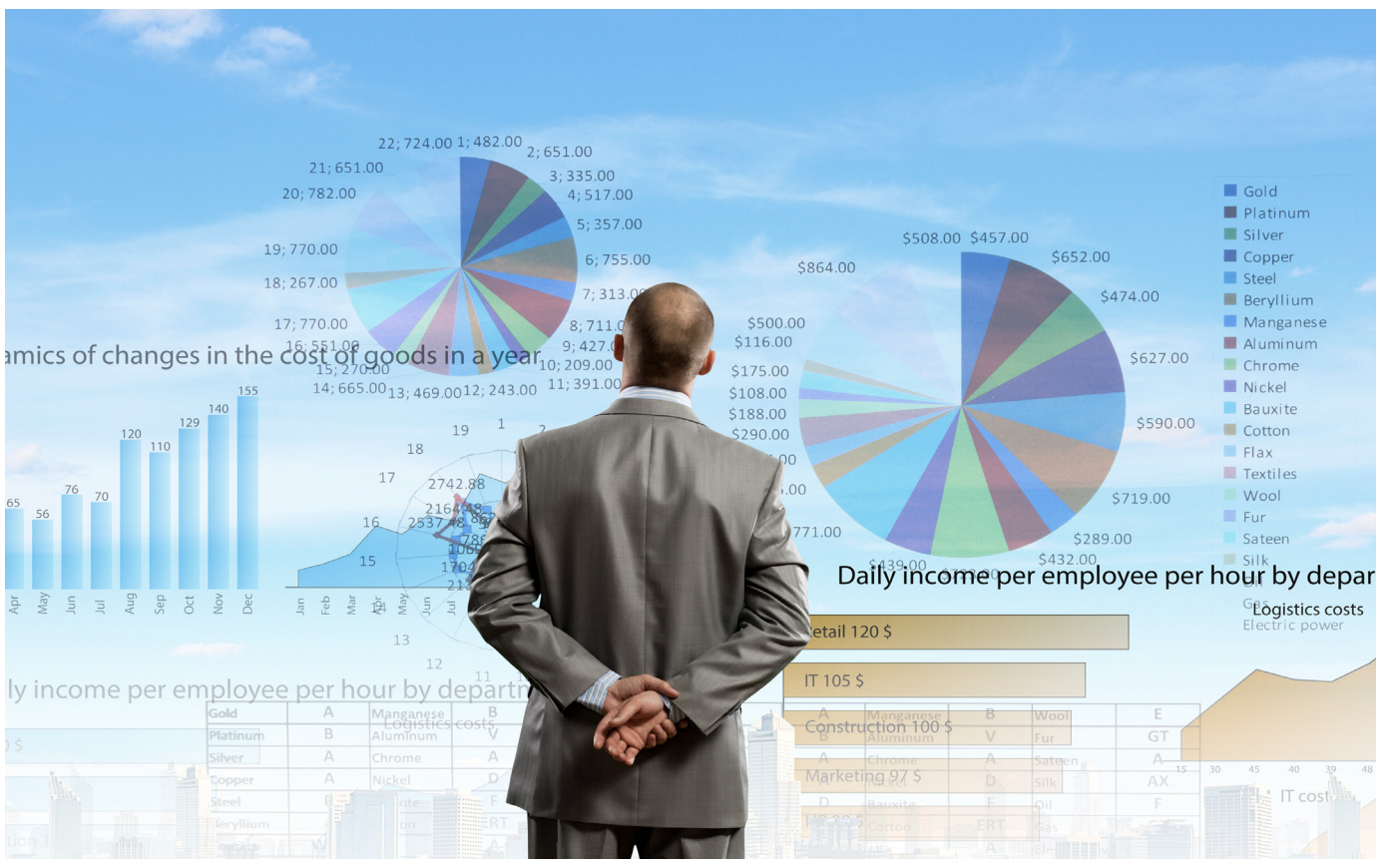
In-House Counsel



Bigstock

Use **Big Data** to Spot Issues Before They Become **FCPA Problems**

BY GABRIELA P. BARON

Over the course of four years, between 2007 and 2011, a general manager at a small African tire company in Kenya, a recently acquired subsidiary of a much larger U.S.-based organization, tries to increase sales. To do so, he writes checks to cash, lists the checks in the company's check register as legitimate business expenses, and gives the money to local authorities and employees of government-owned and private sector companies.

Meanwhile, at another of the company's subsidiaries in Angola, a manager marks up the cost of its tires. When others look at the records, the additional charges seem to be attributable to the rising cost of freight and increased customs clearing fees. Though initially denoted in records as payments to vendors, the manager later reclassified them to a balance sheet account and paid them out to employees of customers to encourage them to give the company more business.

All told, these facts amounted to $3.2 million in bribes and led to a $16 million penalty against the Goodyear Rubber & Tire Co. for violations of the Foreign Corrupt Practices Act (FCPA)[1] earlier this year. Why was the penalty so low, especially following a year when the average corporate penalty for FCPA violations reached a new record? The penalty was mitigated by the fact that although the company initially failed to detect or prevent these payments (it did not conduct adequate due diligence when it acquired the subsidiaries and thereafter failed to "implement adequate FCPA compliance training and controls"[2]) it did take several effective measures to comply with the law and self-reported the incidents to the U.S. Securities and Exchange Commission (SEC).

The company's internal controls worked: Whistleblowing employees alerted Goodyear's corporate office to the violations. Goodyear investigated the matter, put a stop to the improper payments, and reported them promptly. The company then adopted a cooperative posture during the investigation, divested the subsidiaries, and disciplined the employees responsible for oversight of the subsidiaries. Further, it added several new features to its compliance program, including expanded training initiatives, more regular audits of its subsidiaries, quarterly self-assessments and management certifications from its subsidiaries, and annual testing of its internal controls. Goodyear also implemented a new third-party due diligence software tool. As a result of these efforts, Goodyear avoided criminal liability and civil penalties, aside from the disgorgement of profits that resulted from the illegal bribes and an interest payment.[3]

> With an even more robust, data-driven compliance program in place, under the direction of the legal team, **organizations can spot the indicia of FCPA transgressions even earlier.**

There is plenty to learn from Goodyear's example: the company did a number of things right, once it discovered the wrongdoing. But, with an even more robust, data-driven compliance program in place, under the direction of the legal team, organizations can spot the indicia of FCPA transgressions even earlier. In short, organizations have a clear choice: They can continue to rely on the backward-looking detection methods of old, or they can follow the lead of the legal team and transform into a forward-looking culture of compliance that addresses emerging enterprise risks by studying data and identifying (and investigating) risky behaviors before they become full-blown fires.

A Renewed Focus on Regulatory Compliance. When the FCPA was enacted in 1977, organizations were limited in their ability to construct methods of compliance. For many years, that did not matter, as enforcement actions were largely dormant. With little guidance from the government and little threat of penalties, many organizations relied then—and many still today—on tools such as codes of conduct, dedicated fraud teams, hotlines, and external audits. However, these tools are retroactive, which means they only kick in when problems are discovered, allowing fraudulent activity to fester unchecked.

Over the last few years, the government has begun to focus more heavily on antibribery and anticorruption enforcement. In 2012, the SEC and DOJ published A Resource Guide to the U.S. Foreign Corrupt Practices Act, which recommended that organizations implement a strong compliance program.[4] Such a program must do more than check the boxes to satisfy the government; rather, it should help "prevent, detect, remediate, and report misconduct." The key elements of an effective program include the following:

- whether there is commitment from senior management and a clearly articulated policy against corruption;
- whether the company has a code of conduct and compliance policies and procedures;
- whether a company has assigned responsibility for the oversight and implementation of its compliance program to one or more specific senior executives;
- whether it has a risk-based assessment plan;
- whether it provides training and continuing advice;
- whether it offers positive incentives to drive compliant behavior as well as adequate disciplinary measures to deter bad actors;
- whether it conducts due diligence on third parties and payments to them;
- whether it allows employees to make confidential reports of suspected misconduct and has an effective internal investigation strategy; and
- whether it has a continuous improvement strategy.

The Guide makes clear that it expects organizations to devote more resources to the highest areas of risk—an obligation that requires organizations to use data to mine for vulnerabilities—the red flags that the Guide identifies. For third-party relationships, those red flags include excessive commissions, unreasonable discounts, vague "consulting" agreements, mismatches between the business of the consultant and the business engagement, » Page 13

GABRIELA P. BARON *is senior vice president at Xerox Litigation Services in New York, where she oversees global business development activities and major client accounts.*

Navigating State-Based **Ethics Rules** And **Sarbanes-Oxley Requirements**

BY C. EVAN STEWART

Do corporate lawyers have obligations to rat out clients to the U.S. Securities and Exchange Commission? Many believe the SEC requires this result. Is that right? What if state-based ethics rules mandate the opposite? What is a lawyer to do?

