August 2012

Facing IT Risk Head-on

Internal audit departments must confront constantly emerging technology threats without losing sight of previous dangers that never go away.

Russell A. Jackson

If you dined on spaghetti and meatballs in 1982 and paid with a credit card, your server likely took the card to the manager's office and looked up the 16-digit account number in a several-hundred-page publication to see if it had been reported lost or stolen. The whole process took several minutes, and if the number appeared in the listing, which was updated every month and mailed to every merchant that accepted the card, the server had to call a credit card company representative to determine whether to process the charge or confiscate the card.

If you order your dinner in 2012 from a local bistro with delivery service, the restaurant likely knows from your telephone number that you ordered the same dish a week earlier and that you always ask for bleu cheese dressing on the side of your salad. When the driver arrives with your order, he or she probably will be carrying a hand-held mobile card-swiping device that prints a receipt for you on the spot — unless your credit card is defective or you're trying to use it illegally. In that case, the device rejects it, and you go hungry.

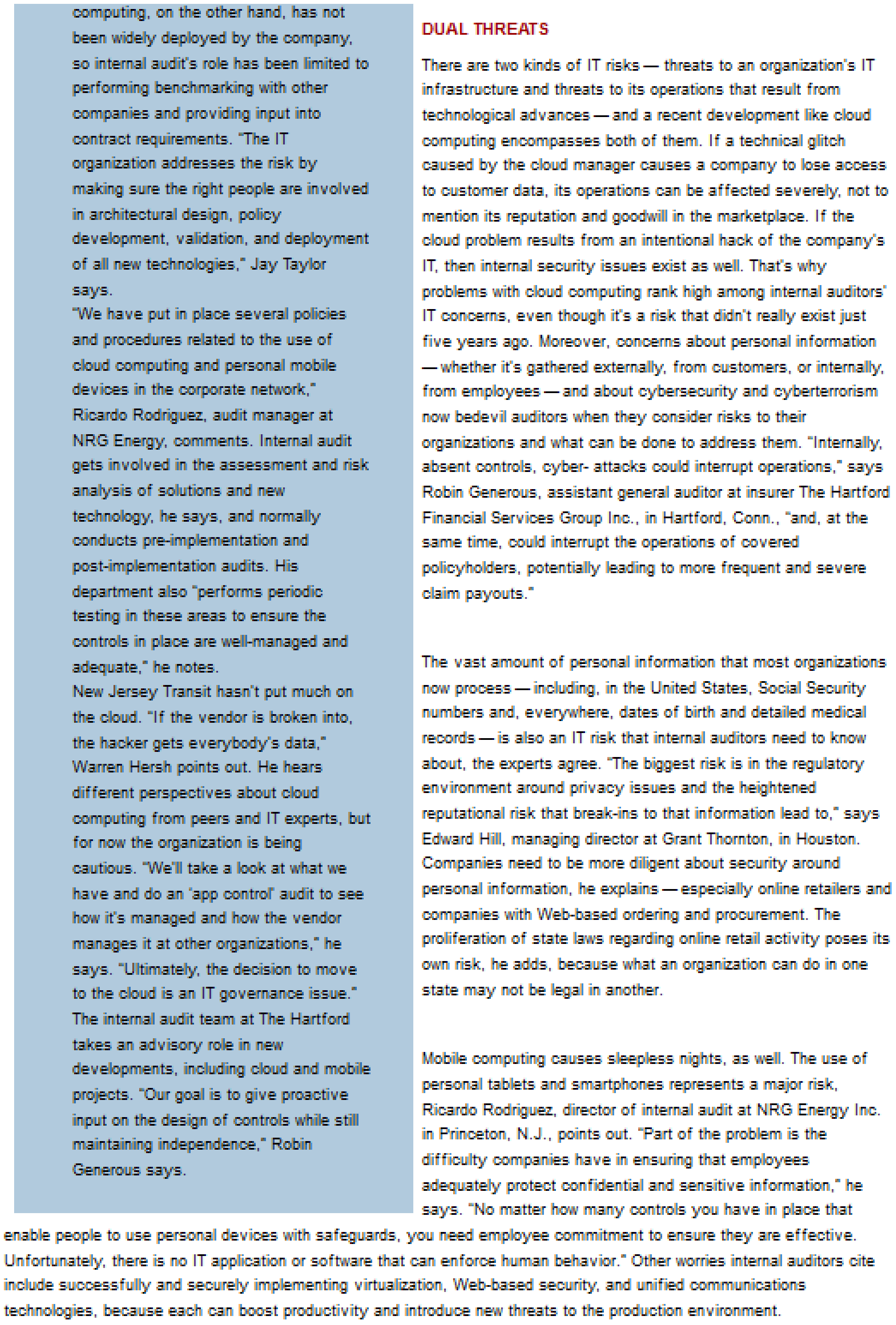
IT has transformed business in profound ways. Customers have avenues of access to companies and their products and services that makes buying something as easy as clicking a mouse. At the same time, businesses can gather data about those customers far faster than any focus group could and then slice and dice the numbers to determine both what those customers are likely to buy and the best way to convince them to buy it.

