Managing Cross-Border and Domestic Compliance Challenges

KAYE | SCHOLER

Table of Contents

Versions of these articles were originally published in InsideCounsel, March–May 2015.

Foreword

With domestic and international regulatory environments becoming more demanding—both in terms of the proliferation of new rules and the increased coordination among global enforcement agencies — global organizations increasingly must navigate complex compliance issues, reconcile conflicting regulations, manage risks and resolve related disputes.

Compliance is no longer a pro-forma, check-the-boxes function. It is now an affirmative enterprise-encompassing discipline that can be embraced to develop business, new opportunities and the bottom line. Quite simply, for market savvy organizations, effective compliance has gone from being a business cost to being a business driver.

This report, *Managing Cross-Border and Domestic Compliance Challenges*, explores how you can make this complex compliance environment work to your advantage. With six related articles authored by attorneys active in our leading M&A, Antitrust, Cybersecurity and White Collar Investigations & Related Litigation practices, the report shows how to create a strong compliance culture with programs that surpass governmental expectations and monitoring. It presents two current case studies, the GM ignition switch failure and Siemens' rebound from a compliance failure that induced record-breaking penalties, as well as four prescriptive pieces for implementing and strengthening domestic and global compliance programs, increasing cross-border investigation readiness, managing global cyber risk, and emerging successfully from a compliance failure.

The current compliance landscape, with its interconnected regulatory regimes, creates intricate business, legal and reputational risks for the foreseeable future. We hope that this report provides insights into the factors and considerations that foster a compliance program that aligns with your operating environment. We look forward to continuing the conversation and welcome the opportunity to help you develop tailored strategies for your compliance and cross-border needs.


RUSSIAN FEDERATION
MONGOLIA
CHINA
NEPAL
BHUTAN
BANGLADESH
MYANMAR
THAILAND
VIETNAM
REPUBLIC OF KOREA
60
45
30
15
0

Four Strategies to Improve Cross-Border Investigation Readiness

These four topics can jump-start the discussion with your team of stakeholders to increase your company's cross-border investigation readiness

Tiffany R. Moseley
Partner

Amy Conway-Hatcher
Partner

Much like military campaigns, cross-border investigations are inherently complex, driven by unique facts, shifting priorities and necessarily shaped by local terrain. Both also require decisive leaders ready to make quick decisions and lead large teams. And, just as there is no way to predict every aspect of a battle, there is no one-size-fits-all cross-border crisis plan or a fool-proof cross-border investigation checklist. General counsel cannot possibly predict and plan for all of the unexpected pitfalls bound to arise in a complex, dynamic cross-border investigation, but they can take steps to anticipate likely issues so that they are not caught flat-footed.

The most crucial step is to engage in a planning exercise with key stakeholders that accounts for the company's structure, priorities, geographic footprint and operational risks, and that clearly identifies the internal and external assets available to protect and defend the company. Create a core list of cross-border issues the company likely will confront to plan for the identifiable challenges but, more importantly, discuss how your team can work together to respond quickly, efficiently and creatively to unexpected pitfalls. Ultimately, preparation—not a cookie-cutter plan—will help make your company mission-ready for the next cross-border crisis. Below are four key topics to jump-start the discussion with your team of stakeholders to increase your company's cross-border investigation readiness.

1. Know where your troops and their records are located. Know where they can get into real trouble and identify problems early.

Companies are constantly re-organizing, changing third party suppliers, working with new customers and acquiring and divesting of assets, all while operating in shifting regulatory regimes. An accurate and up-to-date map of the company's business units, where they are located, who they do business with and where the business records are maintained is an invaluable tool that allows in-house counsel to determine:

a. What laws govern or impact how the company operates?

b. Where does the company need to develop credible local legal assets? How active are local regulators?

c. If there is a problem, what laws will impact the company's ability to investigate and resolve it?

d. How will applicable employment and privacy laws impact the company's ability to speak with or discipline employees?

e. Does the company have local IT assets and data privacy advisers for real-time IT capabilities?

Knowing where your company does business, what limitations may be present due to local regulations and which regulators are likely peeking over your shoulders is invaluable. Just as military tactics may vary depending on the terrain, investigating conduct related to business operations in China will require different investigative tools than in Brazil, Russia or Germany.

2. Allocate and deploy your cross-border assets and budget efficiently.

In today's world of limited compliance and legal budgets, it is not feasible or advisable to prepare for investigations in every country around the world. To maximize a company's cross-border investigation readiness, it is important to understand where your greatest risks are, prioritize the defense of the company's key assets and develop a risk-based monitoring strategy. Do you have a business unit too big to fail? A fledgling business unit key to future growth? A new venture in an emerging market known for anti-corruption issues? A new product launch?

Knowing your company's strategic plan and corporate priorities is fundamental to effectively prioritize the deployment of company resources needed to protect key assets around the globe. It is not possible to predict where a cross-border problem will strike first, but it is possible for a company to be more nimble and better equipped to defend the key business assets in the jurisdictions most likely to be "hot-spots."

