REAL WORLD CASE 1

Texas Health Resources and Intel: Ethics, IT, and Compliance

The IT staff at Texas Health Resources Inc. must deliver more than technical functionality. And it needs to deliver more than the business requirements: It also has to meet the organization's ethical standards.

To that end, its systems must help ensure that Texas Health complies with laws and regulations.

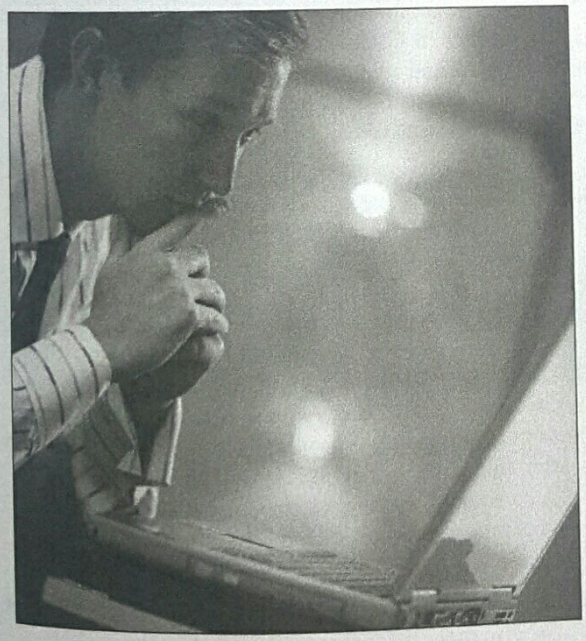
And they also have to promote the right behaviors and prevent or flag undesirable ones, says Michael Alverson, vice president and deputy CIO at the Arlington-based nonprofit health care system. Consider the challenge of handling patients' medical records. Even though the federal Health Insurance Portability and Accountability Act mandates that agencies keep those records private, caregivers still need to access them—when appropriate.

So the organization's electronic health records system "gives doctors and nurses who are caring directly for patients quick access when they use the right authentication," Alverson says.

But additional authentication is required to get records for patients who aren't under the provider's immediate care. The system records who gets access to what, allowing officials to audit and review cases to ensure there's no inappropriate access.

"The IT staff holds itself to similar ethical standards, too," Alverson says. The department has policies that prohibit taking gifts and endorsing vendors, to help guarantee that workers make procurement decisions based only on quality and needs.

FIGURE 13.1



The pervasive use of information technology in organizations and society presents individuals with new ethical challenges and dilemmas.

Source: © Punchstock.

And when there's any question—such as when a vendor proposes a deep discount if Texas Health agrees to be an early adopter of new technology—IT leaders can turn to the systemwide Business and Ethics Council for guidance.

"If we really want everyone to subscribe to the idea that working at Texas Health is special, then we have to have people actively believe in doing the right thing," Alverson says.

Companies are increasingly looking at their ethics policies and articulating specific values that address a range of issues, from community commitment to environmental sustainability, which employees can use to guide their work. The need to comply with federal laws and regulations drives some of this, while consumer expectations, employee demands and economic pressures also play a part.

Information technology consultant Dena L. Smith lays out a hypothetical dilemma: Should an IT department hire a more expensive vendor because the vendor shares its own company's ethics standards, or should it go with a lower-cost provider that doesn't?

Companies with established ethical standards that guide how they conduct business frequently confront this kind of question, Smith says, but it's a particularly tough question today, given the recession. With IT departments forced to cut budgets and staff, CIOs will find it difficult to allocate dollars for applications that promote corporate ethics.

"The decisions were easier in the days when the economics were favorable, but the choices may have to be more limited now," says former CIO John Stevenson, president of consultancy JG Stevenson Associates. "Now it's how much can you afford to do versus how much do you have to do so you don't get burned." Stevenson says companies that had moved toward certain ethical goals before the economic crisis—whether those goals involved green initiatives or corporate responsibility programs—aren't giving up their gains. "But if they haven't done that yet, it gets more difficult to say we'll spend more money than we have to," he says.

"Companies use the term 'corporate ethics' to mean many different things. In many organizations, if not the majority, it means compliance with a set of legal and minimum standards. In other organizations, corporate ethics means defining a set of corporate values that are integral to how they go about business," says Kirk O. Hanson, executive director of the Markkula Center for Applied Ethics at Santa Clara University.

Either way, CIOs have an opportunity to show how technology can further their companies' ethics objectives.

