ethikos

THE JOURNAL OF PRACTICAL BUSINESS ETHICS

JANUARY/
FEBRUARY 2015

Vol. 29 | No. 1

The 7 biggest mistakes companies make

that can erode their ethical culture and destroy their reputation

1

Meaningful change

takes time and dedicated effort

8

EDITOR: KORTNEY.NORDRUM@CORPORATECOMPLIANCE.ORG

www.corporatecompliance.org/ethikos

in this issue

ethikos needs authors like you!

For 28 years, *ethikos* has offered subscribers actionable insights on how to create an ethical business culture through codes of ethics, examples of ethical leadership, and thoughtful and engaging commentary on current events.

Submit your articles
All authors are welcome to submit articles. We accept articles on a continuous, rolling basis. We're looking for 500–1,600 words that address business ethics generally or focus on a particular business ethics topic.

With the article, please include:

- The title of the piece
- Your address and contact information
- A high-resolution headshot (at least 300dpi)

Authors receive 2.0 non-live Compliance Certification Board (CCB)® CEUs for each published article.

Contact editor Kortney Nordrum via email at kortney.nordrum@corporatecompliance.org or by calling her direct line at +1 952 405 7928.

The 7 biggest mistakes companies make that can erode their ethical culture and destroy their reputation

How to avoid them, reduce risk, and demonstrate due diligence *before* the crisis

BY ERIC FELDMAN

You can't pick up a newspaper or turn on the television news today without hearing yet another disturbing story about corporate fraud in all its forms: bribery, gratuities, kickbacks, false claims, violations of the Foreign Corrupt Practices Act (FCPA), and even illegal corporate wiretapping of private citizens. Most of these stories begin with a rogue company employee, manager, or executive violating the rules of the road, followed by a whistleblower reporting the "crime" to the Securities and Exchange Commission (SEC), the Department of Justice (DOJ) or a federal/state Office of Inspector General. A subsequent federal or state investigation leads to government prosecutions of both the employee and the company, followed by lengthy and costly litigation. The DOJ, SEC, or other agencies then demand settlements or fines in the millions or hundreds of millions, forcing the company to sign a consent decree admitting responsibility and accepting years of monitoring and reporting requirements.

The end result is usually disastrous for companies and the people that run them: financial losses that can cripple a company's future; the tanking of corporate and product reputation that took years, even decades to

build; erosion of stock prices; and the loss of jobs in an already weak economy. It is at this point in the process that most companies just *begin* to take action, usually in the form of damage control and crisis management.

The truth is that, in most cases, the most severe consequences of corporate ethical lapses can be mitigated, even avoided, by proactive care and feeding of a company's ethical culture. Even small companies can afford to invest in several very simple steps to demonstrate to stakeholders and government regulators that their commitment to ethics and integrity is real, pervasive, and unwavering. Unfortunately, with all of the pressure surrounding business performance these days, the elements of an ethics program often take a back seat until a crisis blows up—when it's too late to "put the genie back in the bottle."

THE TRUTH IS THAT, IN MOST CASES, THE MOST SEVERE CONSEQUENCES OF CORPORATE ETHICAL LAPSES CAN BE MITIGATED, EVEN AVOIDED, BY PROACTIVE CARE AND FEEDING OF A COMPANY'S ETHICAL CULTURE.

The following is a list of the most frequent mistakes companies make by failing to build in the elements of a credible ethics and compliance program into their business process. Avoiding these mistakes, employing time-tested risk reduction strategies, and demonstrating due diligence and a strong ethical culture in advance of the inevitable crisis can make the difference between a bump in the road or quicksand when the government comes knocking at the door.

1."Put the Code On The Shelf"

A Corporate Code of Business Ethics and Conduct, or the "Code of Conduct," is not a reference handbook, like a dictionary, that contains the list of "thou shalt nots" that can be stored on the shelf in the unlikely event that someone might need to look at it sometime down the road. Nevertheless, bookshelves of many Fortune 100 companies all over America are cluttered with nice, glossy Code booklets with bindings intact and inches of dust. An effective Code of Conduct is the living manifestation of a company's core values. It identifies the company's ethical expectations of its employees in a variety of areas; communicates the CEO's personal priorities and commitments to ethics and integrity; outlines the most common rules and regulations that are applicable to their unique business areas; and lays out the consequences of employee failure to adhere to these rules. Most importantly, it should provide the framework for good ethical decision making by both new employees and veterans that can be applied to virtually every situation, and provide numbers for employees to contact when there are doubts about which path to take.

The Code of Conduct should also form the basis for company ethics training, and be used and referenced in staff meetings, from the boardroom to the mailroom. It needs to be regularly updated to reflect constantly changing laws, regulations, business practices, and new markets, and be included in annual tests of employees' ethics knowledge. I know of one company that attempted to use its code of conduct as a defense of its ethical culture when an employee took bribes from a subcontractor and passed the cost of the bribes along to the government as "overhead. The company said that the employee was a "rogue actor" in an otherwise stellar ethical culture, as supposedly demonstrated by their glossy code of conduct. When asked by prosecutors about the last revision of the Code, the company sheepishly admitted that it hadn't been updated in 6 years. The company was subsequently prosecuted for submitting a false claim.

2. "Ignore the Culture"

There is a lot of confusion these days between the terms "Ethics" and "Compliance," and many businesses think they are one and the same. They are not. "Compliance" refers to adherence to laws, rules, and regulations. It is the "floor" of behavior, the very minimum the government expects companies to honor as it goes about its business. "Ethics" is the set of guiding principles and core values that guide a company's (and its employees') behavior and decision making, and is often a higher standard than what is laid out in the law.