But that transformation has brought with it risks to the business that simply didn't exist before today's age of electronic communications saturation (see "IT Risk at Hyperspeed" on page 40). IT risks have piled up over a surprisingly few years because the technology that carries the information has evolved so rapidly — leaving legacy risks in place even as it creates new risks to worry about. For internal auditors, that means risks from the past are still part of their audit plan, even as concerns about the impact of new and evolving technologies start to pile up. And because IT risks can be the most insidious of all, auditors must ensure their IT risk assessment skills are optimized.

Cloud and Mobile Risks
Two of the key IT risks internal auditors address are cloud computing and mobile communications. Here are the experts' suggestions for handling them.

> Because General Motors has been a heavy user of mobile technologies for many years, its internal audit department is well-versed in assessing installed solutions and global policies. Cloud

Continued…



computing, on the other hand, has not been widely deployed by the company, so internal audit's role has been limited to performing benchmarking with other companies and providing input into contract requirements. "The IT organization addresses the risk by making sure the right people are involved in architectural design, policy development, validation, and deployment of all new technologies," Jay Taylor says.

"We have put in place several policies and procedures related to the use of cloud computing and personal mobile devices in the corporate network," Ricardo Rodriguez, audit manager at NRG Energy, comments. Internal audit gets involved in the assessment and risk analysis of solutions and new technology, he says, and normally conducts pre-implementation and post-implementation audits. His department also "performs periodic testing in these areas to ensure the controls in place are well-managed and adequate," he notes.

New Jersey Transit hasn't put much on the cloud. "If the vendor is broken into, the hacker gets everybody's data," Warren Hersh points out. He hears different perspectives about cloud computing from peers and IT experts, but for now the organization is being cautious. "We'll take a look at what we have and do an 'app control' audit to see how it's managed and how the vendor manages it at other organizations," he says. "Ultimately, the decision to move to the cloud is an IT governance issue."

The internal audit team at The Hartford takes an advisory role in new developments, including cloud and mobile projects. "Our goal is to give proactive input on the design of controls while still maintaining independence," Robin Generous says.