For a number of years, I have been predicting a test case/showdown between lawyers who follow the dictates of the states in which they are licensed to practice law *versus* the conflicting dictates of the rules and regulations promulgated by the U.S. Securities and Exchange Commission after Congress passed the Sarbanes-Oxley Act of 2002.[1] The contrast between the two regimes can be pretty dramatic. Under the SEC's way of doing things, a capital markets lawyer *may* disclose "material violations" (past, current, future) to the Commission. If a lawyer does not handle that "permissive" disclosure obligation correctly, she can be subject to a liability whipsaw: If you fail to disclose to the SEC and you are wrong, the SEC (and possibly the plaintiffs' bar) can go after you; if you disclose to the SEC and you are wrong, clients and stockholders can sue you. In judging the appropriateness of your conduct, the SEC (with the benefit of hindsight) will judge you under the "reasonable lawyer" standard; and the Commission has at its disposal the full panoply of sanctions under the Securities and Exchange Act of 1934 to punish the offending lawyer.

> Well aware of the **conflict** between its rules and regulations and the ethical rules of several states, the SEC has taken the view that there is **federal preemption** of conflicting states' ethics rules. So, will the SEC's position prevail if and when tested?

While a number of the states have *generally* come into line with the SEC's "permissive" disclosure mandate, a number of others have not.[2] Besides Washington and California,[3] another principal outlier is New York. Under New York's Rule 1.6, New York lawyers *may* use their discretion to make permissive disclosure (1) to prevent death or substantial bodily harm, or (2) to prevent a crime. New York specifically carves out *financial fraud* from per- » Page 12

C. EVAN STEWART *is a partner at Cohen & Gresser.*

Those Were the Days

Heed advice from a lawyer who has been there and back.

BY ALAN BEHR

You did it. You are free! All those years of working in a law firm, and you have turned the corner at last, securing a hard-to-get in-house job.

Gone is that frustration as you stared at the computer screen that forced you to account for each minute of your professional life with an exactitude that everyone knew was nonsense but all had to pretend to believe. Gone is the up-or-out partner track, the next phase of which was not really to be a partner in the sense of a business owner but a non-equity partner, in the sense of a salaried employee who has to pay an accountant to mine the veins of the firm's K-1 during each tax season. Gone as well is the recognition that, if you do not eventually shift your career focus from the practice of law to the marketing and sale of legal services largely performed by others, you will be in a delicate and vulnerable position. Three years of law school and a decade or two of practice, only to end up in sales and business administration? That's a career path for someone with a professional degree and license?

So good-bye to all that and welcome to the corporate world. First, a word about corporate organization:

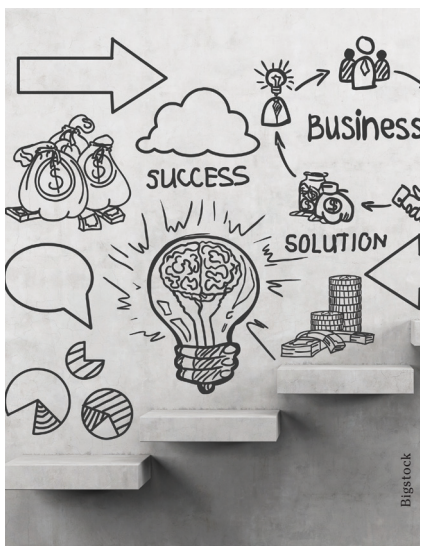
That law firm you left behind was structured something like a teaching hospital, with a large division between the staff and the professionals in terms of both income and responsibility.

In between within law firms stands a small cadre of middle managers (human resources, business development, accounting, etc.), but basically, you are either a bright star (lawyer) or the planet orbiting the star (assistant, paralegal), often not fully aware of what the lawyers, who are ever in such a blazing hurry, really need or why. And all of those stars do essentially the same thing. Of course, attorneys concentrate in different fields of practice, and transactional lawyers tend to behave differently than do litigators, but in the end, it is all about rights, remedies and legal results, and at the core is everything taught in law school. And those equity partners: Did you really head straight from law school, fresh with the sea-breeze enthusiasm of youth—and perhaps burdened by debt—only to go work in a business (for that is what law firms truly are) where an owner sat in every third office, ruminating over your job performance with each memorandum you wrote?

What made you so special in the law firm and that made those partners take a chance on you fresh from school (if it was your first job) was not your self-evident brilliance, your good looks, your boulevardier style, or your Shavian wit. It was that you could quickly be turned into a profit center. The work you did was the very thing that the organization needed to deliver in order to make money. As an associate, if you did enough work—selling your labor to the firm wholesale so that it could mark it up to retail for its clients—you were profitable; as long as you stayed above the mean on the learning curve, all goodness and reward flowed pretty much from that fact alone. As you saw first-hand, there is nothing better liked and more appreciated in a commercial enterprise than its profit center.

Now that you are in-house, guess what? Counselor, you are still a member of the bar, but from a business point of view, you are now overhead, and there is nothing appreciated less in a commercial enterprise—indeed, nothing resented more—than overhead. You are going to have to justify your presence in the organization in a very different way from now on.

To do that, you have to be aware of another fundamental difference: In-house attorneys practice law within an organization that does something altogether different from the practice of law. What lawyers do is likely not well-understood, sometimes not appreciated, and occasionally viewed as an annoyance. Those intermediate grades of managers who were all but non-existent in the law firm? They are everywhere now, and many of them are your "clients" within the company. The fun part is that you finally get to expand your sphere of work contacts and can regularly associate with people whose skills and contributions are different from your own: There are marketers, financial people, researchers, production people, vendor support people, building and grounds administration people, and many more holders of non-legal jobs and specialties within jobs. It makes for a much more interesting work environment to be with co-workers who do so many different things than to have lunch and meetings with attorney after attorney who has little more to talk about on the topic of work than what it is that you are already doing.



Bigstock

> In-house attorneys practice law within an organization that does **something altogether different from the practice of law.**

In the layered and diverse corporate environment, you have to learn as well to deal with people with different levels of education and different career tracks. You have to extend yourself to understand what they do in order to serve them. You have to learn quickly, in short, how to talk to important people who may not have advanced degrees and to those others who simply do not know or perhaps do not care to know why your counsel should be followed.

That, in turn, adds up to something else that a lean organization such as a law firm, where all the professionals are contributing directly to the bottom line, does not produce much of relative to its revenues: politics. The devil does find work for idle hands, and he does as well find mischief to occupy nimble » Page 13

ALAN BEHR *is a partner in Phillips Nizer's corporate and business law department and intellectual property practice, and chairman of the fashion practice.*

Inside

Bank Examination Privilege Presents a **Moving Target** for Counsel

BY TRAVIS P. NELSON AND STEVEN COOPER

In the current banking environment, where private civil litigation is frequently brought simultaneously with, or very closely following, regulatory investigations and enforcement actions, it is crucial for banks to know whether and how communications with federal and state regulators may be used against them in parallel or subsequent proceedings.

The article will discuss the nature of the bank examination privilege generally, who holds and who may invoke the privilege, the scope of the privilege, how to respond to document requests that seek privileged information, and how the privilege has been challenged and defenses to challenge.

Federal and state bank regulators, such as the Office of the Comptroller of the Currency (OCC) at the federal level, and the New York Department of Financial Services (NYDFS) at the state level, during the course of their examinations of regulated banks, generate highly detailed and highly sensitive documents. For example, following an examination of a financial institution (which is similar to an audit), the regulators will issue a report of examination, or ROE. This document is a very candid and sometimes very critical assessment of the financial and managerial performance of the institution. Through the examination process, institutions are assigned ratings in what are called "CAMELS" categories, which stands for Capital, Assets, Management, Earnings, Liquidity, and Sensitivity to Market Risk. The institution receives a rating for each of these areas, as well as a composite rating for overall performance. The institution may also undergo "targeted" examinations, which review the institution's performance in a discrete area, such as compliance with the Bank Secrecy Act/anti-money laundering laws, the Community Reinvestment Act, or fair lending laws. In some cases, the targeted examination may not relate to a specific law but rather to an issue or product line. Still in other cases, the agencies may conduct a "horizontal" examination, wherein the agencies will examine multiple banks on a specific issue of concern.

In addition to ROEs, the agencies will issue less formal written evaluations of supervised institutions. For example, a regulator may issue a "Supervisory Letter" to the institution identifying areas of concern. Regardless of the type, virtually all correspondence requires some written response from the institution that details how the institution's board and management will act to address the regulator's concerns.

