Mobile Computing

Internal auditors and management need to understand the risks surrounding rapidly changing mobile technologies.

Russell A. Jackson
Freelance Writer

"Stuck between a rock and a hard place" characterizes a business enterprise's place in the morass of mobile computing risks. Mobile computing itself is a rock; just try to pretend that embracing it isn't a business imperative. And mobile computing security? It's certainly a hard place. There's no such thing as a technology that doesn't pose any security threats at all. It's often the internal auditor's job to assess the level of what is one of few certainties in modern business — the lack of dependable security that comes with mobile computing — and, in some instances, offer suggestions for ways to integrate mobile computing into the enterprise's ongoing operations. C-suite personnel are the individuals who are actually stuck in the middle, but it's the auditor's job to give them the tools to get unstuck — or at least to find a little wiggle room in that uncomfortably tight spot.

MOBILE CONVENIENCE

The specific devices auditors can expect to encounter include Blackberries and other smart phones, iPads and other tablets, laptops, and any number and type of personal digital assistants. Companies generally accept some level of risk because those devices have become so common — and so important to so many people — and because they enable activities that can make business enterprises more efficient. "As much as anything, mobile computing is about convenience," notes Brian Thomas, a Houston-based partner in the Advisory Services Department at certified public accounting firm Weaver LLP. "So companies have a hard time with the user community when they try to implement really strict policies about how the devices are used." Indeed, he notes, there's little reason to get an Android-powered smart phone or iPhone if you can't download any of the apps that have been developed for it. Salespeople often find that mapping apps are invaluable when they're on the road, along with other apps that allow employees to photograph receipts and automatically

generate an expense report. And laptops and iPads are often used to facilitate employees' telecommuting or taking work home for the weekend.

The steps to assess the risks those devices pose and then to assess whether those risks are being addressed adequately by a company's controls are largely the same as those used in audits all the time. Indeed, a mobile computing risk audit may be something auditors are familiar with — in concept, at least — through ongoing efforts in the broader space of IT audits. The difference is that mobile audits encompass, for example, different rosters of interview subjects — including the people who developed any customized applications the enterprise uses — and there probably will be some issues of executive authority that may not have been encountered in other types of audits (see "Mobile Computing Complications" below).

Mobile Computing Complications

As if internal audit's task of assessing mobile computing risks and the controls put in place to mitigate them wasn't difficult enough, many C-suite executives make the mobile computing security situation worse by effectively exempting themselves from company policy. "Too often, executives set their own policy," says Brian Thomas at Weaver LLP. "They find out that they can't do something they want to do, and they're high enough in the organization that they can get an exception to the rule."

Ironically, the employees most likely to be locked down by a restrictive security policy are those least likely to have control of information that anyone else would want. "But the chief financial officer or chief technology officer might have important information — and that's who probably has more permissive settings on mobile computing devices," he says. "As an internal auditor, I'd want to understand what the policy is and whether there are exceptions. And if there are, I need to know about them." Because of its independence, he adds, "internal audit is in a better position politically to say, 'Look, Mr. Senior Executive, I know you want to do all these things, but it's your data people would really like to have. We need to find a way to let you do what you want to do without creating more risk for the organization.'"

Compounding that problem is the fact that "decision makers often don't understand the risks mobile computing poses on a day-to-day basis," says Cesar Martinez, a former municipal internal audit executive. "In many cases, they only understand if something serious happens internally — or at least locally, if they read about it in the media."

The same complication can be found in assessing controls. "There's often a perception that 'management wants us to do this, but it won't put controls in place companywide or give the IT department the authority to do so,'" Martinez adds. Part of the problem, he says, is the executives who can't get enough of the new technology. Most mobile computing technology innovations are more or less "fad" situations, and when a new product rolls out, executives may see somebody with one — a brand-new iPad, for example — and they want to have one, too. But those executives may not take into consideration the impact on the organization. "Managers may not match up their enthusiasm with the eventual need to audit the risk impact the device can have," Martinez points out. "Internal auditors need to be aware of that so they can better navigate the uncertainty that results."