Companies that focus solely on compliance ignore the ethical culture of their organization, often at their own peril. Ethical culture, loosely defined, refers to "how things are *really* done around here," versus what is in the manual. It is the employees' perception of what their bosses expect and what they will really do under different circumstances. For example, while the company may talk a good line about ethics and integrity and officially denounce the giving of gifts or gratuities to "facilitate" contracts, the culture may value production and reaching quarterly financial goals over the prohibition of gifts and payments. According to the Ethics Resource Center, the state of a company's ethical culture is a key determining factor that drives the amount of employee misconduct within a company.[1]

Ethical culture can be readily assessed through the administration of simple employee cultural surveys at regular intervals (every other year is recommended). Survey areas can include employee perceptions of ethics and integrity at the executive, middle management, and supervisory levels; employee comfort level with reporting observations of code of conduct violations; employee fear of "whistleblower" retaliation; overall knowledge of the content of the code of conduct and other aspects of the ethics program; and perception of the strength of internal controls. These surveys can be benchmarked against other companies to help determine where your company stands, and the results (and trends from year to year) can help form the agenda for constant improvements to the Ethics and Compliance program.

A sound ethical culture is viewed as a key to avoiding corporate scandal, safeguarding a company's reputation, and sustaining brand value. This requires the investment of time and attention, not necessarily a heavy investment of resources. A study on ethical culture by the Woodstock Center at Georgetown University said it best: ***"An ethical corporate climate is either developing or deteriorating, enriching itself or impoverishing itself. It needs constant care and attention."***[2]

3. "Worship the GPA"

Companies often pride themselves on extensive recruitment programs that focus on hiring only the best and the brightest from the nation's finest academic institutions. Their recruitment focuses on student GPAs, extracurricular activities, past work experience, and how much they impress the recruiter during the on-campus interview.

Unfortunately, recent studies of student cheating in high school, college, and graduate school show a disturbing and fundamental shift in the values of the nation's emerging workforce. One recent study revealed that 78 percent of high school students admitted to cheating; another found that the highest percentage of college cheaters was in the field of business, where 75 percent admitted they had cheated to get into MBA programs. This data represents a 360 degree shift from similar studies done 20 years ago. Students acknowledged a belief that the "ends justify the means" in both school and the business world (a perspective which they have unfortunately gleaned from Wall Street foibles over the last several years).

Companies that fail to recognize this fundamental difference in the world-view of newly hired employees do so at great risk of getting burned. For example, the Gen X and Gen Y view of "information" is that it is a commodity that ought to be

freely shared via the internet and social media; this often flies in the face of corporate policies that restrict the flow of information deemed to be proprietary. The Gen X and Gen Y view of the workplace is also fundamentally different; the growth of technology has created workplace mobility where employees feel they don't need to be tied to a desk from 9 to 5 to do their job effectively. Nevertheless, companies with government contracts are subjected to strict, "timeclock" type cost charging, which I have seen create serious conflicts within their younger workforce. Problems with résumé credibility, although by no means limited to the new generation of workers, have also taken on a new dimension in a highly competitive job market.

All of these generational problems can be effectively addressed through proactive steps designed to ensure that new hires understand their company's ethical and behavioral expectations once they walk through the lobby doors. These steps include comprehensive new-hire ethics and compliance orientation; annual values-based ethics training; an effective system of rewards and sanctions; and leadership commitment/tone at the top that inspires employees to do the right thing. In the words of Warren Buffet: ***"In looking for people to hire, you look for three qualities: integrity, intelligence, and energy. And if you don't have the first, the other two will kill you."***

4. "Let Money Talk"

Even the most ethically committed of companies can make the mistake of developing their systems of rewards, including executive and staff compensation and bonuses, completely independent of their ethics and integrity objectives. The result: a system of perverted incentives that focuses solely on financial performance at the exclusion of any other corporate value or objective. As a result, employees hear the usually unintended message that they WILL meet their quarterly financial goals, no matter what they have to do to achieve them. If employees perceive that their jobs may be on the line, or that elusive promotion hangs in the balance, the company's ethics and integrity objectives seem a bit more academic and "advisory" in nature.

Companies with world-class Ethics and Compliance programs have broken the code in this area. Some have developed specific ethics and integrity goals that are given equal weight in employee and manager performance appraisals and bonus decisions. The CEO of one company I visited meets with each business unit VP on a monthly basis, reviewing not just financial performance, but requiring each VP to discuss how she/he has executed the ethics program in their organization. At another company, all VP candidates must be vetted through the Ethics and Business Conduct Office; their active support and performance in maintaining corporate ethics and integrity is a factor considered in the promotion decision.

THE MOST EFFECTIVE COMPANIES HAVE ALSO CREATED A BUZZ SURROUNDING THEIR ETHICS PROGRAMS, REWARDING OR RECOGNIZING EMPLOYEES FOR EXTRAORDINARY COMMITMENTS TO ETHICS.

The most effective companies have also created a buzz surrounding their ethics programs, rewarding or recognizing employees for extraordinary commitments to ethics. Some will privately reward whistleblowers (they often prefer to avoid public recognition) by a private lunch with the CEO. Others give out an annual integrity award at a special event that recognizes good ethical decisions, even those that may compromise financial goals. Recognition of employee contributions

for "doing the right thing" can be an even more powerful motivator than money. The company will ultimately profit as well. According to Ethisphere Institute, companies with highly rated ethics and compliance programs, that include leaders and compensation systems that regularly reward ethical behavior, have financially outperformed virtually every market index over the last ten years.[3] Companies that nurture a robust ethics program that is viewed as credible by their workforce are also more successful at channeling the tremendous internal and external pressures to perform that employees feel during today's economic turmoil.

5. "Do As I Say, Not as I Do"

Some companies believe that the CEO message on the inside cover of the Corporate Code of Conduct is enough to demonstrate leadership commitment to running the business in an ethical manner. Add a videotaped message at the annual Ethics training, and perhaps an article or two in the company newsletter, and the company has received the ethical equivalent of the polio vaccine, right?