It is important to note that the bank examination privilege not only covers materials generated by the regulator, but also "banks' responses thereto."[1] A Pennsylvania federal court put this point succinctly:

> Plainly, to prohibit disclosure only of those materials generated by the [federal regulator] as a result of the examination while allowing discovery of responsive documents prepared by the financial institution would circumvent the objective of the regulation—to protect the confidentiality of the examination process.[2]

The bank examination privilege exists at both the federal and state levels.[3] "Stated broadly, the bank examination privilege is a qualified privilege that protects communications between banks and their examiners in order to preserve absolute candor essential to the effective supervision of banks."[4] "It arises out of the practical need for openness and honesty between bank examiners and the banks they regulate, and is intended to protect the integrity of the regulatory process by privileging such communications."[5]

Unlike other privileges raised in discovery, which may be asserted by the party responding to the discovery request, the bank examination privilege belongs solely to the bank regulatory agencies. The bank examination privilege "may not be asserted by third parties on behalf of the bank agencies."[6] Where a claim of privilege is appropriate, the bank regulatory agency that owns the privilege must be allowed the opportunity to assert the privilege and the opportunity to defend its assertion.[7] The agency asserting the privilege has the burden of establishing its applicability to the documents at issue.[8] Some courts have held that this burden includes demonstrating that the materials are deliberative rather than factual, and that the deliberative portions cannot be redacted from the documents.[9] Purely factual material falls outside the privilege, whereas opinions and deliberative processes do not.[10]

> It is important to note that the **bank examination privilege** not only covers materials generated by the regulator, but also "banks' responses thereto."

In terms of responding to requests for materials that may be subject to the bank examination privilege, while the regulators own the privilege and technically are the only ones with standing to assert the privilege in court, an institution receiving a request from a private plaintiff for materials that are subject to the bank examination privilege can respond in very much the same way that it would respond to any other request for materials that are subject to other privileges, such as the attorney-client privilege. The institution should decline to produce the privileged materials, and note the non-disclosure on the privilege log citing "Bank Examination Privilege" or the relevant provision of the applicable statute or regulation on non-disclosure of examination materials.[11] The institution would then contact the relevant agency informing the regulators that a private litigant has requested potentially privileged materials.

If the documents requested fall within the privilege, i.e., the documents relate to examiners' opinions, a court can override the privilege if the requesting party demonstrates "good cause," because "even with respect to opinions and recommendations, the privilege is not absolute: The privilege is a discretionary one that depends on ad hoc considerations of competing policy claims."[12] "The privilege may be defeated where necessary to promote the paramount interest of the Government in having justice done between litigants, … or to shed light on alleged government malfeasance, … or in other circumstances when the public's interest in effective government would be furthered by disclosure."[13]

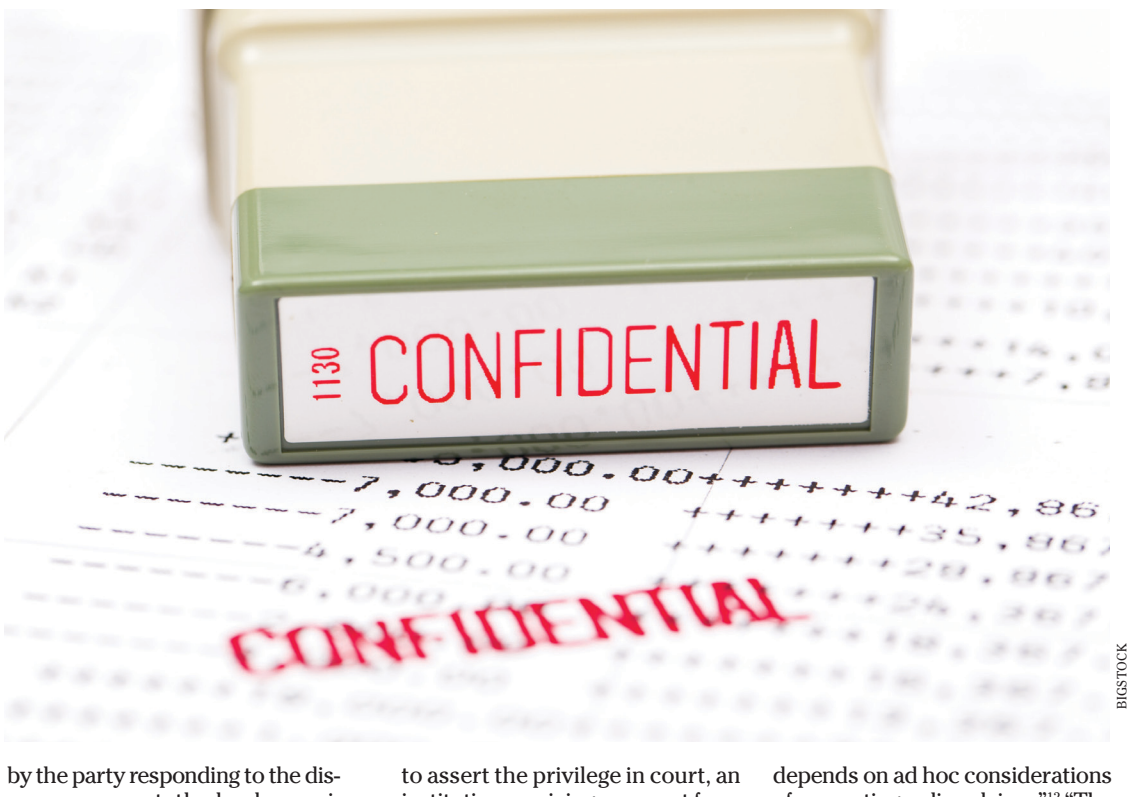
In order to evaluate claims of "good cause," courts "balance the competing interests of the party seeking the documents and those of the government," taking into account several factors. These factors are: (1) the relevance of the evidence sought to be protected; (2) the availability of other evidence; (3) the "seriousness" of the litigation and the issues involved; (4) the role of the government in the litigation; and (5) the possibility of future timidity by government employees who will be forced to recognize that their secrets are violable.[14] "The performance of this balancing of interests may require examination of disputed documents in camera."[15] "Redaction and a protective order may be appropriate to ensure that sensitive information, particularly with regard to third parties, is not unnecessarily disclosed."[16]

Private litigants have repeatedly attempted to overcome the bank examination using the above-referenced balancing test. For example, in *Wultz v. Bank of China*, the plaintiffs served the OCC with a subpoena duces tecum requesting a broad range of documents related to the OCC's enforcement actions against a regulated institution, including various investigative files and regulatory communications. The OCC argued that the entirety of its ROEs were subject to the bank examination privilege. The U.S. District Court for the Southern District disagreed, instead agreeing with prior New York federal courts that have ruled that the factual portions of the ROEs are not privileged. Additionally, as to the non-factual elements, the court evaluated whether there exists "good cause" to override the OCC's interest in asserting the privilege. Specifically, the plaintiffs argued "that banks are required by law to cooperate with their regulators, and banks willing to take the risk of withholding relevant information are unlikely to be swayed by whether their communication with the examiner is privileged as opposed to merely confidential; that a protective order is sufficient to protect the government's legitimate interests in confidentiality; and that permitting [the regulated bank] to avoid discovery would create a perverse incentive for financial institutions to voluntarily submit documents to the OCC just to avoid discovery in private litigation."[17] The court agreed with the plaintiffs and ordered the OCC to produce the non-factual materials from the examination.

While plaintiff's attorneys might attempt to rely on *Wultz* as compelling precedent for overriding the bank examination privilege in the Southern District, its facts make it plainly distinguishable from most cases where the bank examination privilege arises. Specifically, as to the "seriousness" of the litigation and the issues involved, Judge Shira Scheindlin stated:

> With regard to the seriousness of the litigation and the role of the government, I have already ruled that this case implicates the interest of the United States in depriving international terrorist organizations of funding that could be used to kill American

» Page 12



BIGSTOCK

TRAVIS P. NELSON *is a counsel at Reed Smith in New York, where he practices in the financial services regulatory group.* STEVEN COOPER *is a partner in the firm's commercial litigation group.*

Big Enough For Your **Breaches**?

Be diligent with cyber risk management and insurance issues as data security perils shift.

BIGSTOCK

BY JOSHUA GOLD

Data security breaches are now legion. Cyber attacks often prove to be multifaceted, resulting in fraudulent transactions, class action litigation,[1] identity theft, liability for regulatory actions, and a slew of other disruptions and damages to business operations. It has become clear that hackers can easily cause liability and losses to even the most well-prepared businesses.