"Policy decisions at the very senior level need the sensitivity that IT experts can bring to the table," Hanson says. "CIOs will know the capabilities of IT and be able to contribute that to corporate strategy. They will also know the misuses of those capabilities and be able to flag those and prevent the organization from stepping in scandals."

Hanson cites a 15-year-old case in which marketing workers at a large telephone company spent millions of dollars to develop a list of customers with ties to the Washington

area that they planned to sell to other marketers. In violation of company policy, they compiled the list using the company's database of customers who frequently placed calls to the District of Columbia.

Executives learned about the list before the marketing department sold it. IT then developed a system to monitor use and block future unauthorized access to such information, Hanson says. However, it came a bit late, since IT should have developed the application in advance, anticipating the need to protect the information as well as detect any efforts to breach it.

Hanson says IT today can build systems that can screen potential subcontractors and vendors to see if they share certain values.

It's also possible to create tools that flag contracts whose costs exceed expectations in ways that suggest bribery or other improprieties, or set up systems that analyze customer satisfaction surveys to find evidence of unethical behaviors on the part of workers.

Meanwhile, companies that put green initiatives at the top of their ethical concerns can have IT create applications that track energy consumption to flag anomalies that indicate inefficiencies or calculate the corporate carbon footprint and identify ways to reduce it.

"You have to step back a minute and ask, 'What is the role of technology around ethics?'" says Smith. "Technology can help from a monitoring, protection and prevention standpoint in a lot of ways." The notion of corporate ethics hasn't always been so broad, says Mike Distelhorst, a law professor at Capital University Law School, a former adjunct professor of business ethics at the Capital School of Management and Leadership and former executive director for the university's Council for Ethical Leadership.

"You'd be hard-pressed to find any company that doesn't have a beautiful ethics and compliance program," Distelhorst says. "They're talking about it and they're working it all out in various strategic documents. But the question is whether they're actually living by it. Some are, and clearly some aren't."

Regardless of where a company stands in the process, IT leaders should be ready to contribute, he says.

"These policies are worked out on the ethics and compliance committees below the board level, and they're having the CIO as a key player," Distelhorst explains.

That's the case at Intel Corp., says the company's CIO, Diane Bryant.

Intel's Ethics and Compliance Oversight Committee established the following five principles for the company and its workers: Intel should conduct business with honesty and integrity; the company must follow the letter and spirit of the law; employees are expected to treat one another fairly; employees should act in the best interests of Intel and avoid conflicts of interest; and employees must protect the company's assets and reputation.

"Intel's IT staff builds and maintains the systems that allow the company to meet its legal and regulatory requirements. Such as those laid out for accounting and governance by the Sarbanes-Oxley Act," Bryant says.

It also developed applications and a team of workers to handle document retention, which is crucial should there be a legal case with electronic discovery requests.

But IT also enables Intel to enforce its own values and not just meet regulatory requirements, Bryant explains. So there are applications to help perform rigorous checks on suppliers to ensure that they have sufficient business continuity plans and environmental sustainability plans, as well as ethical stances that match Intel's own. IT has also delivered sophisticated systems that monitor the power consumption and carbon dioxide emissions of Intel's data centers. And it developed systems that monitor for potential malicious behavior, such as violations of access management rights or the public release of Intel's intellectual property.

"We put solutions in place that help protect Intel's five principles," Bryant says.

Few companies are that advanced in their use of technology to further an ethical agenda. "Companies recognize that they have to be on record as being committed, but they're not yet as convinced that they have to manage it like other parts of their business," Hanson explains.

But when companies do decide to move in that direction, that's when CIOs can shine, offering ideas on what metrics to use and what to measure.

"That's where IT can be a real leader," Hanson says, "since they know what can be measured and captured."

Source: Adapted from Mary K. Pratt, "Business Ethics Steering Clear of Scandal," *Computerworld*, August 23, 2009; and Mary K. Pratt, "The High Cost of Ethics Compliance," *Computerworld*, August 24, 2009.

CASE STUDY QUESTIONS

1. What are the two meanings of 'corporate ethics' in organizations today? What does each definition imply for IT practices? How does the economic environment affect this?
2. How does IT provide more opportunities for difficult ethics issues to arise? How does IT help address those?
3. Use examples from the case to justify your answer.
4. Should organizations pursue high ethical standards regardless (or in spite of) their bottom-line impact? Or should they limit themselves to those scenarios where "good ethics make for good business"?