Not so fast. Studies have shown that leadership commitment and a demonstrable "tone at the top" are essential pieces of creating a strong ethical culture that prevent employees from making bad decisions that can put a company at risk. What leaders say or don't say, and what they actually DO, can either create confidence and trust, or foster mistrust, cynicism, or indifference—factors that erode the ethical culture. A few years back, a major Fortune 100 defense contractor settled charges of Procurement Integrity Act violations by paying a large fine and agreeing to a revised Code of Conduct and a strengthened ethics and compliance program. Just as they were "selling" this new program to the large employee base and hoping to shift the ethical culture of the company, it was revealed that their married CEO was having a personal relationship with his secretary—a clear violation of the Code. The CEO was removed by the board, but the impact on the workforce perception of corporate integrity, and the devastating impact on the company's ethical culture, is felt to this day.

Leadership commitment to the principles laid out in the Code of Code is watched by employees, day in and day out. In fact, "mood in the middle" may be even more important than "tone at the top," since most employees view "leadership" as their immediate supervisor. Studies have shown that an employee's immediate work group of 25 or less impacts their workplace behavior and ethical decision making in a much more fundamental way than what happens in the "C" Suite. In fact, 40 percent of employees who voluntarily leave their companies do so because of their immediate supervisor.

The most effective CEOs take every opportunity to address business matters in the context of the company's core values, which often include a commitment to ethics and integrity. This includes, staff meetings, speeches, employee gatherings, holiday celebrations, etc. CEOs must constantly remind senior managers and employees alike that they are expected not only to follow all laws, rules, and regulations, but to make decisions that they would be proud to share with their families, friends, and local newspapers—regardless of whether or not those decisions maximized revenue. CEOs and other senior leaders must also follow through on sanctions for those employees who violate the Code of Conduct—regardless of rank or position, financial contributions to the company, etc. A CEO who allows the mail clerk to be fired for stealing petty cash, while giving the Assistant VP for Marketing a "slap on the wrist" for improper client billings because he's in the middle of putting together "a really big deal," has essentially abdicated his credibility, and invalidated the company's commitment to integrity.

6. "Ethics In The Corner"

Nothing says "this isn't really important" more than creating a company Ethics Officer position and

placing it down in the bowels of the organization. Recent amendments to the Federal Sentencing Guidelines for Organizations allow credit only for those corporate ethics and compliance programs where the Chief Ethics and Compliance Officer (CECO) has a direct reporting responsibility to the board and the CEO. Establishing a CECO position with responsibility and authority commensurate with the other company business units makes Ethics and Business Conduct a force equivalent to that of sales, marketing, finance, or legal.

I visited one company a few years back to conduct an assessment of their Ethics and Compliance program. The CEO asked me to brief the senior leadership team about my review at their weekly Monday morning meeting. I agreed, and said I was looking forward to meeting the company CECO at the meeting. He look puzzled, and asked if I wanted him to invite the CECO to that meeting. It turns out that the CECO was NOT a member of the senior leadership team….not even close. The CECO was not present when key business matters were proposed, debated, and decided upon. How, then, was ethics considered as an integral part of the company's business process? In fact, it was not. The Ethics Office was created as a result of a previous consent decree, and although the company was "in compliance" with the letter of the agreement, it certainly was not changing the ethical culture of the organization.

The most effective companies follow several key principles when establishing their CECO positions:

- ***Accountability*** to appropriate authority for fiduciary responsibility.
- ***Independence*** to raise matters of concern without fear of reprisal or conflict of interest.
- ***Authority*** to have decisions and recommendations taken seriously.
- ***Connection*** to company operations, to build an ethical culture and enforce standards.

7. "Shoot (Or Ignore) The Messenger"

The 2009 National Business Ethics Survey found that almost 40 percent of employees who witnessed misconduct in their companies failed to report it to the appropriate company authorities. A similar percentage of employees indicated that they feared retaliation, such as being demoted or fired, if they came forward with allegations of misconduct. Others didn't report because they had little faith that their company would do anything about it.[4]

So, in spite of the widespread use of anonymous reporting hotlines, anti-retaliation policies, and robust corporate investigatory capabilities, company employees are still remaining silent about fraud and misconduct thriving in their organizations. In essence, corporate ethics and compliance programs often don't have credibility in the eyes of these employees.

Why does this matter? Most allegations of fraud, in both public and private organizations, result from employee tips. In essence, employee whistleblowers constitute the eyes and ears of the corporation. Without these tips, the company is operating blind, and is likely to be blindsided later as the fraud becomes larger and more widespread. According to the Association of Certified Fraud Examiners (ACFE) 2010 Report to the Nations on Occupational Fraud and Abuse, companies with an effective, credible anonymous hotline suffered 60 percent lower median losses due to fraud, and the duration of the fraud schemes were 35 percent shorter than at companies without an effective hotline program.[5]

If a hotline is going to be credible, it needs to (1) ensure anonymity (if requested), (2) provide confidentiality, and (3) result in demonstrable company actions in response to the allegations. At one company I recently visited, I asked about whether the company had an anonymous reporting process. I was told that they did, indeed, have a hotline. I then asked about the activity—how many allegations, how many requests for assistance, etc. Company officials "proudly" reported

that the hotline had received no calls…zero during the previous year. They (erroneously) thought that this metric demonstrated the strength of their ethical culture. I then asked who answered the phone. Turns out, the "hotline" was answered by the security director, who was well known by the employees. If this wasn't bad enough, the phone had caller ID capability that was NOT disabled. Thus, the mystery of the unused hotline was solved.

A new sense of urgency to the hotline credibility problem has surfaced this year, with implementation of the whistleblower provisions of the Dodd-Frank Wall Street Reform and Consumer Protection Act. This legislation created awards of 10–30 percent of monetary sanctions for whistleblowers who report their concerns directly to the SEC with information leading to securities law enforcement actions that recover more than $1 million. In essence, Dodd-Frank places corporate ethics programs in direct competition with the SEC for employee loyalty and trust, further increasing the risk of severe company losses to both their reputation and their bottom line.