3. Identify the assets needed to support a cross-border investigation.

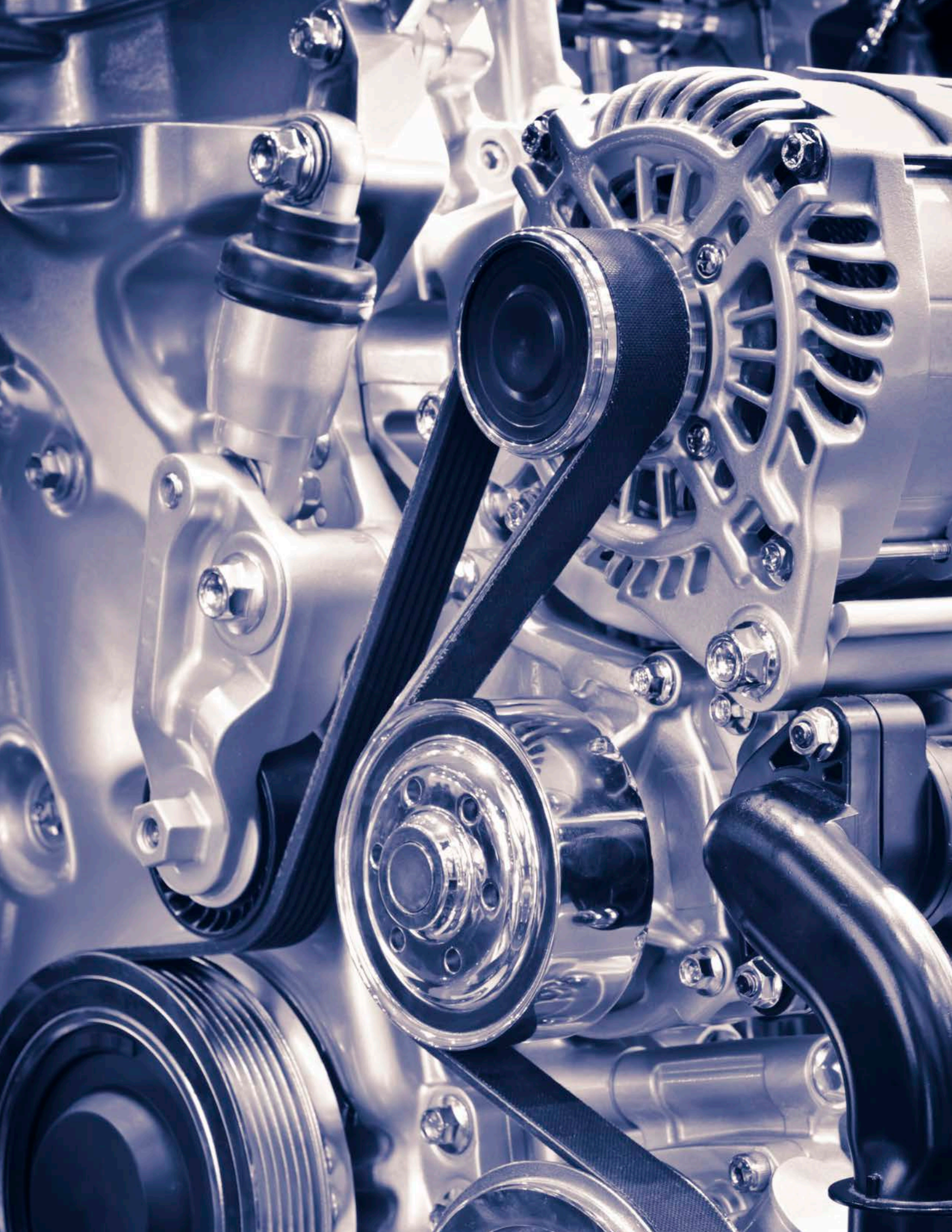
Cross-border investigations by their nature require a cross-functional, efficient, coordinated team capable of facing unexpected and inevitable challenges, such as employee issues, data complications, forensics, financial reporting and communications, to name just a few. Establishing relationships with IT, compliance, regulatory specialists, human resources, accounting, communications and investigative counsel will help in-house counsel pull together a rapid response team in a cross-border crisis and avoid many common investigation start-up delays. For example, given the complexity and volume of e-data in today's global economy, prior identification of internal IT specialists with the knowledge, skills and understanding of jurisdiction-specific restrictions regarding how information may be reviewed, transferred or possibly disclosed a cross-border investigation scenario will likely save the company valuable time and money. In today's enforcement environment, the fewer the complications at the start of the investigation, the better the chances of setting the right internal and external tone and increasing the company's chances of minimizing direct and collateral damage.

4. Huddle with your lieutenants and "table-top" a cross-border investigation. Integrate the lessons learned into company practices.

There is no substitute for practice. Simulate the chaotic first few days of a cross-border crisis and mock-exercise to get a cross-border investigation off the ground. Huddle with the key stakeholders in your organization to identify and discuss mission critical tasks, what is needed to accomplish those tasks, and any known hurdles. Take note of and fix any weaknesses in the system. For example, does human resources have a standard informed consent agreement for data collection? Do your whistleblower hotline procedures have the language capabilities for all relevant jurisdictions? How do cross-border issues currently come to light in your organization? Assign areas of responsibility so that the team can work together efficiently in the event of a real crisis and develop the relationships that will be needed to support a cross-border investigation. Put together a list of possible experienced and practical outside advisors whom you could tap in the event you identified a problem.

As Benjamin Franklin once noted, "By failing to prepare, you are preparing to fail." When supporting your multi-national business, don't let the unexpected issues in a cross-border crisis catch you or your team off guard. Planning today will streamline your investigations of tomorrow.

“Ultimately, preparation—not a cookie-cutter plan—will help make your company mission-ready for the next cross-border crisis.”



Lessons Counsel Should Learn from the GM Ignition Switch Failure

If GM had taken a few simple steps, it would have avoided many of its later problems

Alan Salpeter
Special Counsel

Emily Newhouse Dillingham
Associate

The tragic results of the General Motors ignition switch failure have provided important lessons for in-house counsel around the globe. As context, in May 2001, GM engineers found that the Saturn Ion's ignition switch could move from "run" to "accessory" inadvertently, from the bump of a knee or the weight of a heavy keychain. The engine would stall, and the airbags would disengage. In May 2002, GM approved this same ignition switch design, even though GM's suppliers had stated that the design did not meet GM's specifications. Customer complaints began as early as 2003, but GM continued to use the same switch design in multiple new models, including the Chevrolet Cobalt. In May 2005, GM opened and quickly closed an investigation into the switch design, deciding that the fix was too costly or time-consuming.

Over the next several years, GM began settling lawsuits involving crashes resulting from the defective ignition switch. In 2012—11 years after GM engineers first noticed the problem—GM conducted tests and calculated the costs of a new ignition switch design. The company, however, did not issue a recall of the faulty switches until Feb. 7, 2014, when it recalled 780,000 vehicles. To date, GM has recalled more than 2.6 million vehicles as a result of the ignition switch failure. Up to 90 people died in crashes linked to the faulty switch; 163 have sustained injuries. The National Highway Traffic Safety Administration has imposed a $35 million fine on GM, and the Department of Justice and nearly all state attorneys general are still conducting investigations.

GM hired Kenneth Feinberg to head the GM victim compensation process. GM also hired Anton Valukas, a former U.S. Attorney, to conduct an independent investigation. Valukas and his team conducted more than 350 interviews with over 200 current and former employees. A 276-page report was issued in May 2014. Commonly known as the "Valukas Report," it details many of GM's failures and the changes it could make to avoid such problems in the future. Ultimately, the fallout from these deaths and injuries could have been prevented if GM had taken certain simple steps to make safety the company's number one priority. What are the critical lessons to be learned from GM's failures? Create the right culture!

Elevate and escalate

According to the Valukas report, GM's in-house lawyers first became aware of the ignition switch issue in 2004. Although they began reviewing and settling lawsuits, they did not elevate the issue to the general counsel until 2013. These same lawyers failed to recognize that an ignition switch failure was a safety issue and to escalate

"In-house lawyers can learn from GM's lack of internal coordination. Be sure that you have formal channels of communication and coordination established among the legal, safety and technical, and business teams."

the problem quickly. They should have worked with the company's engineers to launch a safety investigation, and they should have insisted on a tight timeframe for doing so.

In-house lawyers everywhere should learn from these mistakes: If you become aware of an issue, like a safety issue, that requires immediate attention, elevate it to someone who can and will act on it. Demonstrate a sense of urgency. Insist on an appropriate timetable for action. If your superior is not responsive, go to his/her superior and quickly move up the chain of command. Delays or inaction, especially in industries involving consumer products, can lead to significant safety concerns, high litigation costs and potential punitive damages.

