring confidence in their brand and overhauling their culture and work environment to fix the damage.

Unfortunately, meeting such a challenge is complicated by a 24/7 news cycle and social media where initial reports can be uncontrolled, inaccurate and shaped by influencers outside the organization. All organizations today should be keenly aware of the fact that they too are one step away from a compliance failure from which it can take months or longer to recover.

For organizations that have experienced the stress of a reputational hit, one thing is clear – they could have all benefited from having an E&C crisis management plan in place. In many areas of our businesses, we carefully plan for the worst-case scenario; we bring in stakeholders and experts to help identify the risk and develop a detailed and coordinated response plan. Everyone knows who will take charge of the situation, what their role is and how to funnel inquiries and questions to the right person in their organization. When an incident occurs (whether it is a major safety incident, a security issue or even a product failure) the team is quick to action and the organization operates as one in developing a full and effective coordinated response. Such management plans are unfortunately less common with respect to E&C crises.

KEY STEPS FOR ORGANIZATIONS TO TAKE:

» **Create a List of Problem Areas**
Utilize your E&C risk assessment process to identify problem areas that are both most likely to occur, and those that would have the most significant impact on your organization if they were to occur.

» **Include Third Parties**
Ensure that your analysis of E&C risks includes your business relationship with third parties, regardless of their function.

» **Plan from Experience**
Gather together key stakeholders in your organization who have participated in crisis planning to identify best practices. Security and communications are two groups that immediately come to mind and have often done this kind of planning work in the past. If your organization has a sophisticated crisis management process in place, ensure that the E&C function is an active participant and contributor to the plan.

» **Build Your Team**
Establish an E&C crisis response team, and identify the roles and responsibilities of each member of the team. Ensure that each member can be quickly contacted in the event of a crisis.

With the team do the following:

- Identify and define the incidents that must be elevated to the team.
- Establish a simple and direct reporting protocol.
- Develop an incident response plan (or a governing document) that takes into consideration both internal and external communication needs, and identifies to whom the team will report.
- Determine who will be called upon as both internal and external subject matter experts if an incident arises.
- Develop tools and tips for managers so they understand what they can say to employees and where to direct all external inquiries (such as calls from media, enforcement agencies, citizen groups, etc.)

- Ensure that the team remains involved and a central point of information during the crisis and remediation process.
- Develop a process for post-incident debriefs to learn from the incident and your organization's response.
- Periodically review and discuss E&C failures in the news, and use them to do scenario testing. Identify ways to prepare for such incidents and improve your own E&C crisis management plan.

» Prepare formalized materials and make sure they are accessible. Post them where managers can access them and communicate to and train managers about what is expected of them.

10) COMPLIANCE OFFICER LIABILITY

Amid the burgeoning number of global regulations and increasing concern about the rising tide of regulatory scrutiny, CCOs increasingly fear being caught in the crosshairs of regulatory agencies.

While there has always been some unease among CCOs about their personal liability, the issue seems to be heating up despite the fact that only a handful of cases have been brought against CCOs and were mostly in the financial services industry. Nevertheless, recent data suggest CCOs are worried about liability:

» The U.S. Securities and Exchange Commission (SEC) released guidance in 2013 about CCO and CLO liability when they are considered to be acting as "supervisors" and fail to "supervise" the individuals that commit violations.

» When CCOs were polled by Thomson Reuters at a summit in 2015, 93 percent said they expected their personal liability to increase in the next year (64 percent expected the increase to be significant). In addition, Thomson Reuters' customers ranked the liability of CCOs higher than that of CEOs.

» A 2016 DLA Piper survey found that CCOs in private organizations were much more concerned about liability (89 percent) than their peers in public companies (74 percent).

» In 2016, insurance broker Marsh released a new, targeted product that augments directors' and officers' insurance to cover a CCO accused of unintentional conduct that led to an organization's regulatory violation. There are some behaviors that can create risk for compliance officers. These include:

- Not understanding supervisory liability;
- Not ensuring reported issues are appropriately addressed, escalated or documented;
- Not maintaining a robust compliance program;
- Accepting full responsibility for organizational compliance;
- And, of course, contributing to a violation.

The good news is that CCOs can dial down their increased personal risk by taking these key steps.

KEY STEPS FOR ORGANIZATIONS TO TAKE:

» **Realize CCO liability is not limited to public, financial services firms.**
While enforcement actions have largely occurred in this sector, CCOs in all industries, public or private, should take steps to protect themselves from liability.

- **Understand and manage "supervisory liability."**
  Ensure supervisory policies are written. When misconduct occurs, make sure the company documents which supervisor is responsible for handling it. Committees on which a CCO serves should have documented in their charters that the CCO's role is only advisory. Escalate serious concerns about legal violations to designated senior management (per escalation policy).