Credibility is the name of the game for corporate ethics and compliance activities. The hotline is, in many ways, the centerpiece of the ethics program, serving as a bridge between the employee and the company in bringing forth allegations of wrongdoing, ethical concerns, or even questions regarding an ethical dilemma and the various options available. Companies that retaliate against employees for taking the time to bring information to the company, or that ignore employee concerns, do so at their own peril.

Conclusion

Although any of these mistakes can create enormous risks for a company, the good news is that those risks can be mitigated, even avoided, by creating a business ethics and compliance program that includes seven basic principles:

1. Demonstrated leadership commitment and tone at the top;
2. A corporate focus on regularly assessing, and improving, the ethical culture;
3. A CECO that is properly placed in the organization and has the authorities and resources to do the job;
4. A comprehensive, dynamic code-of-conduct that provides the framework for good ethical decision making by employees on a day-to-day basis;
5. A values-based ethics training program that goes beyond compliance with the law and focuses on BOTH entry-level hires and senior executives;
6. A system of rewards and sanctions that equalizes financial and ethics/integrity objectives; and
7. An anonymous hotline that earns the credibility of employees through corporate action. ■

Eric Feldman (efeldman@affiliatedmonitors.com) is the Managing Director of Corporate Ethics and Compliance Programs, Affiliated Monitors, Inc. in Redondo Beach, CA.

ENDNOTES

1 Ethics Resource Center, 2009 National Business Ethics Survey (www.ethics.org).

2 "Creating and Maintaining an Ethical Corporate Climate," Woodstock Theological Center, Georgetown University, 1990.

3 Ethisphere Institute, "2010 World's Most Ethical Companies" (www.ethisphere.com).

4 Ethics Resource Center, 2009 National Business Ethics Survey (www.ethics.org).

5 ACFE 2010 *Report to the Nations on Occupational Fraud and Abuse* (www.ACFE.com).

Meaningful change takes time and dedicated effort

BY KORTNEY NORDRUM

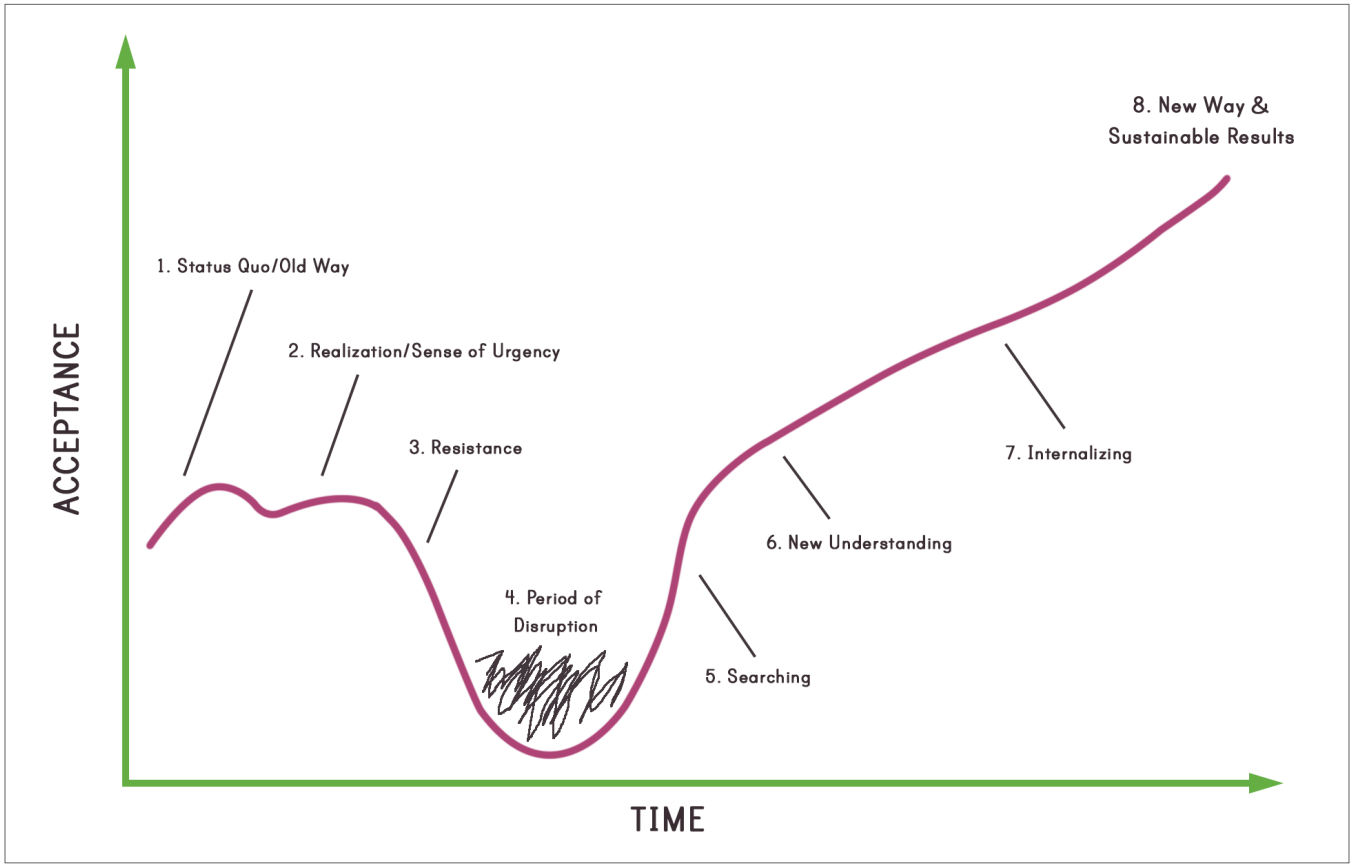
Recently I was reading an article about the Minneapolis School District and how difficult it has been for the school board to implement change. They had a small graphic accompanying the article. That graphic got me thinking. Although the challenges this particular school district is facing are unique (at least to school districts), their struggle is universal. Simplified, the struggle is change.