REAL WORLD ACTIVITIES

1. The passage of the Sarbanes-Oxley Act in the United States has greatly increased the compliance obligations of publicly traded companies. Go online to research how this landmark legislation affected the obligations of IT departments, and the way in which they develop and implement new technologies. Prepare a presentation to synthesize your findings.
2. Should an IT department hire a more expensive vendor because the vendor shares its own company's ethics standards, or should it go with a lower-cost provider that doesn't? This is an important question posed in the case above. What do you think? Break into small groups with your classmates to discuss your positions. Can you reach a consensus on this issue?

REAL WORLD CASE 2 Wyoming Medical Center, Los Angeles County, and Raymond James: End-Point Security Gets Complicated

Users say protecting network end points is becoming more difficult as the type of endpoint devices—desktops, laptops, smartphones—grows, making security a complex moving target. The problem is compounded by the range of what groups within corporations do on these devices, which translates into different levels of protection for classes of users on myriad devices.

"Deciding the appropriate device defense becomes the No. 1 job of endpoint security specialists," says Jennifer Jabbush, CISO of Carolina Advanced Digital consultancy. Depending on the device and the user's role, end points need to be locked down to a greater or lesser degree.

For instance, Wyoming Medical Center in Casper, Wyoming, has four classifications of PCs: "open PCs in hallways for staff use; PCs at nursing stations; PCs in offices; and PCs on wheels that move between patient rooms and handle very specific, limited applications," says Rob Pettigrew, manager of technical systems and help desk for the center.

Pettigrew is deploying Novell ZenWorks to 850 of the center's 900 PCs in order to make sure each class has the right software. With 110 applications and 40 major medical software systems, that makes a huge matrix of machine types and restrictions to contend with, he says.

In addition, physicians in affiliated clinics can access via SSL VPN (a kind of VPN that is accessible over Web browsers), but they are limited to reaching Web servers in a physician's portal, which is protected from the hospital data network. Some Citrix thin clients are also used to protect data from leaving the network but overall the strategy for unmanaged machines is a work in progress, Pettigrew says. "We're hoping to get more help desk to deal with the external physicians," he says.

One concern that can be addressed by endpoint security is data privacy, which is paramount for the Los Angeles County Department of Health Services in California, says Don Zimmer, information security officer for the department. He supports about 18,000 desktops and laptops and operates under the restrictions of Health Insurance Portability and Accountability Act (HIPAA) regulations. "That means disk encryption," he says.

"If it's not encrypted and there is a breach, then we have to start calling people," he says. To avoid violating patients' privacy and a loss of public trust, the department encrypts the drives of all the PC end points with software from PointSec.

Equally important is keeping sensitive information off movable media that can plug into USB ports. The department uses Safend's USB Port Protector product that either denies access to sensitive documents or requires that they be encrypted and password-protected before being placed on the removable device.

Everyone's talking about the insider threat. But protecting data can't supersede the requirement to give users the access they need to do their jobs—otherwise, soon you'll have neither business data nor employees to worry about.

Striking a balance between access and protection isn't easy, however. In an *InformationWeek* Analytics/DarkReading.com endpoint security survey of 384 business technology pros, 43 percent classify their organizations as "trusting," allowing data to be copied to USB drives or other devices with no restrictions or protective measures.

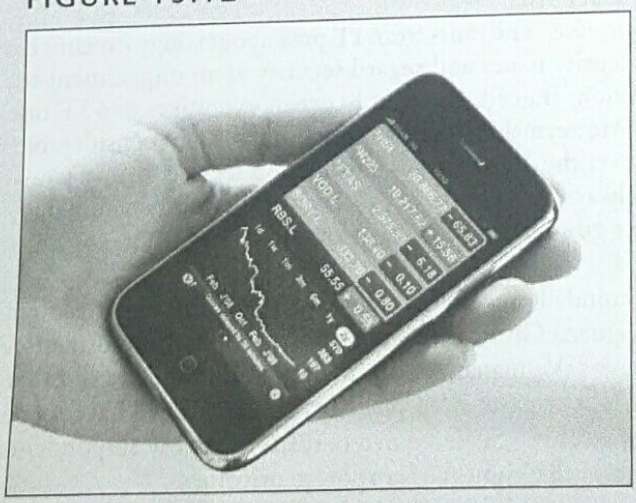
Still, IT is aware of the need to move from a stance of securing end points to assuming that laptops and smartphones will be lost, good employees will go bad, and virtual machines will be compromised. Instead of focusing on end points, let fortifications follow the data: Decide what must be protected, find out everywhere it lives, and lock it down against both inside and outside threats, whether via encryption, multitiered security suites, or new technologies like data loss prevention (DLP).