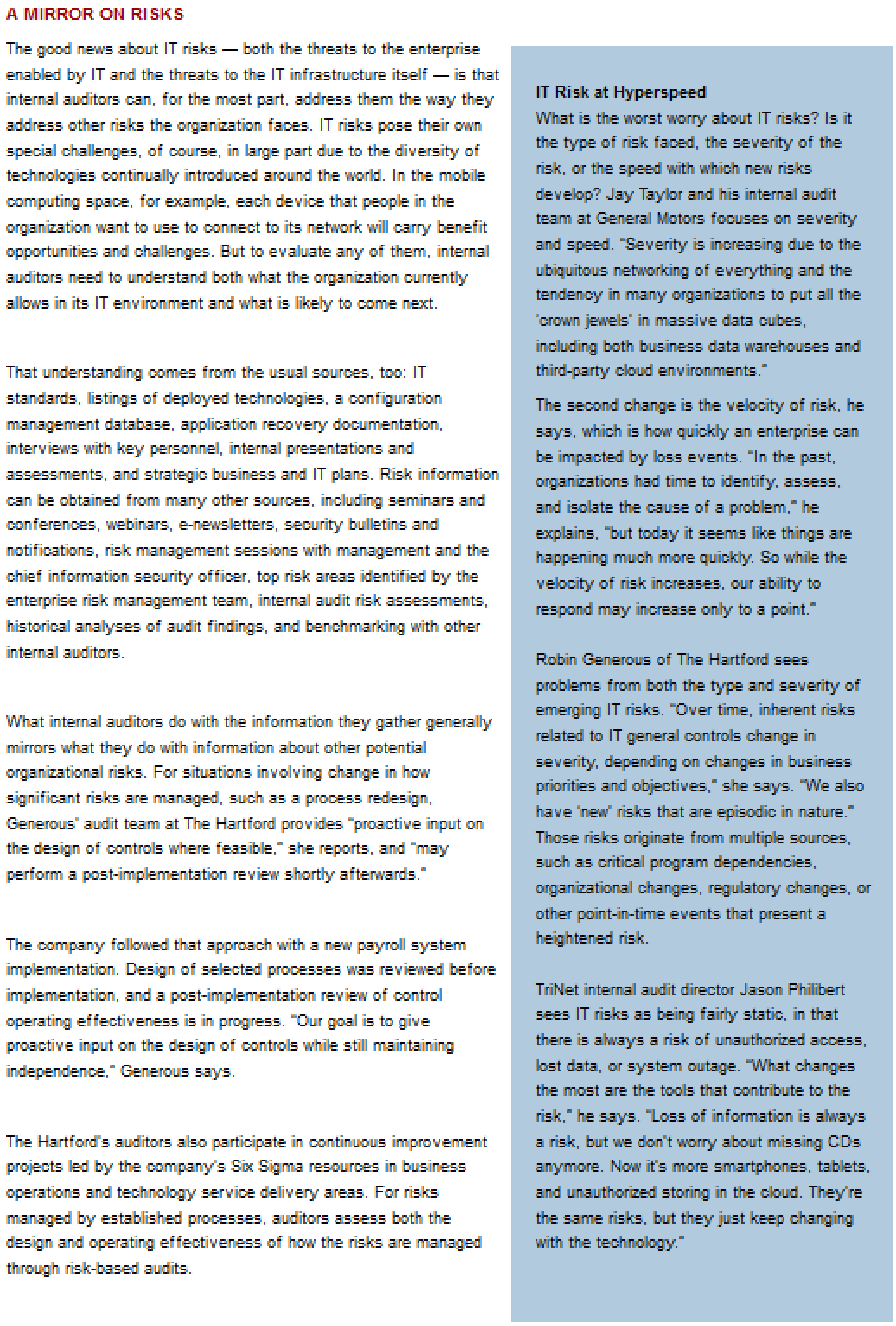
DUAL THREATS

There are two kinds of IT risks — threats to an organization's IT infrastructure and threats to its operations that result from technological advances — and a recent development like cloud computing encompasses both of them. If a technical glitch caused by the cloud manager causes a company to lose access to customer data, its operations can be affected severely, not to mention its reputation and goodwill in the marketplace. If the cloud problem results from an intentional hack of the company's IT, then internal security issues exist as well. That's why problems with cloud computing rank high among internal auditors' IT concerns, even though it's a risk that didn't really exist just five years ago. Moreover, concerns about personal information — whether it's gathered externally, from customers, or internally, from employees — and about cybersecurity and cyberterrorism now bedevil auditors when they consider risks to their organizations and what can be done to address them. "Internally, absent controls, cyber- attacks could interrupt operations," says Robin Generous, assistant general auditor at insurer The Hartford Financial Services Group Inc., in Hartford, Conn., "and, at the same time, could interrupt the operations of covered policyholders, potentially leading to more frequent and severe claim payouts."

The vast amount of personal information that most organizations now process — including, in the United States, Social Security numbers and, everywhere, dates of birth and detailed medical records — is also an IT risk that internal auditors need to know about, the experts agree. "The biggest risk is in the regulatory environment around privacy issues and the heightened reputational risk that break-ins to that information lead to," says Edward Hill, managing director at Grant Thornton, in Houston. Companies need to be more diligent about security around personal information, he explains — especially online retailers and companies with Web-based ordering and procurement. The proliferation of state laws regarding online retail activity poses its own risk, he adds, because what an organization can do in one state may not be legal in another.

Mobile computing causes sleepless nights, as well. The use of personal tablets and smartphones represents a major risk, Ricardo Rodriguez, director of internal audit at NRG Energy Inc. in Princeton, N.J., points out. "Part of the problem is the difficulty companies have in ensuring that employees adequately protect confidential and sensitive information," he says. "No matter how many controls you have in place that enable people to use personal devices with safeguards, you need employee commitment to ensure they are effective. Unfortunately, there is no IT application or software that can enforce human behavior." Other worries internal auditors cite include successfully and securely implementing virtualization, Web-based security, and unified communications technologies, because each can boost productivity and introduce new threats to the production environment.