It's an old adage that change is inevitable, and it's true. Whether in your personal life, or in your organization, change is going to happen. On the next page is a chart that shows what I'm calling the 8 Stages of Organizational Acceptance.

Stage 1 is simple; it's the old way of doing things, the status quo. Everyone is comfortable and there is predictability.

Stage 2 is when an organization realizes there is an issue and that it needs to be addressed. Often this stage is the result of a problem being brought to the attention of management. The severity of the problem may determine the degree of urgency in addressing it. If you have investigators or regulators breathing down your neck, you're likely to seek more urgent change.

Stage 3 is resistance. Resistance can stem from any level of an organization—top to bottom. People like routine and predictability. As soon those things are disrupted, there will be resistance, regardless of what the change actually is or the reasoning behind it.



Stage 4 is a period of disruption. As with all organizational change (from implementing a new code of conduct to switching from Pepsi to Coke in the vending machines), there is going to be a period where things are out of whack. People may not understand what is expected of them, or may be unclear as to how their roles are changing. This is the time when everyone is breaking old habits, and learning new ones. Things may get a little messy during this transition.

Stage 5 is the turning point for those affected by the change. This stage is searching. At this point, everyone is starting to become more comfortable with the new way of doing things. Now is when individuals will begin to search internally as to how they fit into that change.

Stage 6 is the lightbulb moment. At Stage 6, a new understanding has been gained. Everyone has accepted that the change has occurred, and realizes the role they play within it.

Stage 7 is internalizing. Here, everyone has—whether consciously or not—made the "new" way of doing things simply *the way* of doing things. New habits have been formed, and a greater understanding of why the change was implemented has been reached.

Stage 8 is the final stage. At this point, the change has been accepted and become engrained at an organizational level. It's where you can see the lasting effects of the change, and the sustainable results. ■

Kortney Nordrum (kortney.nordrum@corporatecompliance.org) is the Editor of ethikos *and Project Manager at the Society of Corporate Compliance and Ethics.* in */in/knordrum*

Craft questions and live the answers

BY PAUL P. JESEP

In 1903, Rainer Maria Rilke, poet and novelist, counseled an aspiring writer unsure about his future by telling him to "live the questions."

Although Rilke advised the young man about becoming a poet, there is a universal wisdom here also applicable to nurturing an ethical business culture. Put in a practical context, how useful are your surveys? Do your surveys teach, nurture and energize your ethics and compliance culture? How can your team live ethical and compliance questions?

There are different approaches to using surveys. They need not be mutually exclusive and one type can leverage the other. Surveys can gather data and be used to empower your team by making it reflect on "think-questions."

Asking, for example, "On a scale of 1–5 (1 being highly *unethical* and 5 highly *ethical*): How would you rate the organization's overall ethical culture? How would you rate the marketing strategies of products or services? How would you rate the ethical culture in your department? How would you rate the ethics of your manager or supervisor? How would you rate the ethics of the CEO?" are important questions.

You and the Board, if the survey raises issues about senior managers, will want to know if there are actual or perceived problems of this nature. As a side note, there may not be an actual problem, but perception often is reality and must be acted on.

Data collection has its place, yet survey questions can be much more than information gathering. Too often educating your team about ethics isn't done in a manner where individual members are directly engaged to apply lessons.

In short, ask thought-provoking questions that make people pause and humanize the process. Make it about them, as well as the organization.

Here is a selection of questions with several from *Lost Sense of Self & the Ethics Crisis: Learn to Live and Work Ethically* to consider the next time you survey the team.

Do you think about how a decision, internal policy, or marketing strategy may directly impact specific clients, customers, or colleagues?

Can you cite any examples where a decision, policy, or strategy has positively or negatively impacted someone internally or externally?

Do any of these examples suggest values or behaviors that you would want your children or grandchildren to learn and apply, or avoid, in personal and professional settings?

Write down several of the most positive workplace life-lessons you've learned and you think important enough to share with a group of college or high school graduates. "Trust no one" is not a positive life-lesson.

How do you incorporate these positive life-lessons in being a better person and how you do your job? (This question is designed to get individuals who make up any team to integrate and not compartmentalize who they are. Although every business may have unique challenges, ethics and compliance still have universal elements of honesty, fairness, and respect for colleague and customer transcending most, if not all, trades.)

Name three people you most admire and why? How do you apply and integrate their ethics, integrity and character in your work and personal life?

Use surveys creatively that go beyond data gathering. Use them to empower and educate. Engage individuals by getting them to think in new ways not normally expected of them. Independent of using think-questions in surveys, consider them a tool to facilitate discussion as part of workshops when training or re-training your team. Engagement of this nature makes ethics and compliance training into something more than checking off boxes. ■

Paul Jesep (PJesep@gmail.com), JD, MPS, MA, is the author of Lost Sense of Self & the Ethics Crisis: Learn to Live and Work Ethically. *He consults on ethics and compliance and is a corporate chaplain.*

Assessing and understanding insider threats to data security

BY FRANK RUELAS

Here's an interesting exercise to try. Ask someone in your organization's IT or Data Management department to identify the safeguards that are in place to help protect the organization's data. Very often the response you receive will consist of an impressive listing of safeguards that protect the organization's data from external threats. What you may find missing in the response is the identification of safeguards to protect the organization's data from threats that may originate from within the organization, commonly referred to as insider threats. When one considers the significant risks associated with insider threats that may compromise the security of data, it is important to realize that insider threats must also be adequately assessed to minimize or mitigate them to an acceptable level.