- **Make policies, standards and the Code easily accessible.**
  Ensure no one can say "they didn't know what to do" because they could not find the necessary guidance documents.

- **Educate employees and others.**
  Anyone who acts on behalf of the organization (employees, third parties or board members) should be trained or otherwise educated on the standards of workplace conduct, their responsibilities regarding ethics and compliance and the resources provided to ask questions or raise concerns.

- **Develop and follow a board-approved escalation policy.**
  This is a key step in ramping up protection by taking the decision to escalate out of the CCO's hands. Such a policy is more than the chain of contacts for your Helpline. It lays out the specific steps a CCO must take if those in "sensitive" roles (such as CEO, board member and executive management) are implicated in an allegation or if an issue surfaces that could have material impact on the organization's reputation or financials. Escalation should occur within 24-48 hours and should not wait for the completion of an investigation.

- **Screen and monitor those that carry out work for the organization.**
  It is important to know who is coming through the front door. This is essential for engaging third-party partners such as contractors and distributors and also new hires and promotion candidates. Interviewing for integrity to increase the likelihood of hiring those wired for good conduct is a new trend worth considering.

- **Implement a CCO charter with detailed responsibilities, accountabilities and authorities.**
  This is more than a routine job description. It is a blueprint for what a CCO should and is empowered to do, including seeking legal advice from outside counsel when needed. Such a charter also helps avoid turf battles by laying down the bright lines between compliance and its sister functions. Charter authorities may include:

  - Delegation of matters for investigation
  - Ability to raise issues directly with CEO, chair of board committee or full board committee
  - Ability to conduct internal investigation of matters
  - Ability to access any company document when investigating a relevant compliance matter
  - Ability to retain outside counsel on matters of personal professional risk, in collaboration with GC

- **Ensure you are covered by D&O insurance.**
  Don't be afraid to ask if you are covered. Understand the scope of your coverage. And, get the answers in writing.

- **Don't limit program ownership to just you.**
  Ensure you have executive compliance committees to help deepen understanding of risks through executive-level responsibility. Have a strong network of Regional Ethics and Compliance Officers. Ensure risk management is assigned to key subject matter experts including CFO, CTO, GC, HR and E&C.

» **Make documentation rock solid.**
If it isn't written down, it didn't happen. Meticulous record-keeping of training completions, attestations, policies accessed, case files and all the other documents generated by an effective compliance program are best managed with technology. Document important decisions, outcomes of reports, formal advice, escalations, committee minutes and policy reviews. Ask your compliance committee or other party to review key decisions where appropriate. Cite major decisions in board reports. Create and follow a documentation retention plan for all compliance program documents. Paper files, fraught with vulnerabilities, may be the biggest CCO liability of all.

Conclusion

At NAVEX Global, we rely on the insights we gain from research and ongoing discussions with our 12,500 clients – the largest ethics and compliance community in the world. Throughout the year, 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 demonstrates that 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. Give us your feedback to this article. Subscribe to our blog, Ethics & Compliance Matters. Participate in our webinars. Visit with us at conferences. Join our newsletter lists. And let us know what you see as emerging trends and challenges – and how we can help.

Footnotes:

[1] http://theirf.org/research/generations-in-the-workforce-marketplacepreferences-in-rewards-recognition-incentives/1427/

[2] https://www.linkedin.com/pulse/workforce-statistics-generation-heather-kreiger

[3] http://time.com/3854518/millennials-labor-force/

[4] http://www.forbes.com/sites/kathryndill/2015/11/06/7-things-employers-should-know-about-the-gen-z-workforce/#468d0f742188

[5] http://www.informationweek.com/strategic-cio/team-building-and-staffing/gen-z-hits-the-workforce-are-you-ready/d/d-id/1324710

[6] http://www.hrreview.co.uk/hr-news/diversity-news/ageism-workplace-widening-skills-gap/57243 - Ageism in the Workplace is Widening the Skill Gap, 2015.

[7] The Yates Memo, officially titled "individual Accountability for Corporate Wrongdoing" was issues by Deputy Attorney General Sally Yates to all DOJ components and US Attorney's Offices on September 9, 2015

[8] http://www.prnewswire.com/news-releases/leading-cause-of-data-security-breaches-are-due-to-insiders-not-outsiders-54002222.html

ABOUT NAVEX GLOBAL

NAVEX Global's comprehensive suite of ethics and compliance software, content and services helps organizations protect their people, reputation and bottom line. Trusted by 95 of the FORTUNE 100 and more than 12,500 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