DLP suites combine network scanning and host-based tools to collect, categorize, and protect corporate intellectual property. These products can maintain an archive of data and documents, along with associated permissions by group, individual, and other policies.

They then actively scan internal networks and external connections looking for anomalies. This takes data protection beyond perimeter or endpoint protection; DLP facilitates internal safety checks, allowing "eyes-only" data to remain eyes only and minimizing the risk that sensitive data will be viewed by the wrong folks, even in-house.

Zimmer says he is looking into DLP software as well that can restrict the access individual devices have to data.

FIGURE 13.12



The proliferation of end-user devices is making endpoint security more important than ever.

Source: © Bloomberg/Getty Images.

Although the technology can be effective, it also requires that businesses locate and classify their data so they can set policies surrounding it—a job that can seem insurmountable, depending on how data have been stored.

For Pettigrew, this means finding the 5 percent of sensitive data stored outside the medical center's electronic medical records system.

Rather than deal with many vendors for specific endpoint protection products, some businesses opt for endpoint security suites, such as those that evolved from the antivirus roots of vendors, including McAfee and Symantec.

Sam Ghelfi, chief security officer at financial firm Raymond James, opted for Sophos's Endpoint Protection and Data Security Suite, which offers firewall, antivirus, data loss prevention, antispyware, encryption, and network access control (NAC). The company wants tight control over the Web content that is available to users to minimize the malware coming in via basic Web browsing. The company uses a Sophos Web proxy that filters sites based on reputation, but also the content that sites return.

Mobile devices that could contain confidential company information are disk encrypted, again using Sophos agents. If a device is lost or stolen, the encryption key is wiped out, making it impossible to decrypt the contents of the hard drive.

Ghelfi says he believes in personal firewalls on individual machines because they can stop groups of devices from talking to other groups. "Centrally managed, they can reveal network traffic patterns," he says.

He doesn't use all of the features of the Sophos suite, though. For instance, he is just getting around to implementing NAC to let unmanaged guest machines get on the network but still minimize risk that they are infected.

That will clear them based on authentication, access method and type of machine, but for contractors that require access to the main network, he also insists that they install the Sophos suite. Other unmanaged machines, such as those of guests, are allowed access only through a dedicated wireless network that leads to a limited set of servers in a network segment flanked by firewalls, he says.

"Such endpoint security suites can be attractive financially," Jabbusch says, "because customers can wind up with reduced agent, license and support fees and less management overhead." There may be a certain amount of convenience if customers decide to layer on more applications within a suite.

The newest class of devices—smartphones—is presenting ongoing challenges as organizations figure out how to deal with them. Particularly dicey is whether to allow employees to use their personally owned devices for business and to access the business network.

The jury is still out, at least among state government chief information officers. A recent survey by the National Association of State Chief Information Officers says that of 36 states responding to a survey, 39 percent say they allow personal smartphones if they are protected by state security measures. Twenty-seven percent say they don't allow personal smartphones on their networks, 17 percent say they are reviewing state policy, and 17 percent say they don't have statewide control—each agency sets its own policies.

A separate Forrester Research survey says that 73 percent of businesses surveyed are at least somewhat concerned about smartphones being authorized for business use. According to DeviceLock, its survey of more than 1000 IT professionals found that fewer than 40 percent of respondents said yes to the question: "Have you taken any steps to secure your business against the security threat posed by iPhones? "Analyzing the responses by region, researchers found that only 25 percent of respondents in North America and Western Europe said yes to the question, suggesting this is a "back burner" security issue, says the endpoint data leak-prevention specialist.

Jabbush says the type of smartphone is a factor. "I can't imagine allowing an iPhone," she says. "A BlackBerry is somewhat better" because BlackBerries have a management infrastructure and the devices can be locked down to corporate policies.

Mobile device security is one of those areas that should get more attention. However, it is likely that this topic will remain buried—until a lost or stolen iPhone leads to a visible and costly security breach.

Source: Adapted from Tim Greene, "Endpoint Security Gets Complicated," *Network World*, April 1, 2010; and Joe Hernick, "InformationWeek Analytics: Endpoint Security and DLP," *InformationWeek*, April 27, 2009.