Coordinate within the company

At GM, the attorneys, engineers and safety investigators operated within "silos." Each group functioned as its own unit, with little to no coordination among or between them. No one group took ownership of the problem. Although GM's engineers conducted investigations into crashes that resulted in litigation, the findings were rarely shared with either the legal or safety teams. Similarly, in January 2011, GM attorneys discussed setting up a meeting with GM's safety team, but they waited six months to hold that meeting. During those six months, the in-house lawyers continued to settle lawsuits, but without the benefit of input from GM's engineers or safety inspectors. A formal, coordinated effort among the three groups could have expedited litigation review processes and, in many instances, avoided the crashes that led to litigation in the first place.

In-house lawyers can learn from GM's lack of internal coordination. Be sure that you have formal channels of communication and coordination established among the legal, safety and technical, and business teams. Schedule regular meetings for evaluating issues covered by multiple groups within the company. Frequent contact and interaction will help to ensure that when a problem arises, everyone is aware of it early and can take coordinated action. Most importantly, decide at the beginning of the process which group owns the problem.

Appoint a chief

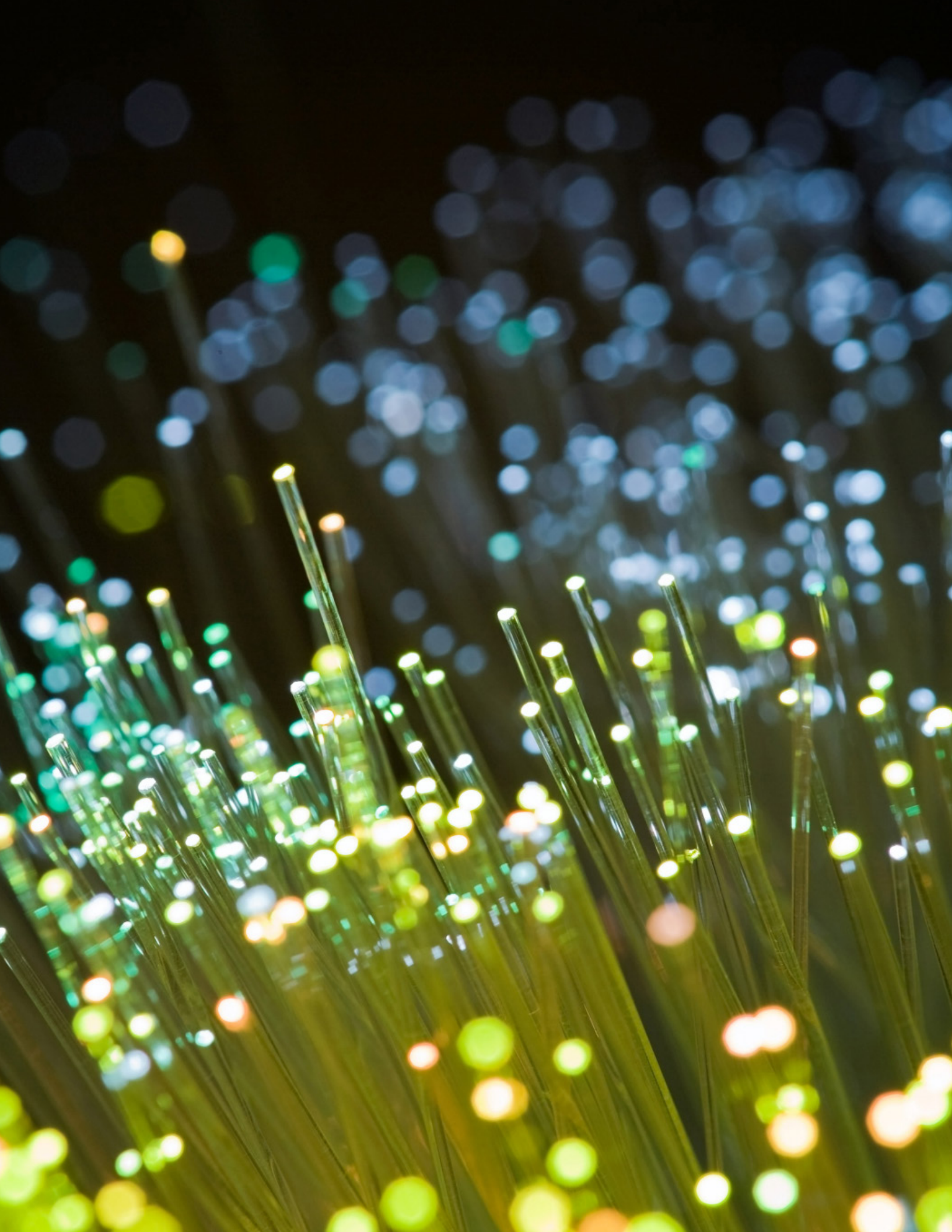
Finally, GM never designated a safety chief within its legal team to serve as the liaison with the engineering and safety teams. No individual ever took charge of the safety concerns raised by the ignition switch issue, so no one felt responsible for addressing the problem. Had GM designated a safety guru, that person presumably would have identified the seriousness of the ignition switch failure at a much earlier date.

Every in-house legal team must decide which department is ultimately responsible for managing the problem under investigation. Is it the law department? Another department within the company? Or a business unit? And which individual is ultimately responsible for the company addressing the problem—which includes taking it to the highest levels necessary to get it resolved? This advice seems so basic and intuitive, yet GM's failure to act cost it a loss of reputation and goodwill, more than $1 billion in recalls, and payments to the victims and their families.

Conclusions

In-house legal teams should learn from GM's failure. Whether your company's issue is safety or compliance with a federal or state regulation, create the right culture. Make sure one individual within your legal department takes ownership of that issue. That person must act with a sense of urgency. Ensure that the designated inside lawyer has the resources to manage the problem. Make sure that that individual knows when and how to escalate the issue within the company.

If GM had taken these simple steps outlined above, it would have avoided many of the problems that resulted from the ignition switch crisis.



Understanding and Managing Global Cyber Risk

Counsel need to help chart a path that effectively deals with risks and allows the company to continue to drive innovation

Adam Golodner
Leader, Global Cybersecurity & Privacy Group

Cyber by definition is global, and businesses and their counsel have to think globally. Yes, of course you have to comply with local law, but faced with increasing national security and economic security cyber threats from organized crime, nation states, non-nation states, hackavists and insiders, counsel need to help chart a path that effectively deals with these risks and allows the company to continue to drive innovation and win in the marketplace, globally. Here's how to do it.

Countries and companies are working their way through this not-completely-charted "cyberspace." Fresh from the headlines are Sony, Target and Anthem, and in the not too distant past, Snowden, Saudi Aramco, Stuxnet, NASDAQ and a spate of new legislative proposals around the globe. A couple of CEOs have lost their jobs, boards of directors are answering questions about what they did or didn't know about cyber readiness and, of course, lawsuits have been filed and litigated.