Continued…



A MIRROR ON RISKS

The good news about IT risks — both the threats to the enterprise enabled by IT and the threats to the IT infrastructure itself — is that internal auditors can, for the most part, address them the way they address other risks the organization faces. IT risks pose their own special challenges, of course, in large part due to the diversity of technologies continually introduced around the world. In the mobile computing space, for example, each device that people in the organization want to use to connect to its network will carry benefit opportunities and challenges. But to evaluate any of them, internal auditors need to understand both what the organization currently allows in its IT environment and what is likely to come next.

That understanding comes from the usual sources, too: IT standards, listings of deployed technologies, a configuration management database, application recovery documentation, interviews with key personnel, internal presentations and assessments, and strategic business and IT plans. Risk information can be obtained from many other sources, including seminars and conferences, webinars, e-newsletters, security bulletins and notifications, risk management sessions with management and the chief information security officer, top risk areas identified by the enterprise risk management team, internal audit risk assessments, historical analyses of audit findings, and benchmarking with other internal auditors.

What internal auditors do with the information they gather generally mirrors what they do with information about other potential organizational risks. For situations involving change in how significant risks are managed, such as a process redesign, Generous' audit team at The Hartford provides "proactive input on the design of controls where feasible," she reports, and "may perform a post-implementation review shortly afterwards."

The company followed that approach with a new payroll system implementation. Design of selected processes was reviewed before implementation, and a post-implementation review of control operating effectiveness is in progress. "Our goal is to give proactive input on the design of controls while still maintaining independence," Generous says.

The Hartford's auditors also participate in continuous improvement projects led by the company's Six Sigma resources in business operations and technology service delivery areas. For risks managed by established processes, auditors assess both the design and operating effectiveness of how the risks are managed through risk-based audits.

IT Risk at Hyperspeed

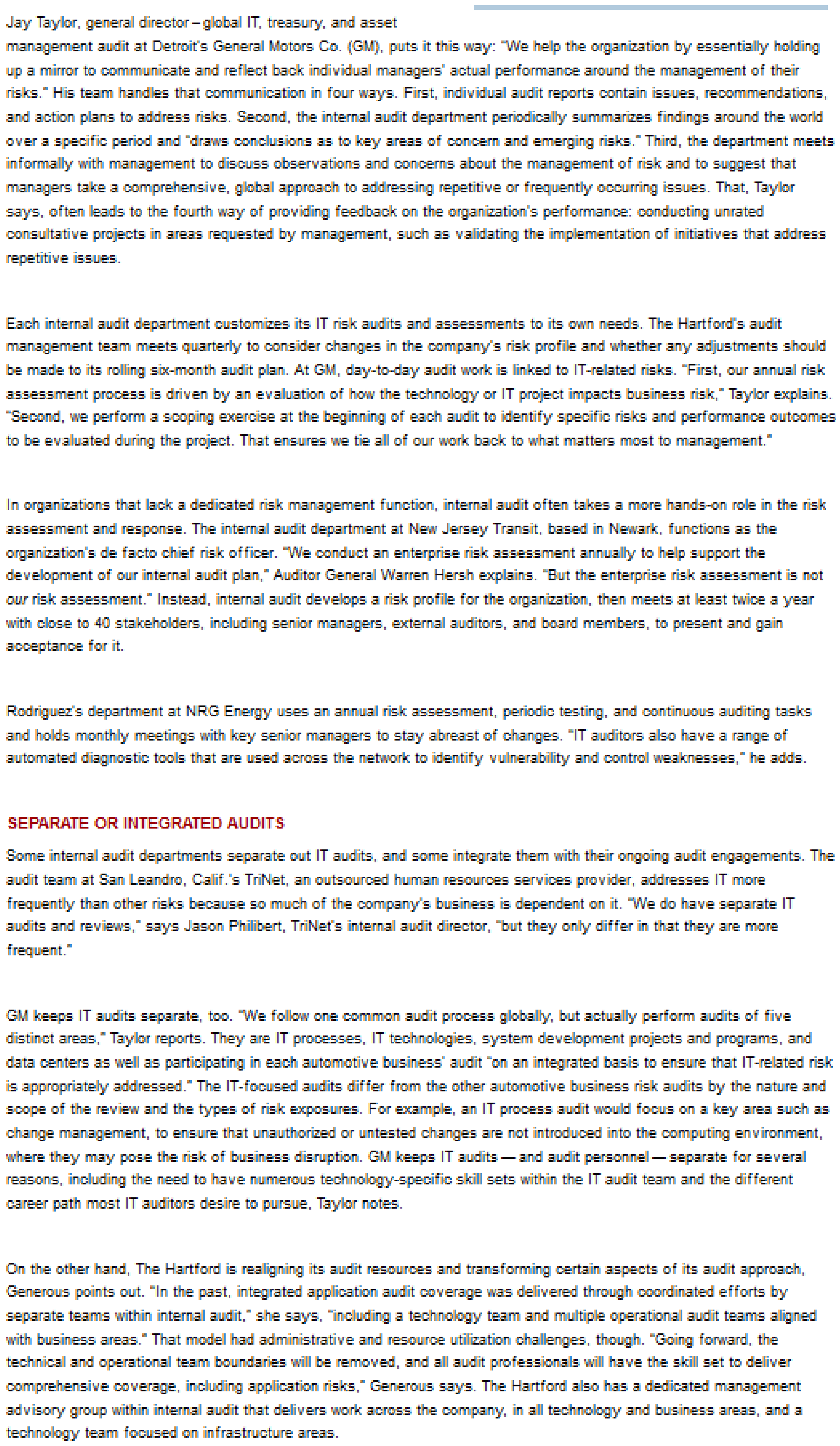
What is the worst worry about IT risks? Is it the type of risk faced, the severity of the risk, or the speed with which new risks develop? Jay Taylor and his internal audit team at General Motors focuses on severity and speed. "Severity is increasing due to the ubiquitous networking of everything and the tendency in many organizations to put all the 'crown jewels' in massive data cubes, including both business data warehouses and third-party cloud environments."