CASE STUDY QUESTIONS

1. What is the underlying issue behind endpoint security, and why is it becoming even more difficult for companies to address it? Define the problem in your own words using examples from the case.
2. What are the different approaches taken by the organizations in the case to address this issue? What are the advantages and disadvantages of each? Provide at least two examples for each alternative.
3. A majority of respondents to a survey discussed in the case described their company as "trusting." What does this mean? What is the upside of a company being "trusting"? What is the downside? Provide some examples to illustrate your answers.

REAL WORLD ACTIVITIES

1. Data loss prevention (DLP) was a technology mentioned in the case, and one that is garnering more and more attention from corporate security departments. Go online and research what DLP involves, and look for examples of its application to actual problems, and their outcomes. Prepare a report to summarize your work.
2. Whether to allow employees to use their own smartphones (or other devices yet to be invented) on corporate networks is quickly becoming a contested issue. What do companies stand to gain, or lose, in either case? What about employees? Break into small groups with your classmates to discuss these questions.

REAL WORLD CASE 3

Ethics, Moral Dilemmas, and Tough Decisions: The Many Challenges of Working in IT

What Bryan found on an executive's computer six years ago still weighs heavily on his mind. He's particularly troubled that the man he discovered using a company PC to view pornography of Asian women and of children was subsequently promoted and moved to China to run a manufacturing plant. "To this day, I regret not taking that stuff to the FBI." It happened when Bryan, who asked that his last name not be published, was IT director at the U.S. division of a $500 million multinational corporation based in Germany.

The company's Internet usage policy, which Bryan helped develop with input from senior management, prohibited the use of company computers to access pornographic or adult-content Web sites. One of Bryan's duties was to use products from SurfControl PLC to monitor employee Web surfing and to report any violations to management.

Bryan knew that the executive, who was a level above him in another department, was popular within both the U.S. division and the German parent. Yet when the tools turned up dozens of pornographic Web sites visited by the executive's computer, Bryan followed the policy.

"That's what it's there for. I wasn't going to get into trouble for following the policy," he reasoned.

Bryan's case is a good example of the ethical dilemmas that IT workers may encounter on the job. IT employees have privileged access to digital information, both personal and professional, throughout the company, and they have the technical prowess to manipulate that information. That gives them both the power and responsibility to monitor and report employees who break company rules. IT professionals may also uncover evidence that a coworker is, say, embezzling funds, or they could be tempted to peek at private salary information or personal e-mails. There's little guidance, however, on what to do in these uncomfortable situations.

In the case of the porn-viewing executive, Bryan didn't get into trouble, but neither did the executive, who came up with "a pretty outlandish explanation" that the company accepted, Bryan says. He considered going to the FBI, but the Internet bubble had just burst and jobs were hard to come by. "It was a tough choice," Bryan says. "But I had a family to feed."

Perhaps it would ease Bryan's conscience to know that he did just what labor attorney Linn Hynds, a senior partner at Honigman Miller Schwartz and Cohn LLP, would have advised in his case. "Let the company handle it," she says. "Make sure you report violations to the right person in your company, and show them the evidence. After that, leave it to the people who are supposed to be making that decision." Ideally, corporate policy takes over where the law stops, governing workplace ethics to clear up gray areas and remove personal judgment from the equation as much as possible.

"If you don't set out your policy and your guidelines, if you don't make sure that people know what they are and understand them, you're in no position to hold workers accountable," says John Reece, a former chief information officer at the Internal Revenue Service and Time Warner Inc.

Having clear ethical guidelines also lets employees off the hook emotionally if the person they discover breaking the policy is a friend, someone who reports to them directly, or a supervisor, says Reece, who is now head of consultancy at John C. Reece and Associates LLC. Organizations that have policies in place often focus on areas where they had trouble in the past or emphasize whatever they are most worried about. When Reece was at the IRS, for example, the biggest emphasis was on protecting the confidentiality of taxpayer information.

At the U.S. Department of Defense, policies usually emphasize procurement rules, notes Stephen Northcutt, president of the SANS Technology Institute and author of *IT Ethics Handbook: Right and Wrong for IT Professionals*. Adding to the complexity, an organization that depends on highly skilled workers might be more lenient. When Northcutt worked in IT security at the Naval Surface Warfare Center in Virginia, it was a rarefied atmosphere of highly sought-after PhDs. "I was told pretty clearly that if I made a whole lot of PhDs very unhappy so that they left, the organization wouldn't need me anymore," says Northcutt.

Of course, that wasn't written in any policy manual, so Northcutt had to read between the lines. "The way I interpreted it was: Child pornography, turn that in," he says. "But if the leading mathematician wants to download some pictures of naked girls, they didn't want to hear from me."