To date, the risk management emphasis has largely been dedicated to addressing potential third-party liability threats. Many companies have focused their efforts on buying cyber insurance to protect against a future privacy rights class action litigation, regulatory investigation, or responsibility for credit card assessments and fines. Similarly, those companies that actually have had to call upon their insurance after data theft have largely sought coverage for charges imposed by others for the theft of data belonging to others. Coverage has been sought for defense of suits alleging theft of medical information and fraudulent card charges, as well as for attorney fees incurred for responding to regulatory lawsuits or inquiries.[2]

What Are Hackers Now After?

What are cyber thieves after these days? In a word, "You." In isolation, this may seem like an obvious proposition. But the conventional wisdom for the last several years has been that the targets of most serious computer hacks were those possessing sensitive *third-party* information (usually that of their customers, students or patients). Thus, a prime target of computer hacking was often (and continues to be) retailers, financial institutions, hospitals, universities, and medical services companies. Financial account numbers and personal health information were thought to be the crown jewels in the world of data theft.

Lately, however, several high profile attacks appear to suggest a distinctive interest by cyber criminals in the hacked institutions' *own* data. Recent targets of this focus include Ashley Madison, Sony Pictures, and the so-called "Internet of Things."

One way to look at the *Ashley Madison hack* is that it stole third-party information, i.e., member data. The hackers dumped a huge cache of compressed data on the so-called "dark web" of account information for nearly 33 million users. But the hackers reportedly also stole data belonging solely to Ashley Madison. If you take the hackers at their word, they are not doing this to sell credit card numbers to criminal gangs overseas. Instead, their stated goal is to have Ashley Madison shutter its business. The stated rationale: morality.

The attack on Ashley Madison's computer systems is an attack on the core of the company's business model: secrecy. Reportedly, the hackers also obtained internal business information including details concerning server architecture. Apparently, the damage from the hack has been great enough to scuttle a planned IPO.

The *Sony Pictures hack* was another significant cyber breach in which it appears that the hackers' primary focus was to harm Sony Pictures' business rather than grab third-party data to sell to financial criminals for a profit. The hackers stole internal communications between senior company executives as well as proprietary information, and threatened widespread imminent violence at cinemas. The breach ultimately caused Sony Pictures to scrap plans for the distribution of one of its films just before its commercial release.[3] The hackers' stated justification: nationalism, morality, and politics.

> Several high profile attacks appear to suggest a distinctive interest by cyber criminals in the **hacked institutions' own data.** Recent targets of this focus include Ashley Madison, Sony Pictures, and the so-called "Internet of Things."

Hacks against the Internet of Things[4] constitute yet another example of this shift in focus. While third-party information may be stolen in association with such an attack, a hack upon a device, vehicle or system controlling critical infrastructure will often aim primarily to cause direct injury to or chaos for a hacked party. The implications are harrowing.

As a recent New York Times Op-Ed observed: "Recently, two security researchers, sitting on a couch and armed only with laptops, remotely took over a Chrysler Jeep Cherokee speeding along the highway, shutting down its engine as an 18-wheeler truck rushed toward it. They did this all while a Wired reporter was driving the car."[5]

In Europe some years ago, police suspected a 14-year-old of using an electronic remote device to cause a tram to derail, resulting in numerous injuries.[6] In California, computer hackers admitted to accessing a municipality's traffic network in order to congest traffic as part of a labor dispute. Obviously, such a feat imperils safety, given the effect on emergency vehicles, among other things.[7] Speculation abounds over whether hackers can wrest control of an airliner's turbo fans or infiltrate power plants. Hackers are actually being employed by device and vehicle manufacturers to help insulate and secure computer systems from remote unauthorized access.

Risk Management

From a risk management perspective, these hacks are a reminder that hackers may target an institution with no profit motive in sight. Instead, their attack may be designed to damage your business if not shut you down altogether. If this trend continues, your company may have "first-party" exposures that equal or exceed any liability you may face in the throes of a cyber breach. If your network is damaged, if your website is taken down, if the patronage of your services/merchandise is tainted by threats of violence, then business income losses can reach catastrophic levels.

New, Specialized Cyber Products

Insurance coverage is available for losses of business income when computer systems are attacked, hacked or damaged. This may be in the form of business interruption insurance coverage, "reputation damage" insurance coverage, network extortion insurance coverage, or some other formulation. Such policies may promise to pay the policyholder for its own losses of business income due to a covered cyber-related event.

There are insurance coverage options specifically dedicated to instances where a hacking incident leads to loss of business income, extra expense, or some other form of loss to the business.[8] For example, one form of cyber insurance promises to pay for "Income Loss and Interruption Expenses … incurred by the Insured during the Period of Restoration as a direct result of the suspension or deterioration of its business caused by the total or partial interruption, degradation in service or failure of the Insured's Network … ."[9] But policyholders will still need to be very careful about how they construct their insurance programs.

For example, if hackers attack an airliner, there can be horrific injuries to passengers, those on the ground, and emergency personnel. In addition, there can be property damage claims and loss of business income. Thus, a catastrophic event like this will lead to liability claims for injuries and property damage, and first-party losses for property and lost income (at a minimum). But many cyber policies will have exclusions for bodily injury or death claims. Meanwhile, some insurance companies are imposing cyber-related exclusions (there are multiple versions of these exclusions varying in scope) into the liability and umbrella insurance policies they sell that protect against liability for bodily injury and property damage. We have even seen cyber related exclusions in some marine cargo policies.

If hacks against the Internet of Things are going to lead to losses, injuries and damage from hijacked elevators, cars and power grids, then the challenge is to apply a big picture approach to insurance coverage. This in turn requires that policyholders work with insurance brokers who are capable of identifying cyber-related insurance gaps and filling them where possible.

Even where there are no gaps in insurance coverage, remember that insurance policy » Page 13

JOSHUA GOLD *is a shareholder of Anderson Kill in New York and chair of the firm's cyber insurance recovery group.*

Ethics Rules

« Continued from page 9

missive disclosure; furthermore, disclosure of *past* client conduct is prohibited. New York also *declined* to adopt in Rule 1.13 a provision allowing lawyers representing corporations to "report out" if they are unable to get their clients to "do the right thing" (i.e., follow their advice) and the corporations face "substantial injury" relating to that advice (taken or not taken).[4]

Well aware of the conflict between its rules and regulations and the ethical rules of several states, the SEC has taken the view that there is federal pre-emption of conflicting states' ethics rules.[5] So, will the SEC's position prevail if and when tested? Two recent court decisions would seem to point to the answer.

'Quest Diagnostics'

On Oct. 25, 2013, the U.S. Court of Appeals for the Second Circuit affirmed the district court's 2011 dismissal of a False Claims Act qui tam action by Mark Bibi, a former general counsel of Unilab.[6] Bibi, together with two other, former Unilab executives, had sued Unilab's new owner, Quest Diagnostics, on the ground that the company *had* engaged in a pervasive kickback scheme. At the district court level, legal academic ethics experts proffered dramatically opposing opinions: Prof. Andrew Perlman of Suffolk University Law School supported Bibi, who had testified that he was entitled to "spill his guts" because he believed Unilab's actions were criminal; Prof. Stephen Gillers of New York University Law School opined that Bibi's disclosure violated his professional obligations to his former client. The district court sided with Gillers, and dismissed the case.

On appeal, the Second Circuit upheld the important ethical obligation that lawyers have in protecting client confidences (under Rule 1.6) and not breaching said confidences (especially to profit thereby). But in order to get to that ruling, the court had to first address Bibi's contention that the False Claims Act pre-empted New York State's Rules of Professional Conduct.

Judge José Cabranes, writing for the panel, initially noted that courts have "consistently" looked to state ethical rules to determine whether attorneys had conducted themselves properly. He then looked at whether the federal statute did anything to change that traditional rule, but found that "[*n*]*othing* in the False Claims Act evidences a clear legislative intent to pre-empt state statutes and rules that regulate an attorney's disclosure of client confidences." As authority for the "clear legislative intent" standard, Cabranes cited two Supreme Court precedents, both of which stand for the proposition that "we [the U.S. Supreme Court] assume a federal statute has not supplanted state law unless Congress has made such an intention clear and manifest."[7]

This determination leaves the SEC in a pretty precarious position. Why? Because there is not one scintilla of evidence that Congress manifested *any* intent to supplant state-based rules for lawyers when it passed Sarbanes-Oxley.