But the cyber "issue" today is hard to define. What does it mean to effectively deal with cyber globally? It means you understand your "crown jewels," competitive advantage and values, employ risk-based "real security" to protect them, and are ready to respond and recover when something inevitably goes wrong. That sounds easy, but in the ill-defined world of cyberspace, it's not. It's hard work, but work that can and should be done.

Understand your "crown jewels"

What are the crown jewels of your company? How do you prioritize them? Is there agreement at the C-suite and the board about what they are? It could be intellectual property, product quality, innovation, brand, data, service quality, culture, customer trust, government trust or global reach. All of these no doubt are important, but which are the real crown jewels (tangible and intangible) that drive competitive advantage and market leadership? Run a cross functional process to define and prioritize your crown jewels—you can then build prioritized real security around those assets.

Understand your adversaries

Who are your adversaries? What group, individual, nation state or non-nation state might be motivated to impact your crown jewels, and why? Yes, unfortunately, you have to think like a bad guy. Who wants to steal your latest innovation, destroy your data, undermine your service delivery, undermine market trust, embarrass you or create market access barriers in local markets? Do you play a critical role in national or economic security (financial services, communications, information technology, electric, energy, transportation, health care, defense or government) or represent values such as free speech, association or the dissemination of viewpoints? In a global

interconnected world, adversaries can reach out and touch you from most anywhere (often masquerading the actual location) and can be insiders too. Understand who your adversaries are, what motivates them and what methods characterize their activities.

Implement risk-based "real security"

Once you understand your global crown jewels and adversaries, you can and should build risk-based real security around the things that matter most. Compliance and security are not the same thing. You have to do compliance, but you should and must do real security. Start with baseline situational awareness, and then plan a risk-based shift. For example, you need to understand basics such as: identifying all your hardware and software assets, the ingress and egress points to the Internet, where your data is stored, how it's secured, who touches your supply chain, your methodology to ensure product integrity, techniques used to stop data exfiltration, denial of service, data destruction, data corruption, service disruption, and what choices you are making about the use of encryption. You then have to ask—are these tied to and focused on protecting crown jewels? There is a saying in security: "If you try to secure everything, you secure nothing." So no doubt, after setting the baseline and the prioritization, a shift will be in order.

Prepare and exercise response and recovery

What is your plan to respond to and recover from a cyber event? Have you exercised those plans? Things you need to understand or set include: who "owns" the overall response, escalation triggers and process for information flow, and who will run impact analysis, forensics, containment, mitigation and external communications. How about recovery: What are the plans to restore systems, assets or data, and who owns it? There is another saying in security: "There are two kinds of companies—those that have been hacked, and those who just don't know it yet." So, know your response and recovery plans, and exercise them—you will likely need them.

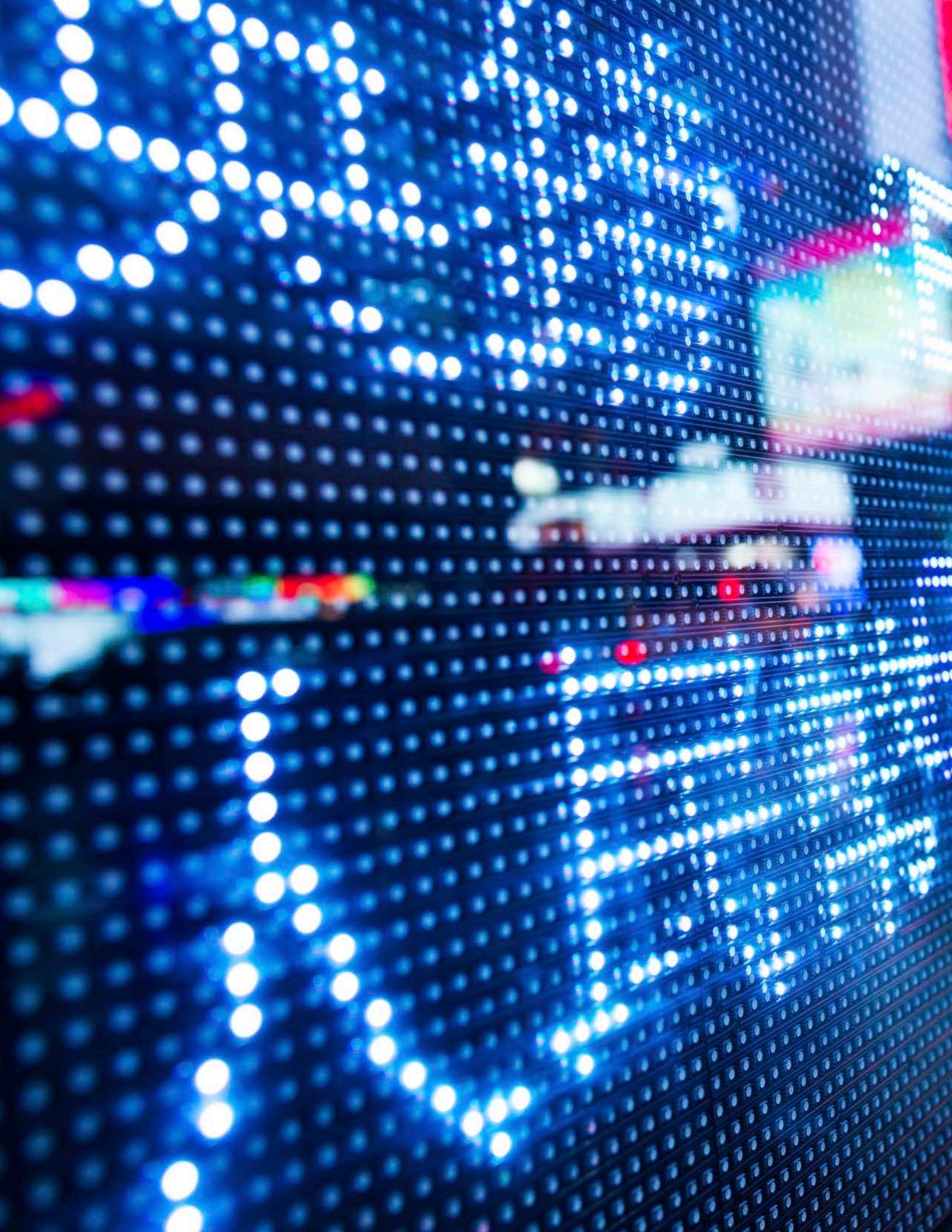
Get help and use best practices

Fortunately, the methodologies to manage cyber risk are improving. Cyber is a team sport, internally and externally. You need representatives from counsel, CIO, CISO, CFO, BUs, HR, PR, IR and others to understand and drive cyber risk management. The board has to understand the issue, buy in and make informed choices. Outside counsel who deeply understand security can work with you top to bottom to understand crown jewels, manage real security, translate law and technology for the board, limit litigation risk, contractually protect cyber assets and help lead teams to respond to incidents in real time. Cyber best practices like the new NIST Framework, and others, create methodologies to organize cyber management and substantiate the use of best practices. And, like other risks, cyber specific insurance can both help manage risk and drive good risk management practices.