Northcutt says that he did find child porn on two occasions and that both events led to prosecution. As for other offensive photos that he encountered, Northcutt pointed out to his superiors that there might be a legal liability, citing a Supreme Court decision that found that similar pictures at a military installation indicated a pervasive atmosphere of sexual harassment. That did the trick. "Once they saw that law was involved, they were more willing to change culture and policy," Northcutt says.

When policies aren't clear, ethical decisions are left to the judgment of IT employees, which varies by person and the particular circumstances. For example, Gary, a director of technology at a nonprofit organization in the Midwest, flat-out refused when the assistant chief executive officer wanted to use a mailing list that a new employee had stolen from her former employer. Yet Gary, who asked that his last name not be used, didn't stop his boss from installing unlicensed software on PCs for a short time, although he refused to do it himself. "The question is, how much was it really going to hurt anybody? We were still going to have 99.5 percent compliant software. I was OK with that."

He says he uninstalled it, with his boss's approval, as soon as he could, which was about a week later.

Northcutt argues that the IT profession should have two things that professions such as law or accounting have had for years: a code of ethics and standards of practice. That way, when company policy is nonexistent or unclear, IT professionals still have standards to follow.

That might be useful for Tim, a systems administrator who works at a Fortune 500 agricultural business. When Tim, who asked that his last name not be published, happened across an unencrypted spreadsheet of salary information on a manager's PC, he copied it. He didn't share the information with anyone or use it to his advantage. It was an impulsive act, he admits, that stemmed from frustration with his employer. "I didn't take it for nefarious reasons; I just took it to prove that I could," he says.

Tim's actions point to a disturbing trend: IT workers are justifying their ethically questionable behavior. That path can end in criminal activity, says fraud investigator Chuck Martell. "We started seeing a few cases about seven or eight years ago," says Martell, managing director of investigative services at Veritas Global LLC, a security firm in Southfield, Michigan. "Now we're investigating a tremendous amount of them."

Whole Foods Market Chairman and CEO John Mackey spent years earning a positive reputation as a corporate leader who was not afraid to take a stand on ethics issues. Before other companies figured out that it pays to be environmentally friendly, Whole Foods led by setting standards for humane animal treatment. In 2006, Mackey took the bold step of reducing his own annual salary to one dollar, pledging money instead for an emergency fund for his staff. Not shy about expressing his views, Mackey challenged leading thinkers, like Nobel Prize–winner Milton Friedman, on business ethics issues. Like many leaders, Mackey seemed to relish the public spotlight.

On July 20, 2007, however, Mackey got more than he bargained for in terms of publicity. *The Wall Street Journal* reported that Mackey had long used the pseudonym "Rahodeb" to make postings in Yahoo Finance forums that flattered his own company and leveled criticisms against the competition. Serious financial and possibly legal repercussions continue to unfold from this incident, and the final consequences may not be known for some time.

Amid the furor that followed this disclosure of Mackey's secret online alias, it is vital that we not lose sight of the critical issues it raises about ethics and leadership in a rapidly evolving business world. There is no question that the current climate has prompted many more companies to tackle ethics issues.

By now, "business ethics" is an established part of doing business, not just in the United States, but also increasingly around the world. People no longer joke that "business ethics is an oxymoron," as society has come not merely to expect, but to demand, that business conduct itself according to basic rules of ethics and integrity. Business will always need to pay attention to ethics and leadership, but these lessons are continually challenged by new developments, including technological advances that promote new kinds of communication online. Business leaders cannot afford to overlook these challenges, as even a single misstep can be enough to undo a reputation for ethical leadership.

Source: Adapted from Tam Harbert, "Ethics in IT: Dark Secrets, Ugly Truths—and Little Guidance," *Computerworld*, October 29, 2007; and David Schmidt, "What Is the Moral Responsibility of a Business Leader?" *CIO Magazine*, September 12, 2007.

CASE STUDY QUESTIONS

1. Companies are developing ethical policies and guidelines for legal reasons, but also to clarify what is acceptable and what is not. Do you think any of the issues raised in the case required clarification? Would you take exception to any of them being classified as inappropriate behavior? Why do you think these things happen anyway?
2. In the first example (Bryan's), it is apparent that he did not believe justice had been ultimately served by the decision his company made. Should he have taken the issue to the authorities? Or was it enough that he reported the problem through the proper channels and let the organization handle it, as was the recommendation of Linn Hynds? Provide a rationale for the position you are willing to take on this matter.
3. In the case, Gary chose not to stop his boss from installing unlicensed software, although he refused to do it himself. If installing unlicensed software is wrong, is there any difference between refusing to do it versus not stopping somebody else? Do you buy his argument that it was not really going to hurt anybody? Why or why not?