'Hays v. Page Perry'

More recently, the U.S. District Court for the Northern District of Georgia weighed in on this topic

> The clear implication of 'Quest Diagnostics' is that the **SEC's pre-emption argument** is in for tough sledding (at best).

in *Hays v. Page Perry*.[8] Dismissing a malpractice action against a law firm, Judge Thomas Thrash held that the firm had no duty to report its client's possible securities fraud to the SEC.

In a prior ruling, Thrash had opined that "Georgia law never obligates a lawyer to report even the most serious client misconduct to regulators."[9] On a motion to have the judge reconsider his prior ruling, he was even more emphatic, finding the plaintiff's theory "a strange perversion of lawyers' professional responsibilities" and its legal claim "profoundly flawed." If the plaintiff were to be correct, he reasoned, there would be dire consequences: "The risk of civil penalties would cause attorneys, out of self-preservation, to err on the side of disclosure when in doubt. Consequently, such a rule could even deter potential clients from seeking advice from a lawyer." Thrash also (correctly) noted that part of the flaw in the plaintiff's approach was that it "conflate[d] attorney-client confidentiality with the attorney-client *evidentiary* privilege." Violating the former (an ethical rule), of course, could subject a disclosing attorney to being disbarred;[10] the privilege, on the other hand, is something that is owned by the client (*not* her attorney).

Conclusion

In neither of these two cases were the SEC's disclosure obligations directly at issue. Indeed, it is a tad surprising that the plaintiff in *Hays* never invoked those obligations. Nonetheless, the clear implication of *Quest Diagnostics* is that the SEC's pre-emption argument is in for tough sledding (at best). And for judges coming after Thrash confronted with this issue, we can hope that they will follow his lead and side with states' ethics rules regarding attorney obligations of confidentiality.

1. See, e.g., C.E. Stewart, "Sarbanes-Oxley: Panacea or Quagmire for Securities Lawyers?" N.Y.L.J. (March 21, 2003); C.E. Stewart, "This is a Fine Mess You've Gotten Me Into: The Revolution in the Legal Profession," NY Business L.J. (Summer 2006); C.E. Stewart, "The Pit, the Pendulum, and the Legal Profession: Where Do We Stand After Five Years of Sarbanes-Oxley?" 40 Sec. Reg. & L. Rep. (Feb. 18, 2008); C.E. Stewart, "New York's New Ethics Rules: What You Don't Know Can Hurt You!," NY Business L.J. (Fall 2009); C.E. Stewart, "'Here's Johnny!': Carnacing the Future of the SEC's Preemption Overreach," 46 Sec. Reg. & L. Reg (April 28, 2014).

2. See "The Pit, the Pendulum, and the Legal Profession," supra note 1; "Here's Johnny!," supra note 1.

3. Washington's and California's interplay with (and challenge to) the SEC's disclosure regime is set forth in detail in "Here's Johnny!" See supra note 1.

4. New York also does not use the "reasonable lawyer" standard, opting instead to judge lawyers' behavior on an "actual knowledge" standard. This is a very important safeguard for lawyers, protecting them from a harsh, 20-20 hindsight judgment. See, e.g., *In re Jordan H. Mintz* and *In re Rex R. Rogers*, SEC Release Nos. 59296 & 59297 (Jan. 26, 2009).

5. See "Here's Johnny!," supra note 1.

6. *United States ex rel. Fair Lab. Practices Assocs. v. Quest Diagnostics*, 2013 U.S. App. LEXIS 21709 (2d Cir. Oct. 25, 2013), aff'm, 2011 U.S. Dist. LEXIS 37014 (S.D.N.Y. April 5, 2011).

7. *Bates v. Dow Agrosciences*, 544 U.S. 431, 449 (2005); *Cipollone v. Liggett Grp.*, 505 U.S. 504, 516 (1992). Cabranes also noted that the False Claims Act, while allowing a qui tam suit, "does not authorize [the plaintiff] to violate state laws in the process." Citing *United States ex rel. Doe v. X.*, 862 F. Supp. 1502, 1507 (E.D. Va. 1994).

8. See http://www.bloomberglaw.com/public/document/Haysv.PagePerry_LLC_No_113CV3925TWT_2015_8L_71863_ND_Ga_Mar_17_.

9. 26 F. Supp. 3d 1311 (N.D. Ga. 2014).

10. The judge noted that while Georgia's Rule 1.13(c) allows "reporting out", that disclosure option is permissive (and the drafters of the rule changed "shall" to "may"). In New York, as noted above, there is no "reporting out" option.

Privilege

« Continued from page 10

citizens, which is a profound and compelling interest.[18]

Wultz reflects the highly charged security issues unique to that case. Obviously, a plaintiff's interest in combatting terrorist financing poses far greater "seriousness" than a garden variety civil action over, e.g., a teller misappropriating funds from the cashier's drawer.

A federal court in Texas applied the balancing test in evaluating examination materials of the NYDFS in *Ex rel. Fisher*.[19] At issue in this case was the NYDFS' statutory provision on the confidentiality of bank examination materials. The New York Banking Law provides: "All reports of examinations and investigations, correspondence and memoranda concerning or arising out of such examinations and investigations … shall be confidential communications, shall not be subject to subpoena and shall not be made public … ."[20] By statute, only the superintendent of financial services may make N.Y. Banking Law §36(10) material public if "in the judgment of the superintendent, the ends of justice and the public advantage will be subserved by the publication" thereof.[21] In *Fisher*, the NYDFS neglected to apply the required analysis under the balancing test for the bank examination privilege, which the Texas federal court noted is applied by New York federal courts.[22] Nevertheless, the court found that even if the NYDFS had conducted such analysis, "it would still lead the Court to the conclusion that the privilege should not apply to highly relevant documents[.]"[23]

In *Rouson v. Eicoff*, a plaintiff served a subpoena on the NYDFS seeking "all reports of examinations and investigations, correspondence and memoranda concerning or arising out of its investigation of" a supervised institution.[24] The NYDFS objected to disclosure of the documents, citing N.Y. Banking Law §36(10). The court conducted an in camera review of the documents that the NYDFS believed to be privileged, applying the above-discussed balancing test for disclosure of non-factual examination materials. In its review, the court found that much of the material submitted by the NYDFS under a claim of bank examination privilege was in fact factual material containing no examiner opinions, and the few non-factual opinions stated in the materials were "negligible" and "so intertwined with factual allegations that to redact them would distort the tenor of the document."[25]

While both the OCC and the NYDFS alike strongly believe that the bank examination privilege is essential to the candor and frankness crucial to the iterative process, the federal courts are clearly in disagreement as to its relative value. In *McKinley v. Board of Governors of the Federal Reserve System*, the D.C. Circuit noted: "If supervised institutions no longer believe the Board could or would maintain the confidentiality of information it collects through the supervisory process, they would be less willing to provide the Board with the information it needs to assure a robust supervisory environment."[26] Similarly, in *In re Subpoena Served Upon Comptroller of the Currency*, the D.C. Circuit said that the "success of [regulatory supervision] depends upon the quality of communication between the regulated banking firm and the bank regulatory agency."[27] In fact, the U.S. Supreme Court, in discussing the very similar "deliberative process privilege,"[28] in a unanimous decision noted that this type of governmental privilege rests "on the obvious realization that officials will not communicate candidly among themselves if each remark is a potential item of discovery and front page news, and its object is to enhance the quality of agency decisions, by protecting open and frank discussion among those who make them within the Government."[29] However, Scheindlin of the Southern District appears to have less faith in the value of the privilege: "The description of the 'iterative process' of communication between banks and regulators … is more the prescription of an ideal than the description of an observed state of affairs."[30]

This difference of viewpoints necessarily creates a moving target for the banking bar in New York, particularly for attorneys representing financial institutions. Given this uncertainty, counsel should consider several steps to reduce

> Beyond the very important goals of protecting and promoting the iterative process, and encouraging candid dialog between an institution and its regulator, preservation of the bank examination privilege has **very compelling market benefits.**

the risk that adverse information or communications may be disclosed. First, counsel should advise their bank clients that the risk remains, albeit often remote, that communications with regulators may be ordered released to a requesting plaintiff. This is especially concerning where the issue is one of a sensitive nature implicating national security or consumer protection issues. Second, in drafting management's response to regulators' ROEs, particularly responses to "matters requiring attention," counsel should consider whether under the facts it would be appropriate to contest the examiners' findings, or at least acknowledge that the institution takes a contrary view, even when the institution is ultimately acquiescing to the regulators' requested remedial goal. Third, and perhaps more for agency counsel, consider isolating strong supervisory criticism in designated sections of the examination material and correspondence. This may help to avoid the challenge like that found in *Rouson*, where the examiners' opinions were so "intertwined with factual allegations" so as to render redaction impractical and disclosure unavoidable. Fourth, agency counsel should consider collaborating with outside counsel for institutions in conducting the analysis of whether "good cause" exists. Disregarding the bank examination privilege has very significant implications for both institution counsel as well as agency counsel; thus, close collaboration on this important issue is warranted.