Conclusion

The cyber issue is fundamentally global, here today, and will continue to grow as companies drive more innovation through the use of technology. Now is the time to drive leadership in cyber for the company. It is important, possible and fundamental for competitive advantage.

"Cyber is a team sport, internally and externally. You need representatives from counsel, CIO, CISO, CFO, BUs, HR, PR, IR and others to understand and drive cyber risk management."



Multinational Compliance in the Financial Services Industry

Key issues to consider when implementing global compliance programs and conducting investigations to enforce potential rule and regulation violations

Jonathan E. Green
Partner

Hartmut T. Renz
Counsel

Aaron F. Miner

Establishing an effective global compliance program

In recent years, particularly in the aftermath of the global financial crisis, the financial services industry has seen an unprecedented increase in regulatory demands. Amidst the economic recovery that is taking place, regulatory authorities in many countries are in the process of implementing stricter regulations in order to prevent another financial crisis. While these new and comprehensive regulations may provide the financial market with necessary certainty and stability, they also provide financial institutions operating in these markets with new challenges. Confronted with these challenges—not only within the European Union and the United States, but all around the world—financial institutions have begun to realize the growing importance of an effective compliance function in navigating through the maze of regulatory demands.

Within the financial sector, the meaning of the term "compliance" implies adherence to the laws, regulations, rules and standards applicable to the banking services provided in the financial markets. In the United States, it relates to compliance with all standards, not just those related to services. Failure to adhere to those standards can in turn expose the financial institution to various risks, including financial losses, reputational damage or sanctions by regulatory agencies. While initially the supervision of employee transactions and insider trading were the primary focus of the compliance function in Germany, today investor protection is gradually becoming the focus of attention.

In that regard, in order to ensure adherence to the applicable rules and regulations, the compliance function is assigned various responsibilities all over the world. While specific responsibilities differ depending on the country—although increasingly harmonized within the European Union—the following core responsibilities, which have been recognized by the Basel Committee on Banking Supervision, are to be found in some form in most jurisdictions.

First, the compliance function should be entrusted with the identification, assessment and measurement of risks. Second, the compliance function should advise the financial institution, particularly management, on compliance with the applicable rules and regulations and inform them about any changes. Third, the compliance function should be tasked with the education and guidance of the financial institution's employees. Fourth, the compliance function should monitorcompliance and the controls in place and test them for their effectiveness. Fifth, given that the financial institution's management will be responsible for any infringement of the applicable rules and regulations, the compliance function should also report—on a regular

basis—to management regarding the assessed risks, changes and developments in the applicable regulatory and legislative framework, any infringements and corrective measures, as well as any other compliance-related matters. In structuring a compliance program that incorporates the aforementioned responsibilities, firms should take into account, on a risk-based approach, the different compliance risks associated with particular tasks.

Today's compliance function plays four roles: First, compliance continues to serve in its traditional role of protecting the financial institution against potential financial or reputational losses has gradually expanded in today's complex financial services market. Second, the traditional role has expanded to include an advisory role, namely providing the institution and its employees with legal certainty regarding the applicable rules and regulations. Third, the compliance function plays a marketing role, viz. strengthening the relationship with, and trust of, the consumers as a component of increased fairness and transparency. Fourth, compliance has an innovative function, namely stimulating new practices and procedures within the financial institution.

The compliance function constitutes a vital part of any financial institution, especially multinational credit institutions which engage in cross-border activities and are subject to different legal systems and supervisory authorities. Not only does it ensure adherence to the applicable rules and laws regarding the provision of services and products within the financial markets and thereby help prevent financial and reputational losses, but the compliance function also helps strengthen consumer relations and stimulate innovation by helping the financial institution to navigate through today's rapidly growing and ever more complex regulatory landscape, be it in the United States with the Dodd-Frank Act, in Germany with the Securities Trading Act or in the European Union with the upcoming revised Markets in Financial Instruments Directive II.

Investigating and enforcing potential violations

An effective compliance program should include a mechanism for investigating and enforcing violations of internal policies and external regulations. Any such policy should have protocols for reviewing trading data, account information and electronic communications; interviewing employees and other potential witnesses; and formulating risk analyses and remediation plans. For multinational financial services firms with offices and affiliates around the world, investigations often take on cross-border dimensions. Such firms and their counsel should consider the following issues when planning and conducting cross-border investigations.

Understanding the legal system and social customs in each country in which a firm is conducting an investigation is critical to avoiding potential liability. U.S. and local law can differ in ways that materially affect an investigation, including the substantive law governing the fraud or misconduct at issue in the investigation; the laws protecting employees and whistleblowers; the degree of freedom a business has to investigate violations without involving local government authorities; and how to collect and use evidence.

A firm conducting an investigation involving the exterritorial application of a U.S. law such as the Foreign Corrupt Practices Act, for instance, should also consider whether the investigation implicates local law and how those laws differ. For example, criminal penalties can be imposed against corporate entities under U.S. law, but other countries' laws may provide for criminal liability only for natural persons. Such distinctions could create unexpected conflicts and affect a firm's approach to an investigation.

In the employment context, unlike in the United States, employees in some jurisdictions cannot be terminated or disciplined for failure to cooperate with an employer's investigation. In addition, some jurisdictions have a very narrow window of time—in some cases, just a few days—after an employer discovers evidence of wrongdoing during which it can use that evidence in support of a termination for good cause.

Firms should also understand that some jurisdictions' criminal procedure laws can limit, or even forbid, private parties from conducting investigations because such investigations are considered intrusions on the function of the government. Before initiating a cross-border investigation, it is important to identify any local procedural rules or customs that might restrict private internal investigations or require the involvement of local law enforcement.