The second change is the velocity of risk, he says, which is how quickly an enterprise can be impacted by loss events. "In the past, organizations had time to identify, assess, and isolate the cause of a problem," he explains, "but today it seems like things are happening much more quickly. So while the velocity of risk increases, our ability to respond may increase only to a point."

Robin Generous of The Hartford sees problems from both the type and severity of emerging IT risks. "Over time, inherent risks related to IT general controls change in severity, depending on changes in business priorities and objectives," she says. "We also have 'new' risks that are episodic in nature." Those risks originate from multiple sources, such as critical program dependencies, organizational changes, regulatory changes, or other point-in-time events that present a heightened risk.

TriNet internal audit director Jason Philibert sees IT risks as being fairly static, in that there is always a risk of unauthorized access, lost data, or system outage. "What changes the most are the tools that contribute to the risk," he says. "Loss of information is always a risk, but we don't worry about missing CDs anymore. Now it's more smartphones, tablets, and unauthorized storing in the cloud. They're the same risks, but they just keep changing with the technology."

Continued…



Jay Taylor, general director – global IT, treasury, and asset management audit at Detroit's General Motors Co. (GM), puts it this way: "We help the organization by essentially holding up a mirror to communicate and reflect back individual managers' actual performance around the management of their risks." His team handles that communication in four ways. First, individual audit reports contain issues, recommendations, and action plans to address risks. Second, the internal audit department periodically summarizes findings around the world over a specific period and "draws conclusions as to key areas of concern and emerging risks." Third, the department meets informally with management to discuss observations and concerns about the management of risk and to suggest that managers take a comprehensive, global approach to addressing repetitive or frequently occurring issues. That, Taylor says, often leads to the fourth way of providing feedback on the organization's performance: conducting unrated consultative projects in areas requested by management, such as validating the implementation of initiatives that address repetitive issues.

Each internal audit department customizes its IT risk audits and assessments to its own needs. The Hartford's audit management team meets quarterly to consider changes in the company's risk profile and whether any adjustments should be made to its rolling six-month audit plan. At GM, day-to-day audit work is linked to IT-related risks. "First, our annual risk assessment process is driven by an evaluation of how the technology or IT project impacts business risk," Taylor explains. "Second, we perform a scoping exercise at the beginning of each audit to identify specific risks and performance outcomes to be evaluated during the project. That ensures we tie all of our work back to what matters most to management."

In organizations that lack a dedicated risk management function, internal audit often takes a more hands-on role in the risk assessment and response. The internal audit department at New Jersey Transit, based in Newark, functions as the organization's de facto chief risk officer. "We conduct an enterprise risk assessment annually to help support the development of our internal audit plan," Auditor General Warren Hersh explains. "But the enterprise risk assessment is not *our* risk assessment." Instead, internal audit develops a risk profile for the organization, then meets at least twice a year with close to 40 stakeholders, including senior managers, external auditors, and board members, to present and gain acceptance for it.