While the courts are in universal agreement that the bank examination privilege exists, it is not universally upheld. Thus, the circumstances that might necessitate disregarding the privilege require an intensive analysis of competing factual and public policy considerations. Because such considerations are necessarily case-specific, relying on prior cases is of limited utility other than to say that the current policy implications are far less serious than in prior cases. In the end, an institution can only hope to have good counsel that understands the regulatory landscape, how much management can push back on examination correspondence in an attempt to frame the record, and that can recommend effective strategies for assisting the agencies in defending their own privileges.

Beyond the very important goals of protecting and promoting the iterative process, and encouraging candid dialog between an institution and its regulator, preservation of the bank examination privilege has very compelling market benefits. "A less cited but important justification for the privilege is the financial system's sensitivity to public questioning of bank soundness. Open, adversarial, litigation between banks and their regulators is destabilizing and regulators seek to avoid it."[31] Disregarding the bank examination privilege and allowing the highly technical and context-driven remarks and opinions found in examination materials out into the public arena, particularly without any explanation or filter, would have serious and unwarranted consequences for individual institutions and the system as a whole.

1. *Sharkey v. J.P. Morgan Chase & Co.*, 2013 WL 2254553, at *1 (S.D.N.Y. May 22, 2013).

2. *In re Atlantic Fin. Fed. Sec. Litig.*, 1992 WL 50074, at *4 (E.D. Pa. March 3, 1992). See also *Federal Housing Finance Agency v. HSBC North America Holdings*, 2014 WL 1908446, at *7 (S.D.N.Y. May 13, 2014) (documents sent to regulator reflecting items to be discussed in meeting and narrative answers sent to regulator are privileged and properly withheld).

3. While the "bank examination privilege is a common law privilege," *Federal Housing Finance Agency v. J.P. Morgan Chase & Co.*, 978 F. Supp. 2d 267 (S.D.N.Y. Oct. 16, 2013), federal and state regulators have attempted to codify this privilege in statutes and regulations. See, e.g., 12 C.F.R. §4.36 (prohibition on unauthorized disclosure of non-public OCC information without OCC authorization); N.Y. Banking Law §36(10) (prohibition on disclosure of NYDFS examination materials without the Superintendent's authorization).

4. *Wultz v. Bank of China Ltd.*, 61 F. Supp. 3d 272, 281 (S.D.N.Y. 2013).

5. Id. at 281-82.

6. Id. at 282.

7. Id.

8. Id. See also *Schreiber v. Society for Sav. Bancorp*, 11 F.3d 217, 220 (D.C. Cir. 1993).

9. Id. See also *In re Providian Fin. Sec Litig.*, 222 F.R.D. 22, 26 (D.D.C. 2004).

10. Id.

11. See, e.g., 12 C.F.R. Part 4 (as to OCC examination materials), or N.Y. Banking Law §36(10) (as to NYDFS examination materials).

12. *Rouson v. Eicoff*, 2006 WL 2927161 (E.D.N.Y. Oct. 11, 2006).

13. *Wultz*, 61 F. Supp. 3d 272.

14. *Id.*

15. Id. at 283. See also *Stratford Factors v. New York State Banking Department*, 10 A.D.2d 66 (1st Dept. 1960).

16. Id. at 283. See also *In re Citigroup Bond Litigation*, 2011 WL 8210671 (S.D.N.Y. Dec. 5, 2011).

17. Id. at 291.

18. *Wultz*, 61 F. Supp. 3d at 290 (internal quotations omitted).

19. 2015 WL 3942990 (E.D. Tex. June 16, 2015).

20. N.Y. Banking Law §36(10).

21. *Fisher*, 2015 WL 3942990 at *3.

22. Id. at *5.

23. Id.

24. 2006 WL 2927161, *1 (E.D.N.Y. Oct. 11, 2006).

25. Id. at *6.

26. 647 F.3d 331, 339 (D.C. Cir. 2011).

27. 967 F.2d 630, 633 (D.C. Cir. 1992).

28. See *Redland Soccer Club v. Department of the Army*, 55 F.3d 827, 853 n.18 (3d Cir. 1995) ("Our discussion of the deliberative process privilege is based, in part, on interpretations of the bank examination privilege. The two privileges are similar and precedent concerning them is often relied upon interchangeably.").

29. *Department of Interior v. Klamath Water Users Protective Association,* 532 U.S. 1 (2001).

30. *Wultz*, 61 F. Supp. 3d at 291.

31. *Federal Housing Finance Agency v. J.P. Morgan Chase & Co.*, 978 F. Supp. 2d 267 (S.D.N.Y. Oct. 16, 2013). See also *Delozier v. First National Bank of Gatlinburg*, 113 F.R.D. 522, 526 (E.D. Tenn. 1986) (a "second interest in nondisclosure [of bank communications] which must be considered is the effect of such disclosure on the public's confidence in the bank.").

Advice

« Continued from page 9

minds not obsessed over delivering boatloads of billable hours.

I have practiced in several law firms and in several in-house positions—in two of the latter as general counsel. My law firm stories you have probably already heard because they are surely not much different from yours. In-house, there was much politics and there was much maneuvering around the rules. Each case was unique and specific to the particular corporate culture in which it occurred. Just a few examples of what was floated over the years as confirmed corporate gossip:

• There was the staff lawyer who convinced the general counsel that an attorney was needed on the scene daily during the workout of a troubled loan in Latin America. The lawyer went south and pretty much stayed there, coming back at intervals, trying not to show how much he was enjoying himself, never all that clear about what he was doing there.

• Every few years, an executive newly arrived at the level of senior management at the company would immediately stir things up by conceiving of a new and original business strategy for submission to the lawyers—who had already been asked those very same questions several times before, from the last inductees to senior management. On each occasion, an old memorandum on point (fondly called the "stupid memo") would be brought up, refreshed and submitted as if for the first time. No one ever caught on.

• In exchange for shielding his staff lawyers from the unpopular leader of a team in the legal department, the second-in-command dropped most of the team's work onto them. Fit and relaxed, he spent much time at the gym, interceding, when called upon, whenever the boss got out of hand. At the appropriate moment, one of the put-upon staffers gathered others together to pull an Ides of March on the problem team leader, who eventually pushed upstairs—to a very private job watching over the company's privacy policy.

• A business unit head whose legal work was done by a skilled staff lawyer delivered spurious charges to the CEO about both her and the general counsel who protected her. The GC discovered his true reason: The unit lead wanted to control legal support from within his own branch office. Seeing a good lawyer's career potentially compromised and his own power base threatened, the GC dutifully presented a promising candidate for the job, knowing full well from the ever-reliable GC gossip underground that the unit head and the prospective hire could never possibly get along. They didn't, the staff lawyer kept her job and kept doing good work—and all was well, except that the new face in the legal department, competent as she also proved to be, often did not have all that much to do.

For propriety, I have left out stories of intra-office marital infidelities, blatant come-ons to vulnerable young women, cougar attacks on beefy young men, good advice gone unheeded, the mail-fraud conviction, and those rare examples of bad advice that was followed by business managers who did not understand what went wrong until it was too late.

The key point is this: As a lawyer in a legal department, you are part of a larger organization with a unique culture and informal rules of governance. To prosper, you have to learn what those are—and keep in mind that they can vary considerably from organization to organization in the same line of business. There are, however, some universal constants:

> One of your hardest moments may come when you give valuable counsel, only to find that the **company asks you to bring in an outside lawyer for a second opinion.**

In business, business comes first. Back in the firm, you could consider, write about, and engage in discussions about legal questions worthy of a law review note or Supreme Court brief. You could urge that client first and foremost accept the imperative of respecting the legal consequences of his or her actions—and otherwise prosper, as so many lawyers do, by taking yourself far too seriously. In-house, you are considered a member of the business team. Written commentary full of anticipated legalisms and case citations will likely be seen as a negative. Say what you have to say as simply and clearly as you can, and be practical. Always write for an informed lay reader. As I alerted my staff lawyers when I was GC, anyone submitting a memo with *and/or* or *document(s)* would be held after work to write 50 times, "Herewith and as aforesaid, I swear and declare that I shall never author another document(s) so obtuse and/or ponderous." I never needed to make good on the threat; the secondary point here is that sometimes the boss is right.