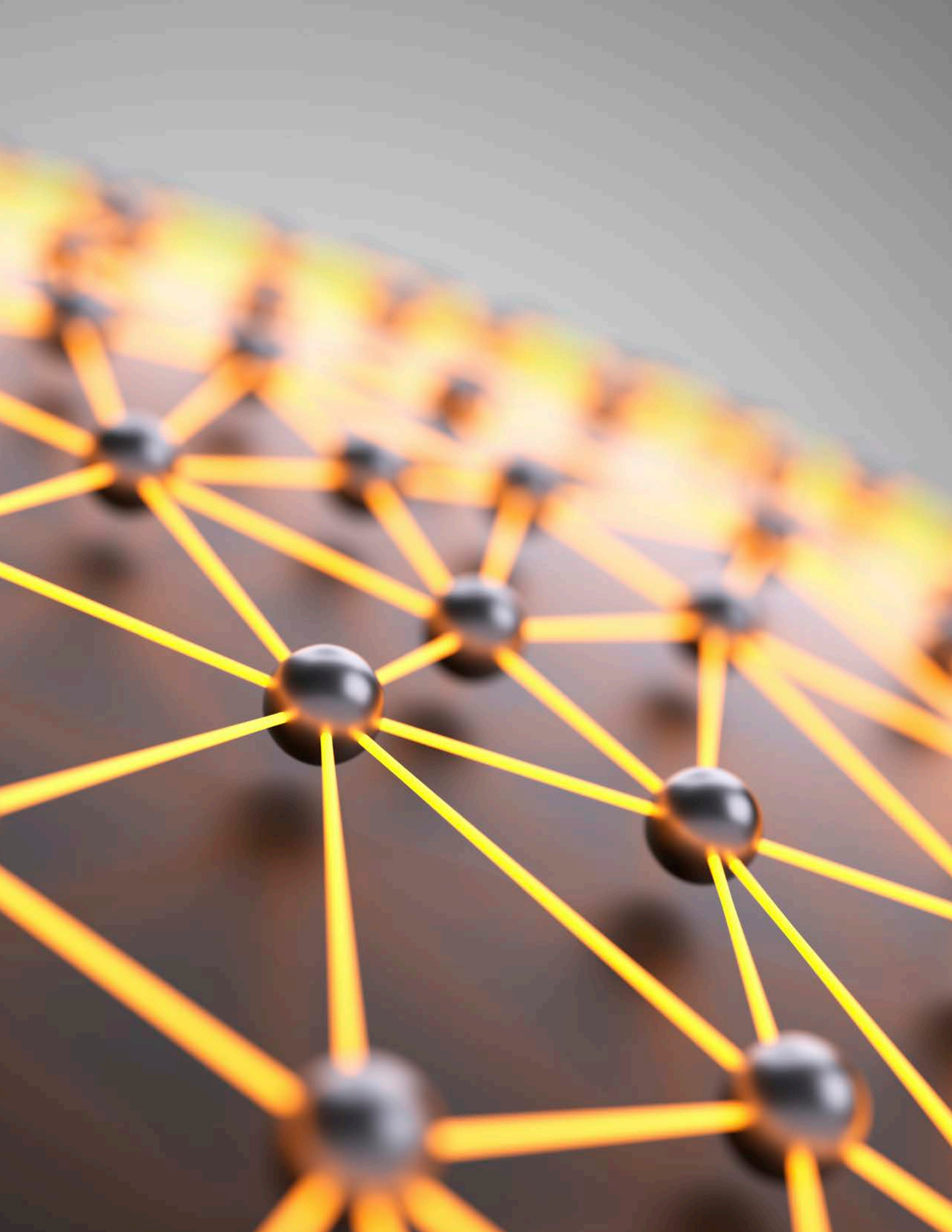
Multinational firms conducting cross-border investigations often need to access and transfer data back and forth between offices and affiliates in different jurisdictions. But in certain circumstances, that might trigger data protection or

privacy laws in regions like Europe, Asia or Latin America. For example, the European Union has adopted data protection laws that protect a broadly-defined category of "personal data" from being "processed" (a broadly defined term) unless the individual whose information is at issue consents, the data is necessary for the performance of a contract with the individual, it is necessary to comply with local legal obligations, or the legitimate interests of the entity collecting the information outweigh the individual's privacy interests.

Some jurisdictions have also enacted "blocking statutes," which criminalize the exportation of certain categories of information. For example, Switzerland's well-known bank secrecy law prohibits banks from disclosing bank account information, and China's state secrets law imposes severe penalties for disclosing information relating to "state security and national interests," which could be construed expansively.

Finally, U.S. lawyers routinely rely on the attorney-client privilege to prevent employee interviews and other investigative communications from being disclosed. But the relatively robust attorney-client protections recognized under U.S. law may not apply to investigations in other jurisdictions. Some jurisdictions—China, for example—do not recognize the attorney-client privilege at all. Other jurisdictions may recognize a privilege, but it may not apply to U.S.-licensed lawyers or in-house counsel.

These are only some of the key issues multinational financial services firms should consider when implementing global compliance programs and conducting investigations to enforce potential violations of the applicable rules and regulations. It is important that such firms understand the legal and regulatory framework in the jurisdictions in which they are operating in order to reduce potential risks and strengthen business operations.



Antitrust Division Renews Emphasis on Compliance Programs

Effective compliance programs are high on its agenda, and given the opportunity, the Division will seek monitors with increasing frequency

Philip Giordano
Counsel

Dr. Sebastian Jungermann
Partner

Robert Bell

The Antitrust Division is charting a course for more robust corporate antitrust compliance programs in 2015. Taking advantage of its win last year in U.S. v. AU Optronics Corp., in which it imposed a court-appointed monitor on a convicted cartelist for the first time, the Division made a point of wrapping up the year with two policy speeches setting forth its expectations. Though in keeping with past Division policies, the speeches made clear that effective compliance programs are high on its agenda, and that given the opportunity, the Division will seek monitors with increasing frequency. Investment in sound compliance policies are particularly important in today's enforcement climate, and given the expense and intrusiveness of compliance monitors, companies in the United States and abroad should pay close attention to guidance about how to avoid them.

In a speech at the Georgetown University Law Center Global Antitrust Enforcement Symposium, Assistant Attorney General Bill Baer explained that the Division sought probation and a monitor in the AU Optronics case because the company, a Taiwanese corporation, and its U.S. subsidiary demonstrated a lack of commitment to implementing an effective compliance program. Despite its conviction, the company refused to acknowledge the illegality of its conduct, and it refused to remove convicted and indicted senior executives from positions of responsibility. Under the circumstances, a court-supervised monitor was therefore necessary to change the corporate culture and reduce the risk recidivism.

In comments before the International Chamber of Commerce and United States Council of International Business, Deputy Assistant Attorney General Brent Snyder said that, in keeping with longstanding departmental policy, the Division would not require termination of culpable executives. However, Snyder observed that retention of "culpable employees in positions where they can repeat their conduct, impede a company's internal investigation and cooperation, or influence employees who may be called up to testify against them" would raise significant doubt about a company's commitment to effective antitrust compliance.

Snyder cautioned that the Division would seek probation in cases where a company does not have a compliance program or makes no effort to strengthen a preexisting compliance program. He added that companies may be able to avoid probation by adopting or strengthening a

"If culpable, a company may face the choice between stripping its culpable executives of such authority or having a compliance monitor do it."

compliance program while under investigation.

The Division also typically seeks probation for recidivists, as it did in its April 2014 plea agreement with Bridgestone Corp. Bridgestone admitted to fixing the price of automotive anti-vibration rubber parts in 2014; only three years previously, it had pled guilty to fixing the price of marine hose. Under the terms of its probation, Bridgestone must report on its antitrust compliance program to a probation officer and the Antitrust Division annually for three years. If Bridgestone fails to make timely and complete reports, the Division may seek a court-appointed monitor.