Basic concepts

To understand why insider threats may be overlooked or minimally assessed, we need to first understand some basic concepts related to data security, threats, and how threats are identified and managed.

Data security essentially deals with three important objectives aimed at safeguarding or protecting data—confidentiality, integrity, and availability.[1] Although these objectives may be associated with very technical or detailed definitions and attributes, let's look at them from a practical and non-technical perspective, along with examples that help illustrate the concepts associated with each of these objectives.

Confidentiality refers to the protection of data from intentional or unintentional access by an unauthorized individual. Simply put, this means making sure that data is accessible by those who have a need to access it. At the same time, these same processes prevent access to data by those who do not have a need to access it. This is frequently referred to as role-based access, where a person's role is used to determine what data he/she may access. For example, if a person has a role where accessing patient data is an integral part of the job duties or function, this person may have access to an organization's Electronic Health Record (EHR), while those without such a job-related duty or function do not.

Integrity refers to ensuring that data is not altered in an unauthorized manner. An example of this is where computer users are able to access a file in a shared location within a network in a read-only capacity. This allows computer users to view the information within the shared location, but also prevents users from changing the file's contents.

Availability is that data security objective aimed at protecting data against intentional or unintentional deletion. Availability also is aimed at ensuring that users are able to access data when it is needed. An example of this is data backup procedures that allow for the restoration of data if the data is deleted by a user or replaced by another file with the same name, thus making the original data unavailable. This objective also includes efforts to maintain the computer system's operability. Downtime, either as a result of failure of computer equipment (hardware) or by failure of its operating system (software) is another point of emphasis within the availability objective.

So with these three objectives in mind, those responsible for implementing safeguards to protect and promote data security conduct a risk assessment to identify those circumstances or events (referred to as threats) which may compromise any of these objectives, either individually or in combination.[2] By analyzing the results of a risk assessment, organizations can then decide what types of safeguards may be used to offset the identified threats. However, threats originating from outside of the organization are often the prime points of focus of a risk assessment, and insider threats may get overlooked or minimally assessed. When this occurs, data security may be significantly at risk.

Insider threats

The significance of insider threats to data security cannot be understated and should not be underestimated. Research shows that the greatest risk to data security comes from insider threats.[3] This may sound alarming, given that we would expect insiders (e.g., employees, contractors, and others with access to the data) to conduct themselves in the best interests of the organization, including safeguarding its data. This same research also points out something that people may find quite surprising as well as encouraging.

Although there are instances when data security is breached by insiders with malicious intent, this group does not pose the most commonly encountered threat to data security. The group of insiders that does pose the most significant threat to data security consists of insiders who are committing unintentional acts that negatively impact data security. What is encouraging is that there are root causes that, if addressed, can significantly decrease the threats associated with this group of insiders.

Raising awareness on data security and relating it to a user's access to data may be one of the most effective ways to promote work practices that safeguard, rather than threaten, data security. By taking this approach, and combining it with a hands-on training strategy, users are placed in a position where their increased awareness is associated with their job-related functions, which then constantly

reinforces work habits that safeguard data security.[4] Too often users are left to their own devices to figure out what they can and can't do in terms of accessing or using data. By *showing* users, rather than leaving them to figure things out for themselves, extemporaneous activity (which may include activity that users are unaware may jeopardize data security) may be reduced or eliminated.

TOO OFTEN USERS ARE LEFT TO THEIR OWN DEVICES TO FIGURE OUT WHAT THEY CAN AND CAN'T DO IN TERMS OF ACCESSING OR USING DATA.

It is not uncommon for problems to occur right from the start when a new employee comes to his/her department. In the rush that precedes getting someone set up on the computer system, the new employee does not have credentials to access data. In turn, this new employee may be provided a generic user login or even provided the login and password for someone assigned to the department who may be out on leave until the new employee's log in credentials and access is defined. Now you have a situation where someone's role-based access may not be in alignment with his/her needs and allows this new employee to access data he/she has no need to view.

In addition, there may be options to monitor the data use and data access patterns of employees to determine if they are exhibiting behavior that may contribute to an unintentional risk to data security. Are employees going to certain locations on the network in attempts to locate needed files and while doing so, venturing into folders that they have no reason to view? Are employees monitored to determine if there may be activity that may warrant additional attention? For example, is there a department where the employees are calling the IT or Data Management department to reset passwords much more frequently than other departments? If so, what insider activity is contributing to this type of activity?

All of these questions can be asked without users feeling they are being interrogated or investigated for any potential wrongdoing. Falling back on data that justifies the need to ask these questions is a very nice and neat way to stay objective while helping to keep the emotions of anyone involved in check. When doing these types of inquiries, I have found people to be much more willing to share their comments and ideas when I can show them the data that prompted me to ask. This puts people at ease and also makes them feel that their input is necessary to help find much needed answers. In short, it helps prevent an adversarial approach while fostering collaboration, including the identification of opportunities to make both short-term and long-term improvements.

Disgruntled employees

I would be shortchanging the information about internal threats if I didn't bring up what is, hopefully, a very small group of individuals within your workforce. I am referring to are those who may be described as "disgruntled" employees.

The mere idea that disgruntled employees, particularly those who may believe they are about to be fired, would access and take data is troubling enough.[5] References to disgruntled employees and their impact on data security have even been mentioned in Presidential speeches.[6] Combine this with the likelihood that some disgruntled employees may know how to operate within a mode that specifically attempts to avoid detection of their data use and data access, and you have the proverbial recipe for disaster for compromising an organization's data security.

Additionally, the threat associated with a disgruntled employee doesn't necessarily mean that the threat goes away once a disgruntled employee is let go. A disgruntled employee may also be able to exploit known gaps in data security. For example, if federal or state rules and regulations require that an organization take certain precautions to protect data security, and the newly released, disgruntled employee is aware that the organization has not fulfilled these requirements, what is there to prevent the disgruntled employee from reporting this fact to the federal or state entity responsible for enforcement of the rule or regulation which has not been satisfied? Although there is certainly something to be said about organizations that do not fulfill their requirements to be held accountable, my point is that for this to be addressed due to the actions of a disgruntled employee is likely not the best way for everyone involved to deal with unfulfilled requirements.