Rodriguez's department at NRG Energy uses an annual risk assessment, periodic testing, and continuous auditing tasks and holds monthly meetings with key senior managers to stay abreast of changes. "IT auditors also have a range of automated diagnostic tools that are used across the network to identify vulnerability and control weaknesses," he adds.

SEPARATE OR INTEGRATED AUDITS

Some internal audit departments separate out IT audits, and some integrate them with their ongoing audit engagements. The audit team at San Leandro, Calif.'s TriNet, an outsourced human resources services provider, addresses IT more frequently than other risks because so much of the company's business is dependent on it. "We do have separate IT audits and reviews," says Jason Philibert, TriNet's internal audit director, "but they only differ in that they are more frequent."

GM keeps IT audits separate, too. "We follow one common audit process globally, but actually perform audits of five distinct areas," Taylor reports. They are IT processes, IT technologies, system development projects and programs, and data centers as well as participating in each automotive business' audit "on an integrated basis to ensure that IT-related risk is appropriately addressed." The IT-focused audits differ from the other automotive business risk audits by the nature and scope of the review and the types of risk exposures. For example, an IT process audit would focus on a key area such as change management, to ensure that unauthorized or untested changes are not introduced into the computing environment, where they may pose the risk of business disruption. GM keeps IT audits — and audit personnel — separate for several reasons, including the need to have numerous technology-specific skill sets within the IT audit team and the different career path most IT auditors desire to pursue, Taylor notes.

On the other hand, The Hartford is realigning its audit resources and transforming certain aspects of its audit approach, Generous points out. "In the past, integrated application audit coverage was delivered through coordinated efforts by separate teams within internal audit," she says, "including a technology team and multiple operational audit teams aligned with business areas." That model had administrative and resource utilization challenges, though. "Going forward, the technical and operational team boundaries will be removed, and all audit professionals will have the skill set to deliver comprehensive coverage, including application risks," Generous says. The Hartford also has a dedicated management advisory group within internal audit that delivers work across the company, in all technology and business areas, and a technology team focused on infrastructure areas.

Continued…

At New Jersey Transit, Hersh operates a fairly integrated department as well. "Every one of our internal auditors — financial or IT — is required to take the same seminars exposing them to the latest issues regarding IT risk and emerging IT issues," he says. Rodriguez's team at NRG Energy performs integrated audits that cover IT general controls related to a system or application that supports a main process or department, as well as IT-specific audits such as network security and application reviews. IT auditors with more specialized skills work alongside operations auditors. "On the integrated audits, we generally cover only those controls that relate to the particular process," he says. "On the IT-specific audits, we review all the controls from beginning to end."

NO END TO SLEEPLESS NIGHTS

If it sounds as though awareness of IT risks permeates just about everything internal auditors do, that's because it does. IT simply has become that integral to just about every move any organization makes. "While changes in business environments have refocused and, in some cases, redirected where the more significant IT risks exist," Generous points out, "inherent risk areas — such as availability, information protection, and data integrity — simply adjust over time in relation to business changes."

Indeed, IT risks' frustrating habit of proliferating, rather than just changing over time, is a common concern among internal auditors who must provide assurance on them. "Controls have improved, but so have hackers, so the issues that used to keep IT auditors up at night are still there," Rodriguez says. Given the severity of the risks that IT poses and the calamitous effects those risks could have on an enterprise, however, some sleeplessness might be merited.

Translating IT Risk Into Business Terms

It doesn't matter how skillfully an internal audit department assesses IT risks. If it can't get the message out to management — which owns the risk and the solutions used to address it — the assessment might as well not take place. Internal auditors who are experienced at making themselves heard offer these tips:

> General Motors' Jay Taylor concedes that IT auditors aren't always adept at communicating issues to management. "The reason is they often write their findings from a technical, rather than a business, standpoint," he says. To be effective, IT auditors must describe the business significance of their findings "in the language management understands." For example, they can connect a control weakness to the specific business information, system functionality, or process that would concern executives.
>
> Robin Generous of The Hartford encourages discussions about IT risk to be "business-driven," too. "We should view governance holistically, rather than only focusing on IT," she says.
>
> Warren Hersh, with New Jersey Transit, also recommends explaining IT risks in a language the listener speaks. "We try to increase awareness out in the units about what could happen," he says. "We explain what can go wrong and get their perspective on it." His department starts with a risk inventory of 45 or so things that can go wrong — whether financial, terrorism-related, or something else. The internal audit team then "rolls that up into the top seven or eight, and we discuss the rationale behind each with management," he says.

Russell A. Jackson is a freelance writer based in West Hollywood, Calif.