But even when the Division seeks probation, it typically allows a company to design and implement its own compliance program, within general guidelines. Snyder emphasized that the Division will not provide such autonomy to companies that refuse to remove culpable executives from positions of authority. Instead, the Division will seek to impose a compliance monitor to oversee the adoption of an effective compliance program. In the case of AU Optronics, the Division specified that its compliance program prohibited indicted executives from holding any pricing, sales or marketing authority. In practice, then, if culpable, a company may face the choice between stripping its culpable executives of such authority or having a compliance monitor do it.

Snyder refuted the charge that the Antitrust Division does not adequately reward companies for antitrust compliance programs already in place before unlawful conduct is discovered. In the Division's view, such preexisting programs are by definition ineffective if they fail to prevent cartel conduct or fail to detect it early. Therefore, the Division rarely recommends credit at sentencing for such programs, much less allows a target to avoid charges. Snyder observed that the benefit of an effective compliance program is that it prevents unlawful conduct in the first place, or uncovers the conduct in time for the company to enter the Division's leniency program. In his view, "receiving leniency is the ultimate credit for having an effective compliance program." He also stated that the Division was actively considering ways to credit companies that proactively adopt or strengthen compliance programs after coming under investigation. But he did not provide any details, and to date the Division has not provided any company with such credit.

Snyder summarized the elements of an effective antitrust compliance program as including:

- The full support and active involvement of senior executives and the board of directors
- Training for all executives and managers, and all relevant employees
- A means for any member of the organization to report suspected criminal violations anonymously without fear of retaliation
- Regular monitoring and auditing of risky activities
- Regular evaluation of the compliance program itself
- Improving the compliance program when it fails to detect wrongdoing
- Disciplinary action for employees who commit antitrust crimes

The Division's message is clear: At the end of the day, an antitrust compliance program is only as good as the executives that establish and nurture it. Through example and leadership, senior executives shape a company's compliance culture. If they cannot or will not, they must step aside. In Snyder's words, "It starts at the top."

Out of the Tunnel and Into the Light: Emerging from a Compliance Failure

Attention to the company culture is a must following a compliance failure

Z Scott
Co-Chair, White Collar Litigation and Internal Investigations Practice

Laura Shores
Partner

Saul P. Morgenstern
Chair, Antitrust Practice

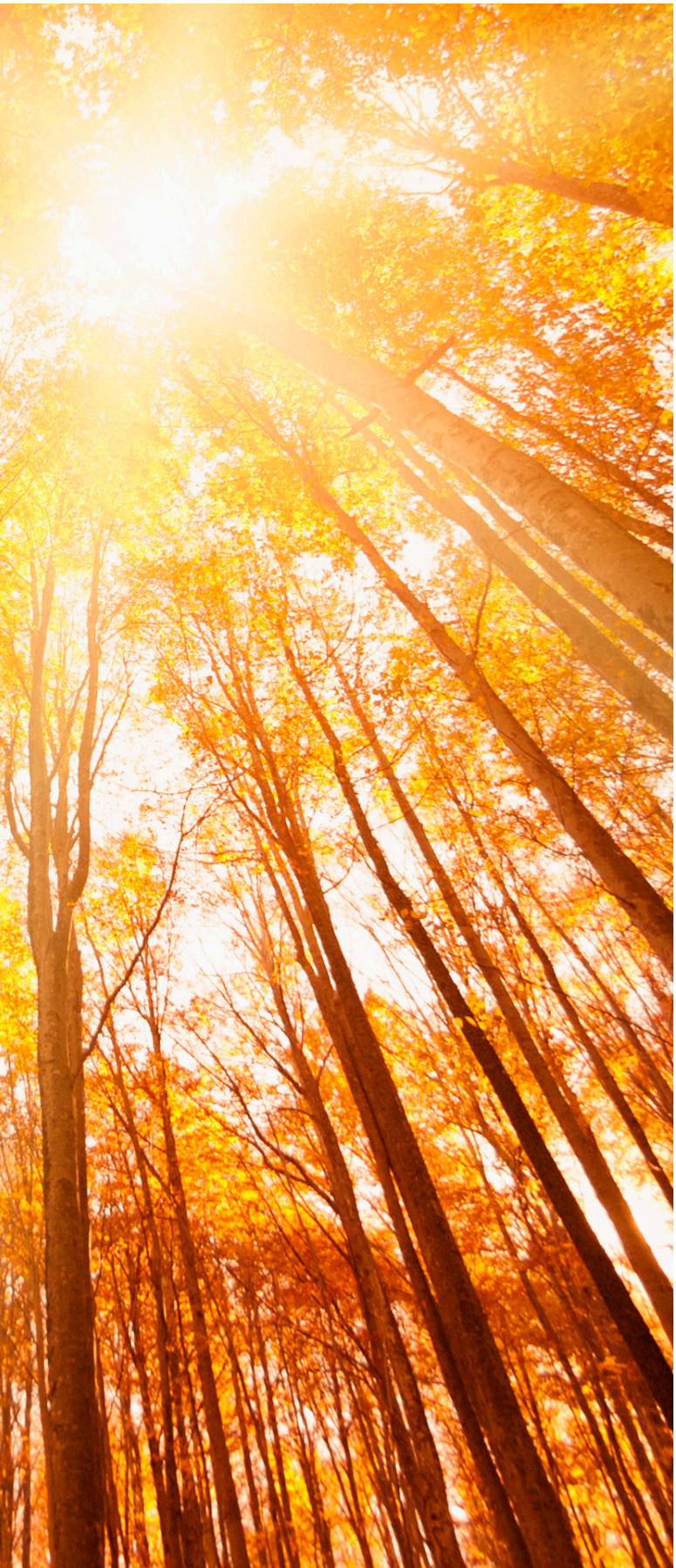
In December 2008, the U.S. Department of Justice (DOJ) and German regulators announced a $1.6 billion settlement in the Siemens case, $450 million of which was paid to DOJ, blowing all prior records in foreign bribery prosecutions. In the years that followed this settlement, the company conducted a very public overhaul of its management structure and global compliance organization. Those efforts involved a number of significant changes to Siemens' operations, aimed at reinforcing throughout the company's, board's and management's determination to operate the business in an ethical and compliant manner. It has since been reported that Siemens is more profitable than it was before, suggesting that investing in and communicating a strong compliance culture does not hurt profitability and may, by enhancing corporate reputation and employee morale, improve it.

For many corporations' board members and managements, the Siemens bribery prosecution was a "let's get serious" moment. Some initiated formal assessments of the risk of a similar crisis occurring within their own organizations. Many learned from that effort that it takes more than instituting complex compliance structures to address compliance risk. To prevent compliance failures, a company must be prepared to change the culture and ensure that company employees are properly focused on doing business with ethics and integrity. According to Siemens' chief executive, "[o]perational excellence and ethical behavior are not a contradiction of terms. We must get the best business—and the clean business."