Conclusion

So, although insiders can pose a significant threat, organizations can do well to position themselves to effectively counteract the insider threat through detection, monitoring, effective training, and the use of effective countermeasures. By maintaining a watchful eye on insiders, an organization is better able to minimize the risks associated with insider threats and thereby do a better job in promoting and strengthening its efforts in maintaining data security. ■

Frank Ruelas (frank@hipaacollege.com) is a Compliance Officer with Gila River Health Care in Sacaton, AZ.
bit.ly/in-frank-ruelas *@Frank_Ruelas*

ENDNOTES

1 Gary Stoneburner: "Underlying Technical Models for Information Technology Security." National Institute of Standards Technology (NIST), Special Publication 800-33, page 2. December 2001. Available at: http://1.usa.gov/1EHhBjF

2 Joint Task Force Transformation Initiative Interagency Working Group: "Guide for Conducting Risk Assessments." National Institute of Standards Technology (NIST), Special Publication 800-30, page 30. September 2012. Available at http://1.usa.gov/1uha4oy

3 Heidi Shey: "Understand The State Of Data Security And Privacy: 2013 To 2014." Forrester Research Inc., page 2. Available at http://bit.ly/1GTsKjw

4 Fred Beisse: *A Guide to Computer User Support for Help Desk and Support Specialists*. Course Technology Cengage Learning; 5th edition, page 500. March 26, 2012.

5 Jeff Goldman: "Disgruntled Employees Present Significant Data Breach Threat." *eSecurity Planet*, July 16, 2013. Available at: http://bit.ly/1tNIIYE

6 Barack Obama, "Remarks by the President On Security Our Nation's Cyber Infrastructure," May 29, 2009. Available at: http://1.usa.gov/1tNlnjl

Compliance 101

The intersection between employee morale and compliance

BY SHAKEBA DUBOSE

It may seem like an elementary question but, what is employee morale? Merriam-Webster's online dictionary defines "morale" as "*the mental and emotional condition (as of enthusiasm, confidence, or loyalty) of an individual or group with regard to the function or tasks at hand*." Accordingly, one Human Resources (HR) expert states that "employee morale is defined by employees' outlook, optimism, self-concept, and assured belief in themselves and their organization, its mission, goals, defined path, daily decisions, and employee appreciation."[1] Now, let's look at compliance. Merriam-Webster's online dictionary defines "compliance" as "*the act or process of doing what you have been asked or ordered to do*" or "*conformity in fulfilling official requirements*." Here, one can clearly connect these two general concepts.

Employee morale: high vs. low

It does not require a comprehensive study to conclude that if employee morale is high, employees feel positive about their work environment and, in most cases, go above and beyond in completing their job responsibilities. On the other hand, if employee morale is low due to employees being overworked, underappreciated, or resentful (due to a lack of growth opportunity or because of others receiving preferential treatment), these employees may only do the bare minimum to complete their given tasks. Thus, they are not paying attention to detail or spending an

appropriate amount of time to ensure that simple mistakes are avoided, which when compounded, can cause major compliance issues. Accordingly, as time passes, if the issues contributing to the low morale of one group are not addressed, eventually those who are typically positive about their roles and responsibilities are drained—they too become negative about their work environment and discontinue any exceptional efforts. And just where does this leave the unit, department, or even the entire organization? A breeding ground for compliance issues.

Compliance staff's role

As a compliance professional in your organization, what do you do? First, compliance staff has to be aware of low employee morale by consistently assessing the environment:

- Are employees generally happy while at work?
- Do they take pride in the organization and its mission?
- Are they given the opportunity to express their ideas?
- Do most view the organization as one in which they can grow and advance?
- Are departments properly staffed?
- Are employees praising their managers or leadership with respect to their abilities to manage and lead the organization?
- Are employees open when asked for their concerns?
- Do employees feel that they are treated fairly?

If the answer to some of these types of questions is "no," there may be morale problem.

Once low morale is identified, the Compliance team should assess what risks it poses to compliance and execute a plan to address those risk areas. This plan may include: (1) working with leadership, management, and HR to identify and properly discipline problem employees and managers who are contributing to the issues that result in low morale; (2) developing or improving departmental policies and procedures and monitoring to ensure that actual practices are in accordance with these policies and procedures to minimize potential compliance issues; and/or (3) re-training and re-educating the employees on compliance policies and procedures.

The reality of low employee morale

As compliance professionals, we spend a tremendous amount of time discussing one of the essential elements of a compliance program: developing effective lines of communication whereby individuals can report their concerns under the protection of a non-retaliation policy. However, the reality is, if employee morale is low and it is low due to the actions or lack thereof of management and leadership and it appears that the rules do not apply to them, it is most probable that employees will not engage in any disclosures of non-compliance issues for fear of retribution by management. Unfortunately, this fear is not unfounded. In many organizations, we find that certain compliance issues result from some action or inaction by management and that management is guilty of harassing or discriminating against certain employees. And, in some cases, it is not that a particular manager was unethical—he/she followed the tone set by leadership.

So, what are rank-and-file employees to do when they have made a mistake because they are overworked due to understaffing, or when they know that management is not properly instructing

staff on a particular procedure, or when they see that leadership does not take any action against bad managers or fellow leadership who have displayed unethical or inappropriate behavior? We as compliance professionals say, "Report it." But, what incentive does an employee have to report compliance issues? What real assurances does an employee have that he/she will not be harassed or even worse, lose their job?