In-house legal reasoning is a bit reverse in its thinking from law-firm practice. Back at the firm, you typically started with the legal proposition and drove toward the conclusion the law would provide and then applied that to what your client wanted to do—seeking, if you could, a way to bridge from legal conclusion to business expectation. In-house, it is often best to start with the business objective and work backward from there. Practice that as a mental exercise, if need be; the approach will show even in how you talk and write about the problem, and you will gain more respect and trust as a result.

That does not mean you must say *no* when the answer should be *yes*. I saw a company lose an enormous sum and much public trust due to the *yes* an in-house lawyer gave in an effort to accommodate a profitable but rogue salesman when his answer should have been a resolute *no*. His career did not fare well after that episode. If there is one overriding challenge of in-house practice, it is making sure that the game is played by the rules of the law without sounding officious or appearing to be an obstruction. The skills required to do that are as much interpersonal as they are intellectual—and law schools and law firms do little to teach how to master them.

One simple and always-effective way to start is easy: Learn your company's business. You would think that an in-house lawyer would naturally do that, but too many come into a company thinking about keeping its legal house in order and not to the big picture: the markets, the products and services, the competitors, the vendors, the customers, earnings, plans and forecasts—and all the other elements that, in application, are particular to each business. Study with care the roles played by your in-house "clients." Get to know them personally and understand how you can help them, which is almost the same as getting to understand how they can help you, because your job performance rating will depend in large measure on how they evaluate your assistance.

Expect, just the same, a lack of understanding about what goes into performing your own job. There will be those who hand you a 20-page contract the day before (or the day after) signing, asking if you see any problem with it. Somehow, you will have to find a way to make those coworkers happy and at the same time get them to understand that you need enough lead time to be effective.

Proving your economic worth in-house can be tough. Because you can no longer simply prove how much money you brought in, as was essential in a firm, about the most you can do is try to show how efficient you are and demonstrate much you saved, whether by avoiding a legal danger or simply getting something done that might otherwise have required engaging outside counsel.

One of your hardest moments may come when you give valuable counsel, only to find that the company asks you to bring in an outside lawyer for a second opinion. That is the downside of being a member of the team: You are one of the guys, but you are not the authority—since everyone in business knows that authorities (a) are expensive, and (b) work somewhere other than here. There is no point reminding everyone that Clarence Darrow worked in-house too. You hire a law firm; the typical result: Someone over there who earns a good bit more than you charges a small fortune to tell management the same thing you did—and everyone goes happy in a backhanded win-win kind of way.

The outside lawyers you hire must understand one thing: They need to have your back. They must be sympathetic and supportive of your position, with full understanding that you serve non-lawyers who must be made satisfied with the results of what you and outside counsel will do together. The outside lawyer needs to know your budget limitations and needs to understand your company's business enough to ask you the right questions before spending your money. Successful outside attorneys partner closely with in-house counsel, never forgetting that outside counsel looks its best when the in-house counterpart looks his or her best. Find those outside lawyers who can help you that way, whether in a pinch or on an ongoing basis, and you will have turned a for-hire vendor into an effective resource—for your company and especially for you.

Big Data

« Continued from page 9

and improper relationships with foreign officials. Unless a tipster informs someone at the organization, these red flags can be hard to identify—even with more proactive measures such as internal audit. In fact, according to a recent report by the Association of Certified Fraud Examiners, internal audit detected only 14 percent of corporate fraud.[5] That means one thing: Old ways of looking for corruption should exit stage right, and make way for the entrance of Big Data Analytics.

Why Existing Enterprise Risk Management (ERM) Approaches Fall Short in Today's World of Big Data. As time passes, the speed of business continues to accelerate, and with it, so does risk. Globalization, technology and data have combined to foster unprecedented growth, but they also raise unprecedented threats. In response, applicable regulations continue to become more complex, making doing business in the global economy fraught with even greater peril, particularly when it comes to your organization's information.

Unfortunately, organizations have historically taken a myopic view of risk, and many cling to this approach today. In other words, they focus on risks according to the silo where they are most likely to originate. So, the information technology team may focus its efforts on searching for cybersecurity risks, while the benefits department may be heavily invested in looking for breaches of privacy with respect to the improper sharing of protected health information under the Health Insurance Portability and Accountability Act. Meanwhile, the finance team may be studying transactions for fraudulent credit transactions. However, a holistic approach to risk that crosses departmental boundaries is far more likely to yield results and detect risky behaviors. With the velocity and amount of data at play, risks are more likely to involve multiple teams. A cybersecurity breach could lead to the leak of benefits data, which would then lead to a legal and public relations nightmare with reputational and financial consequences.

Today's global approach to business raises the specter of unprecedented risk that makes a narrow, department-based focus untenable. Businesses that operate in multiple countries must understand how the laws of those nations intersect and conflict and find ways to ensure their operations remain compliant. This is particularly true when organizations outsource work to third-party partners located abroad. With decentralized workgroups making idiosyncratic decisions and leveraging technology to engage in real-time communication, it is imperative that executives and corporate counsel gather insight as to where and how employees are conducting transactions and communicating. The legal department must take an active role in assessing how laws and regulations intersect across multiple jurisdictions and navigate any conflicts. Active risk management is a necessity; otherwise, legal's role will be limited to damage control.

The greater mobility and globalization of work and the workforce itself has caused organizations to relinquish tight controls over their data, which further complicates the current risk environment. Corporate data can be an incredibly valuable asset or it can be a corporation's greatest liability if it is not properly controlled. Whether stored in the cloud or on mobile devices, data can be easily deleted, shared, or transferred instantly and without notice to the organization—and with serious implications. For example, data transfer—even internally within an organization or between its subsidiaries or partners—can be particularly risky in the global environment, given the increasing number of regulations imposing data privacy. Many nations outside the United States have strict rules that limit the transfer of personally identifiable information over national borders. Therefore, cloud computing can be of great concern, and corporate legal teams should analyze all service-level agreements with providers of cloud-based services to ensure they have adequate security measures and business continuity plans, as well as rules governing how they transfer data between locations or share it with other third parties.

> Organizations have a clear choice: They can continue to rely on the backward-looking detection methods of old, or they can follow the lead of the legal team and transform into a **forward-looking culture of compliance** that addresses emerging enterprise risks by studying data and identifying (and investigating) risky behaviors before they become full-blown fires.

Data mobility is only part of the problem. The other is the number of data sources that businesses draw from. Between email, social media, mobile apps, and the Internet of Things, there are more immediate connections between employees and the outside world, which breeds greater risk. Whether by external means (hackers who prey on unsuspecting recipients of malware and viruses) or by internal means (intentional or negligent employee disclosure of confidential information) there are more ways than ever that organizations can find their information compromised. Legal teams must become familiar with the organization's data conduits and policies; they must also ensure there are adequate means in place to preserve data in the event of litigation or regulatory or internal investigations.

For these reasons, demonstrating compliance with the FCPA requires more than merely implementing policies and controls. Without more, organizations cannot be sure whether their anticorruption and antibribery mechanisms are actually working. Therefore, legal teams must take the lead in implementing technology and practices that can make a compliance program truly effective.

How Legal Can Take the Lead With ERM. With stringent regulatory requirements and accelerating data velocity, the legal department plays a key role in ensuring that organizations identify and mitigate their risks. They must be the champions of a forward-looking approach to enterprise risk management; one that does not discard the tried-and-true tools of policies, procedures, and audits but rather rounds it out with advanced tools that are designed to make the most of the organization's data resources.

An early warning system must be able to scour data—both structured and unstructured—for red flags. Keyword searches are a fairly basic way to look for names of government officials or high-risk vendors. They can also search emails and social media communications for suspicious words and phrases. But they are only effective if they are well conceived. The legal team should work with subject-matter experts and linguists to choose keywords that are neither overinclusive nor underinclusive, so that the ERM team is not overwhelmed with too much irrelevant information yet does not miss key information. But standing alone, keywords are often not enough to detect the hidden indicators of malfeasance: Many fraudsters are sophisticated enough to couch their misdeeds in more innocuous language or code words. Companies should not underestimate the creativity that may be at play in this area.

Therefore, legal should encourage the organization to look to data analytics tools equipped to do more than scratch the surface of files and communications. These tools can unearth risks by transforming seemingly random data scattered among many documents. For instance, technology-assisted review (TAR) can prioritize documents based on the likelihood that they contain problematic material. This may then be used to create more targeted search terms or to automatically detect potentially problematic communications.