Where does a company start after a significant compliance failure? An independent and thorough investigation, in many instances, will provide a roadmap for correction by identifying rogue employees, failed internal controls and risks. But there is scant reason to think that a company and its employees will automatically learn from past mistakes. An overhaul of its business and compliance processes may be required, and attention to the culture is a must.

Top down and bottom up

To begin the process of recovery, a corporate board and senior executives must set a strong "tone at the top." This is critical in a weak global economy and a push for business in emerging markets where conduct is often governed by different legal standards. In this regard, senior management's perceived and continued tolerance for misconduct can be devastating. A recent example involves a large U.S. retailer who, despite allegations that a division CEO was the key architect of a foreign bribery scheme, reportedly publicly extolled his virtues and gave him a promotion.



"Top" means very top: the board of directors. The U.S. Federal Sentencing Guidelines requires boards to exercise reasonable oversight in connection with the implementation and effectiveness of the organization's compliance and ethics program. The Delaware Chancery Court's opinion in *In re Caremark International Inc. Derivative Litigation* confirmed a board's fiduciary duty to oversee a corporate compliance program.

It is equally important to foster a culture and practice of listening to what is being said by rank and file employees. A staggering percentage of whistleblowers say that they reported suspected violations internally before going to the government. An effective system must be designed to ensure that complaints are heard and properly vetted.

Implement a strong compliance structure

Over the years, government regulators have made known their views about the components of an effective program. For example, according to prosecutors, one of Siemens' essential modifications was to shift control and accountability for compliance to a chief compliance officer who reports directly to the general counsel and the chief executive officer. Any company serious about compliance that does not have a chief compliance officer should have one. Assuring that the chief compliance officer has the clear ability to report to the CEO and the board is equally important. Moreover, the compliance function in a major corporation, particularly one with global scope or ambitions, is not a one-person job. It is critical that sufficient resources, at headquarters and on the ground in subsidiaries and distant operations, have local compliance presence with clear communication lines to the chief compliance officer.

The U.S. Federal Sentencing Guidelines provide useful insight into what the U.S. government expects. Under these guidelines, to have an effective ethics and compliance program, an organization must act to prevent crime and promote an organizational culture that encourages lawful behavior. If a company is prosecuted, the severity of the potential penalty can be reduced if an effective compliance program was in place at the time of the misconduct.

Following the Sentencing Guidelines, other regulatory bodies have issued written guidance describing effective compliance programs and policies. However, it is not enough to have policies and a program. The FCPA Resource Guide jointly published by the U.S. Securities and Exchange

Commission and the DOJ notes that:

A well-designed compliance program that is not enforced in good faith, such as when corporate management explicitly or implicitly encourages employees to engage in misconduct to achieve business objectives, will be ineffective. DOJ and SEC have often encountered companies with compliance programs that are strong on paper but that nevertheless have significant FCPA violations because management has failed to effectively implement the program even in the face of obvious signs of corruption.

A recent case in the Northern District of California federal court illustrates the point. Following a conviction on antitrust offenses, a federal judge sentenced AU Optronics (AUO), a Taiwan-based corporation, to three years' probation and imposed a $500 million fine. As part of the sentence, the court required that AUO "develop, adopt and implement an effective compliance and ethics program." The government recently accused AUO of violating the court's directive. The government cited the company's failure to hire a chief antitrust compliance officer and its board of directors' failure to exercise the appropriate oversight over antitrust compliance. A hearing is currently scheduled for May 29.

AUO's alleged compliance failures should be contrasted with Siemens' successful implementation of its program. Based on the Siemens' efforts, as documented by a corporate monitor, the government concluded that the company had complied with the requirements of its plea agreement and its final judgment in the SEC civil action.

Training is key

It is not uncommon for companies experiencing a compliance failure to have had a training program in place. The failure is often perceived to suggest some deficiency in the program. Distributing an ethics policy, or even having periodic general lectures on compliance, is unlikely to create either a compliance culture or a sufficiently educated workforce. It is also unlikely to impress prosecutors in the event of a compliance failure.

> "The compliance function in a major corporation, particularly one with global scope or ambitions, is not a one-person job. It is critical that sufficient resources, at headquarters and on the ground in subsidiaries and distant operations, have local compliance presence with clear communication lines to the chief compliance officer."

In addition to straightforward explanations of the types of prohibited and expected conduct, employees should be given information designed to help them understand the reasons behind the compliance policy. Such training should also be tailored to the employees' functions; "cookie cutter" web-based training will not suffice. For individuals in high risk positions, in-person training is ideal.

Conclusion

A compliance failure is likely to be expensive, even if the government does not pursue enforcement action. The money is not all wasted if the company takes the "opportunit[y] that comes from a good crisis" to invest in a stronger compliance function that is better suited to the company's specific business and culture, as well as today's ever-changing conditions. Effective leadership, clearly articulated standards, robust employee education and user-friendly reporting lines might make the difference in the future between reporting questionable conduct by a colleague or external contact and ignoring or, worse, concealing it.

Contributors

Amy Conway-Hatcher
Partner
amy.conway-hatcher@kayescholer.com
+1 202 682 3530

Emily Newhouse Dillingham
Associate
emily.dillingham@kayescholer.com
+1 312 583 2435

Philip A. Giordano
Counsel
philip.giordano@kayescholer.com
+1 202 682 3546 | +1 650 319 4530

Adam Golodner
Leader, Global Cybersecurity & Privacy Group
adam.golodner@kayescholer.com
+1 202 682 3575

Jonathan E. Green
Partner
jonathan.green@kayescholer.com
+1 212 836 8478

Dr. Sebastian Jungermann
Partner
sebastian.jungermann@kayescholer.com
+49 69 25494 300

Aaron F. Miner
Associate
aaron.miner@kayescholer.com
+1 212 836 7123

Saul P. Morgenstern
Chair, Antitrust Practice
saul.morgenstern@kayescholer.com
+1 212 836 7210

Tiffany R. Moseley
Partner
tiffany.moseley@kayescholer.com
+1 202 682 3518

Hartmut T. Renz
Counsel
hartmut.renz@kayescholer.com
+49 69 25494 230

Alan Salpeter
Special Counsel
alan.salpeter@kayescholer.com
+1 312 583 2450

Z Scott
Co-Chair, White Collar Litigation and Internal Investigations Practice
z.scott@kayescholer.com
+1 312 583 2347

Laura Shores
Partner
laura.shores@kayescholer.com
+1 202 682 3577

Kaye Scholer at a Glance

1917	400	120	9	75
Year Founded	Lawyers	Partners	Offices	Practice Rankings— *U.S. News & World Report/ Best Lawyers* 2015

Chicago
Frankfurt
London
Los Angeles
New York
Shanghai
Silicon Valley
Washington, DC
West Palm Beach

www.kayescholer.com