REAL WORLD ACTIVITIES

1. Go online to follow up on John Mackey's story and search for other instances of debatable behavior where IT has been an important factor. Are the ones featured in the case exceptions, or are these occurrences becoming more and more common? How do organizations seem to be coping with these issues? What type of responses did you find? Prepare a report to summarize your findings.
2. The case features many examples of what is arguably unethical behavior, including child pornography, accessing adult content on company-owned equipment, installing unlicensed software, and so on. Are some of these practices "more wrong" than others? Is there any one that you would not consider problematic? Break into small groups to discuss these questions, and make a list of other ethical problems involving IT that were not mentioned in the case.

REAL WORLD CASE 4

Raymond James Financial, BCD Travel, Houston Texans, and Others: Worrying about What Goes Out, Not What Comes In

It's not what's coming into the corporate network that concerns Gene Fredriksen; it's what's going out. For the chief security officer at securities brokerage Raymond James Financial Inc. in St. Petersburg, Florida, leakage of sensitive customer data or proprietary information is the new priority. The problem isn't just content within e-mail messages, but the explosion of alternative communication mechanisms that employees are using, including instant messaging, blogs, FTP transfers, Web mail, and message boards. It's not enough to just monitor e-mail, Fredriksen says. "We have to evolve and change at the same pace as the business," he explains. "Things are coming much faster."

So Fredriksen is rolling out a network-based outbound content monitoring and control system. The software, from San Francisco–based Vontu Inc., sits on the network and monitors traffic in much the same way that a network-based intrusion-detection system would. Rather than focusing on inbound traffic, however, Vontu monitors the network activity that originates from Raymond James's 16,000 users. It examines the contents of each network packet in real time and issues alerts when policy violations are found.

Network-based systems do more than just rule-based scanning for Social Security numbers and other easily identifiable content. They typically analyze sensitive documents and content types and generate a unique fingerprint for each. Administrators then establish policies that relate to that content, and the system uses linguistic analysis to identify sensitive data and enforce those policies as information moves across the corporate LAN. The systems can detect both complete documents and "derivative documents," such as an IM exchange in which a user has pasted a document fragment.

When BCD Travel began to investigate what it would take to get Payment Card Industry (PCI) certification for handling customer credit card data, Brian Flynn, senior vice president of technology, realized that he didn't really know how his employees were handling such information. Not only could PCI certification be denied, but the travel agency's reputation and business could also be harmed. At the National Football League's Houston Texans, IT Director Nick Ignatiev came to the same realization as he investigated PCI certification.

In both cases, vendors they'd been working with suggested a new technology: outbound content management tools that look for proprietary information that might be leaving the company via e-mail, instant messaging, or other avenues. Flynn started to use Reconnex's iGuard network appliance, with vivid results. "It was a shock to see what was going out, and that gave us the insight to take action," he says. After Ignatiev examined his message flow using Palisade Systems's PacketSure appliance, he too realized that his employees needed to do a better job protecting critical data, including customer credit cards, scouting reports, and team rosters.

How does the technology work? Basically, the tools filter outgoing communication across a variety of channels, such as e-mail and IM, to identify sensitive information. They're based on some of the same technologies—like pattern matching and contextual text search—that help antivirus and antispam tools block incoming threats.

Tools typically come with basic patterns already defined for personally identifiable information, such as Social Security and credit card numbers, as well as templates for commonly private information, such as legal filings, personnel data, and product testing results.

Companies typically look for three types of information using these tools, notes Paul Kocher, president of the Cryptography Research consultancy. The first, and easiest, type is personally identifiable information, such as Social Security numbers and credit card information. The second type is confidential company information, such as product specifications, payroll information, legal files, or supplier contracts. Although this information is harder to identify, most tools can uncover patterns of language and presentation when given enough samples, Kocher notes. The third category is inappropriate use of company resources, such as potentially offensive communications involving race.

The traditional security methods may restrict sensitive data to legitimate users, but Flynn and Ignatiev found that even legitimate users were putting the data, and their companies, at risk. At BCD Travel, a corporate travel service, nearly 80 percent of its 10,000 employees work in call centers and thus have legitimate access to sensitive customer information. BCD and the Texans did not find malicious activity; instead, they found people who were unaware of security risks, such as sending a customer's credit card number by e-mail to book a flight or room from a vendor that didn't have an online reservations system.