Other advanced tools can detect even more nuanced patterns in data. For example, linguistic analysis techniques take keyword searches several steps further and identify words and phrases that may refer to suspicious activity. Anomaly detection tools can scan records for irregularities in accounts payable transactions. Data visualization tools can analyze relationships between foreign officials, vendors, and employees. Concept clustering can find hidden patterns within documents that are seemingly unrelated. These tools can operate continuously and monitor ongoing transactions for patterns or anomalies, often in real or near-real time.

The Path Forward. Regulators have raised the bar as to their expectations of what constitutes an effective compliance program. Legal teams must stop responding to risk and begin anticipating it, and they must ensure their organizations do likewise by adopting a more data-driven, future-oriented approach to ERM. Instead of waiting to examine data until an issue surfaces, legal teams must partner with risk and compliance professionals and use advanced data analysis techniques to find the latent risks lurking in their data. This will bring about a cycle of improved fraud prevention and detection which will more than pay for itself if and when a problem arises.

1. 15 U.S.C. §§78dd-1, et seq.
2. Id.
3. Goodyear Tire & Rubber Co., Order Instituting Cease-and-Desist Proceedings, Pursuant to §21C of the Securities Exchange Act of 1934, Making Findings, and Imposing a Cease-and-Desist Order, No. 3-16400 (Feb. 24, 2015), available at http://www.sec.gov/litigation/admin/2015/34-74356.pdf.
4. U.S. Department of Justice & U.S. Securities & Exchange Commission, A Resource Guide to the U.S. Foreign Corrupt Practices Act (2012), available at http://www.sec.gov/spotlight/fcpa/fcpa-resource-guide.pdf.
5. Association of Certified Fraud Examiners, Report to the Nations on Occupational Fraud and Abuse: 2014 Global Fraud Study (2014), available at http://www.acfe.com/rttn/docs/2014-report-to-nations.pdf.

Data Security

« Continued from page 11

sub-limits often can come into play to limit coverage. Many cyber forms have not only a "module" approach to the various insuring grants they offer for cyber claims, but also sub-limits applicable to certain aspects of insurance coverage within those particular modules. A large "blanket limit" of insurance is a lot less valuable when the majority of important coverages are subject to an absurdly low sublimit. Again, be very careful here and work with a seasoned broker who can benchmark certain levels of insurance coverage that are right for a policyholder your size and appropriate to your industry.

Cyber Insurance Fine Print

Just because you purchase insurance with the word "Cyber" in the title, does not mean your cyber insurance company intends to pay. A pair of recent insurance coverage lawsuits involving "Cyber" policies make this painfully clear. In *Travelers Property Cas. Co. of America v. Federal Recovery Services*, a May 11, 2015 decision from a federal trial court in Utah denied the policyholder coverage for a customer suit over the handling and return of customer data. While this may be a somewhat odd case, it is a reminder that you have to look beyond the titles of insurance policies.

In another recent case, *Columbia Casualty v. Cottage Health System* (C.C.D. 2015), the insurance company filed a lawsuit in California federal court against its policyholder, Cottage Health System. The policyholder had suffered a breach of patient data and was sued over it. The underlying suit ended with a settlement that the insurance company then argued was not covered due to the policyholder's alleged lax computer security. The insurance company argued that the alleged lax security violated the insurance policy conditions.

The California trial court recently dismissed the insurance company's action for failing to engage in alternative dispute resolution before proceeding to litigation against its policyholder. However, because the dismissal of the insurance company's complaint was made without prejudice, it is possible that this dispute will make its way back to the federal trial court for ultimate rulings on the merits. The issue of coverage conditioned on the robustness of computer security measures employed by the policyholder will be one with major implications for those purchasing cyber insurance.

Damage Systems and Hacking

Even where dedicated cyber insurance is purchased, policyholders should still consider insurance coverage under other business insurance policies that they regularly purchase in the event of a cyber claim.[10] While more and more cyber exclusions are being imposed on other types of insurance policies to encourage the purchase of stand-alone cyber insurance, coverage often still exists under non-cyber policies. For example, in one lawsuit, *NMS Services v. The Hartford*, 62 Fed. Appx. 511, 514 (4th Cir. 2003), the U.S. Court of Appeals for the Fourth Circuit held that the deliberate destruction of computer files and databases by a former employee was covered damage to the policyholder's computer systems.[11]

In *American Guarantee & Liability Insurance v. Ingram Micro*, 2000 U.S. Dist. LEXIS 7299 (D. Ariz. April 18, 2000), a policyholder's computer system went down after a power outage. The federal trial court held that the insurance policy covered the loss, including loss of business income, because the loss of use of programming instructions and custom configurations left the system inoperable and was a covered event under the policyholder's property insurance. See also *Southeast Mental Health Center v. Pacific Ins. Co.*, 439 F. Supp. 2d 831, 837 (W.D. Tenn. 2006) (holding that the corruption of the pharmacy computer was a covered loss of property and the policyholder was owed business income coverage); *Lambrecht & Assoc. v. State Farm Lloyds*, 119 S.W.3d 16 (Ct. App. Tex. 2003) (holding coverage for costs of restoration of data resulting from computer virus).

> If hacks against the Internet of Things are going to lead to losses, injuries and damage from hijacked elevators, cars and power grids, then **the challenge is to apply a big picture approach to insurance coverage.**

In *Retail Ventures v. National Union Fire Insurance Co. of Pittsburgh*, 691 F.3d 821 (6th Cir. 2012),[12] the U.S. Court of Appeals for the Sixth Circuit affirmed the federal trial court rulings and found insurance coverage for all losses suffered by a retailer as the result of a computer hack. The losses recovered under the subject crime insurance policy included amounts for stolen credit card account information, checking account data, computer forensic investigation costs, legal fees, call center expenses, P.R. expenses, FTC compliance costs, among other categories of loss.

Conclusion

It is increasingly clear that liability for the theft of third-party data is not the only cyber peril to be concerned about. The risk of hackers targeting a company's core assets to inflict harm or damage to its ability to operate is very real. With the Internet of Things gaining greater traction, this risk profile will only increase. Policyholders are wise to conduct an insurance and risk management check-up that extends beyond safeguarding employee health data and customer account data. There are options in the insurance marketplace to help protect against these broader operational and reputational risks. The insurance products, however, sometimes leave something to be desired. Having a good broker or insurance consultant by your side can help greatly.

1. Kevin LaCroix, "O.K., This Is a Big Deal: 7th Cir. Reinstates Neiman Marcus Consumer Data Breach Class Action," The D&O Diary, July 22, 2015.
2. See, e.g., Jeff Sistrunk, "11th Circ. Partially Revives HIPAA Data Theft Coverage Suit," Law360, Aug. 17, 2015; *Retail Ventures v. National Union Fire Insurance Co. of Pittsburgh*, 691 F.3d 821 (6th Cir. 2012) (in which author Joshua Gold was coverage counsel for the plaintiffs).
3. The U.S. OPM breach also can be fairly viewed as one directed at the "institution." While the OPM cyber breach did concentrate on stolen information concerning millions of federal employees, most agree that the aim was an attack on the U.S. government through espionage and knowledge of state secrets. Not only was personal employee information stolen, but so too were the actual background investigation reports compiled by the government.
4. The Internet of Things refers to the network of objects or machinery via a wired or wireless connection.
5. Zeynep Tufekci, "Why 'Smart' Objects May Be a Dumb Idea," N.Y. Times, Op. Ed., Aug. 10, 2015.
6. "Could hackers take down a city?" Hamilton Spectator, Aug. 18, 2015.
7. The California hack on the traffic system is also a reminder that the threat can come from those working for you or from subcontractors you or your vendors hire.
8. Some cyber events do not involve hackers but may be the result of system error, human error, or natural causes such as severe weather. Many cyber policies extend insurance coverage to losses and claims caused by circumstances other than just hackers or viruses.
9. Paragon Cyber and Privacy Insurance specimen policy form, dated April 2013.
10. See, e.g., Jeff Sistrunk, "11th Circ. Partially Revives HIPAA Data Theft Coverage Suit," Law360, Aug. 17, 2015.
11. If you do find yourself making a cyber claim with your insurance company, be careful to preserve information including any computer system components and forensic reports. Whether it is financial information used to support a business income loss, or damaged computer parts, err on the side of preserving evidence. In *Southeast Mental Health Ctr. v. Pac. Ins.*, 439 F. Supp. 2d 831, 840, (W.D. Tenn. 2006), the defendant insurance company accused the policyholder of spoliating a damaged computer drive and sought to bar the introduction of any evidence related thereto. The court rejected the insurance company's position, finding that the policyholder kept the damaged drive for a year after promptly inspecting it and noting that the defendant never requested that the drive be made available for examination.
12. Author Joshua Gold was coverage counsel for the plaintiffs in this insurance litigation against National Union.