Conclusion

As compliance professionals, we must not only develop and implement "seven element" compliance programs, we must also must demonstrate that we are approachable and open to hearing about compliance issues that place the organization or even employees at risk. Moreover, we must develop and maintain a reputation for flushing out issues and working with leadership, management, and HR to resolve the issues that negatively impact employee morale, which in turn increases the potential for non-compliance. By doing so, compliance professionals build trust with the employees who view the Compliance department as one of the pillars of an ethical organizational culture. We must recognize that our roles should not be siloed; otherwise, our time and energy spent on the development and implementation of compliance programs are wasted and the programs will be ineffective. ■

Shakeba DuBose (sdubose@theduboselawfirm.com) is the Founding Member of The DuBose Law Firm, LLC and TDLF Healthcare Compliance Consulting Group, LLC in Columbus, OH. /in/shakebadubose
TheDuBoseLawFirmLLC

ENDNOTES

1 Heathfield, Susan M: "You Can Boost Employee Morale." About.com website. Available at http://humanresources.about.com/od/glossarye/g/employee-morale.htm

Incentives

BY SHAWN DEGROOT

It seems to be an appropriate time of year to discuss the incentives that are often associated with rewards. As a noun, an incentive is something that incites action or greater effort as a reward offered for an action. Many compliance incentives were developed as a result of the Federal Sentencing Guidelines; however, there are new compliance and ethics officers who may not be aware of or who have chosen to ignore the following standard:

> CHAPTER EIGHT
> PART B – REMEDYING HARM FROM CRIMINAL CONDUCT, AND EFFECTIVE COMPLIANCE AND ETHICS PROGRAM
> (6) The organization's compliance and ethics program shall be promoted and enforced consistently throughout the organization through (A) appropriate incentives to perform in accordance with the compliance and ethics program; and (B) appropriate disciplinary measures for engaging in criminal conduct and for failing to take reasonable steps to prevent or detect criminal conduct.

The key word in the statement above is *shall,* meaning "not optional." To initiate a plan, criteria should be developed to incentivize the workforce consistently. Without criteria there will more than likely be inconsistency and an employee who constantly calls with issues

simply to receive the reward. Drawing a name at an employee meeting for a reward is an easy approach; however, it's not as effective. Best practice would be to develop incentives for compliance reporting that result in change. An example: Reward an employee who submits a concern and/or issue that results in a policy revision, a change in a process, or leads to enhancing the compliance education.

The type of reward or incentive can be tangible or intangible, such as a designated parking spot for a month, four hours of vacation time, free cafeteria meals for a week (although that may be taxable in the near future), coffee cards, gift certificates, cash, or items with your company's logo. The issue and incentive could be generated and awarded to a department. If you have appropriate influence and supportive management, wouldn't it be nice to collaborate with the director and provide an item staff have been requesting for their break room or an item on their budgeted wish list? Another approach with incentives is to work with the Marketing department (as applicable) to select logo jackets, portfolios, or caps to be distributed during Corporate Compliance & Ethics Week.

The last component with incentives is who decides whether the issue/concern submitted has value and resulted in change. The compliance team could decide, or the compliance committee could make the decision. Selection by the multi-disciplinary compliance committee would promote inherent awareness simply through the act of reviewing the issue that was submitted with the associated change.

Regardless of the type of reward, developing criteria for incentives and implementing and executing a plan of action will benefit the organization, demonstrate effectiveness, and create awareness of the compliance program in a positive manner. ■

Shawn DeGroot (shawn.degroot@navigant.com) is an Associate Director at Navigant Consulting in Denver.
bit.ly/in-ShawnDeGroot

Add some ethics *to your reading list*

Subscribe to *ethikos* and get the latest, best practices written by and for the business ethics community

- Receive six issues each year, filled with deep insights
- Hear from experts in business ethics
- Take away practical ideas designed to help your program

Enjoy special pricing for SCCE members:
JUST $125 A YEAR

Not yet a member of SCCE?
Subscribe to *ethikos* for $135 a year

Subscribe online at
www.corporatecompliance.org/ethikos

UPCOMING CONFERENCES

from the Society of Corporate Compliance and Ethics

FEBRUARY 2015

Basic Compliance & Ethics Academy
February 9–12 ▪ San Francisco, CA

Regional Compliance & Ethics Conference
February 13 ▪ Phoenix, AZ

Utilities & Energy Compliance & Ethics Conference
February 22–25 ▪ Houston, TX

MARCH 2015

Basic Compliance & Ethics Academy
March 9–12 ▪ Las Vegas, NV

Regional Compliance & Ethics Conference
March 13 ▪ Miami, FL

European Compliance & Ethics Institute
March 29–April 1 ▪ London, UK

LEARN MORE ABOUT SCCE EVENTS
www.corporatecompliance.org/events

ethikos
THE JOURNAL OF PRACTICAL BUSINESS ETHICS

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS (SCCE)®

Managing & copy editor: Kortney Nordrum
Design & layout: Sarah Anondson
Business manager: Adam Turteltaub
Contributing editors: Lee Essrig and Roy Snell

ethikos (ISSN 0895-5026) is published bimonthly, copyright © 2015 by the Society of Corporate Compliance and Ethics, 6500 Barrie Road, Suite 250, Minneapolis, MN 55435-2358, United States. Editorial comments, questions, article proposals, and reprint requests should be directed to the editor, Kortney Nordrum, via email at kortney.nordrum@corporatecompliance.org or phone at +1 952 405 7928.

An annual subscription to *ethikos* is $135. SCCE or HCCA members receive a special rate of $125. To subscribe, visit www.corporatecompliance.org/ethikos or call +1 952 933 4977 or 888 277 4977.

Past issues of *ethikos* are available to current subscribers on the website, www.corporatecompliance.org/ethikos. Authorization to photocopy items must be obtained from the Society of Corporate Compliance and Ethics.

Visit www.corporatecompliance.org/ethikos to sign up for our free weekly *ethikos* email newsletter.