Fidelity Bancshares Inc. in West Palm Beach, Florida, is using the message-blocking feature in PortAuthority from PortAuthority Technologies Inc. in Palo Alto, California. Outbound e-mail messages that contain Social Security numbers, account numbers, loan numbers, or other personal financial data are intercepted and returned to the user, along with instructions on how to send the e-mail securely.

Joe Cormier, vice president of network services, says he also uses PortAuthority to catch careless replies. Customers often send in questions and include their account information. "The customer service rep would reply back without modifying the e-mail," he says.

"The challenge with any system like this is they're only as valuable as the mitigation procedures you have on the back end," notes Fredriksen. Another key to success is educating users about monitoring to avoid "Big Brother" implications. "We are making sure that the users understand why we implement systems like this and what they're being used for, he says.

Mark Rizzo, vice president of operations and platform engineering at Perpetual Entertainment Inc. in San Francisco, learned in a previous job the consequences of not protecting intellectual property. "I have been on the side of things disappearing and showing up at competitors," he says. The start-up online game developer deployed Tablus's Content Alarm to remedy the problem. Rizzo uses it to look for suspicious activity, such as large files that are moving outside the corporate LAN. Now that the basic policies and rules have been set, the system doesn't require much ongoing maintenance, he says. Still, Rizzo doesn't use blocking because he would need to spend significant amounts of time to create more policies in order to avoid false positives.

Although companies in highly regulated industries can justify investing in outbound content monitoring and blocking tools, other organizations may have to sharpen their pencils to justify the cost. These are very expensive solutions to deploy. Fredriksen, who built a system to support 16,000 users, says that for a setup with about 20,000 users, "you're in the $200,000 range, easily."

With outbound content management tools, "you can build very sophisticated concept filters," says Cliff Shnier, vice president for the financial advisory and litigation practice at Aon Consulting. Typically, the tools come with templates for types of data that most enterprises want to filter, and they can analyze contents of servers and databases to derive filters for company-specific information, he says. (Consulting firms can improve these filters using linguists and subject matter experts.)

As any user of an antispam tool knows, no filter is perfect. "A big mistake is to have too much faith in the tools. They can't replace trust and education," says consultant Kocher. They also won't stop a determined thief, he says.

Even when appropriately deployed, these tools don't create an ironclad perimeter around the enterprise. For example, they can't detect information that flows through Skype voice over IP (VoIP) service or SSL (Secure Sockets Layer) connections, Kocher notes. They can also flood logs with false positives, which makes it hard for IT security staff to identify real problems.

That's why chief information officers should look at outbound content management as a supplemental tool to limit accidental or unknowing communication of sensitive data, not as the primary defense. Fredriksen says that although Vontu is important, it's still just one piece of a larger strategy that includes an overlapping set of controls that Raymond James uses to combat insider threats. "This augments the intrusion–detection and firewall systems we have that control and block specific ports," he says. "It's just a piece. It's not the Holy Grail."

Source: Adapted from Galen Gruman, "Boost Security with Outbound Content Management," *CIO Magazine*, April 9, 2007; and Robert Mitchell, "Border Patrol: Content Monitoring Systems Inspect Outbound Communications," *Computerworld*, March 6, 2006.

CASE STUDY QUESTIONS

1. Barring illegal activities, why do you think that employees in the organizations featured in the case do not realize themselves the dangers of loosely managing proprietary and sensitive information? Would you have thought of these issues?
2. How should organizations strike the right balance between monitoring and invading their employees' privacy, even if it would be legal for them to do so? Why is it important that companies achieve this balance? What would be the consequences of being too biased to one side?
3. The IT executives in the case all note that outbound monitoring and management technologies are only part of an overall strategy, and not their primary defense. What should be the other components of this strategy? How much weight would you give to human and technological factors? Why?

REAL WORLD ACTIVITIES

1. Technologies such as VoIP used by Skype and similar products make it more difficult to monitor outgoing information. Search the Internet to help you understand these technologies and why these problems arise. Other than banning them, what alternatives would you suggest to companies facing this problem? Prepare a presentation to deliver your recommendations.
2. As a customer of many of the companies noted in the case, or others in the same industries, what is your expectation about the measures and safeguards that these organizations have implemented to protect inappropriate leaking of your personal information? After reading the case, has your expectation changed? Break into small groups with your classmates to discuss these issues.