THE FULL PICTURE

"Risk is still risk," notes Philip Chukwuma, chief technology officer at consultants Securely Yours LLC, in Bloomfield Hills, Mich. "You don't need to change anything just because you're auditing smart devices. The devices may be new and sexy, but that just means you need to expand the

scope of an audit." The first step, he says, is finding out who's using what kind of devices and how they're networked to the company's internal IT infrastructure. Everybody uses smart phones and laptops, so the question is not whether mobile devices impact the organization, but how. "A lot of people connect personal devices to corporate email and the data it can contain," he explains. "But that may not be something that's reported up to general management." When auditing remote access, then, internal auditors shouldn't stop at an employee working at home on a virtual private network connecting through a desktop to the corporate network; they should expand instead to an employee connecting to the corporate network from a hotel room with a laptop, tablet, or phone — on a nonsecured network. The pieces of information auditors need to put together the puzzle are likely available; and their job is finding them and making sure they construct a complete picture.

To do that, auditors may need to expand their information quest to additional departments. Procurement, for example, may have employees who have been issued a company laptop or other mobile device. And some sophisticated enterprises may have an asset management solution that keeps records on the type of device each employee has and the specific terms each of them operates under as far as accessing company information and networks. Is it internal only? Or can some employees access proprietary business data from external locations or devices? And if external access is allowed, what type of exposure does it represent? Are internal data tagged and classified, so that some can be copied and taken off site and others can't? The same caution exists in the opposite direction, Chukwuma adds. If some employees have access that breaches the technological borders of the enterprise, what kind of risks are they possibly introducing to internal systems? There's a lot of malware that's designed to destroy business records and alter access to important information. "Every week there's another report that some organization's network has been breached and that data were possibly stolen. It's imperative that the scope of audits extend to smart devices," he notes.

Auditors should expect efforts to get their arms around the organization's exposure to be arduous. "Most places — and it doesn't matter if you're public or private — do a poor job of inventory control because most of the items are 'expensed,'" says Cesar Martinez, a former municipal internal audit executive. "That means the enterprise doesn't have to account for them. If they were capitalized, the enterprise would have control over them."

He notes that many municipal department heads are required to conduct at least semi-annual inventory updates, and that devices issued and approved by some city governments are tagged with scannable IDs. Setting up and carrying out such activities is not internal audit's job, emphasizes Jacques Lourens, chief IT auditor at Nedbank Ltd. in Sandown, South Africa. "An independent internal audit department shouldn't have a consulting role, but one that facilitates oversight of IT

security policies and procedures," he says. "Internal audit should provide valuable guidance in determining whether emerging risks and technology are adequately covered by policies and procedures," adds Thagrai Moodley, the firm's audit manager for information security. "Equally as important is the collaborative effort that should exist between business units in ensuring that technology and security initiatives resonate through the business."

GETTING CONTROL

Once internal audit has established how many mobile computing devices are out there, what types of devices they are, and who's using them and how, it needs to determine the technological risks they pose by vetting security internally. Although it's not audit's job to set policy for mobile computing security checks, it's critical that someone does that, Martinez stresses. Relying on device makers' assurances can do little more than impart a false sense of security. "Department heads have to be aware of the security issues involved," he says, "and they have to support it with a solid company property policy."

"There's a very good, growing body of knowledge online," Thomas says. "A Google search can uncover tons of information, and more and more industry conferences address mobile computing risks." Internal auditors will want to assemble that information and then sit down with internal security people, who have approved the use of the devices, to ask what risks they evaluated. The list of risk issues likely assembled will involve, for the most part, lost and stolen data — and the cascade of business nightmares that can result.

What happens to a major product launch if the specs for it are on an engineer's laptop when that laptop is dropped while the engineer is dashing through an airport — and shatters irreparably? "Say a company is going through an acquisition," he explains, "and details get out via a lost laptop." That kind of disaster can happen, he notes, when the CEO has just gotten, say, a new iPad that he has to brag about to his colleagues. "He's got sensitive documents on it, and he's showing it off — and all of a sudden he loses it," Chukwuma comments. "Now you're looking at all the information about the merger or acquisition being in somebody else's hands. The data on the device are now public."

WHO IS RESPONSIBLE?

Once auditors have assessed the risks their enterprise faces and advised management on ways to mitigate them, the next step is auditing the resulting controls to make sure they're doing what they're supposed to do. "You want the auditor to perform a walk-through first, before the audit, to make sure

it has adequate scope and coverage. The auditor, at a minimum, has to make sure these issues are covered: identification, authentication, passwords, encryption, access to information, device anti-virus and firewall features, logging and log review, extension of disaster recovery, and incident management and backup," said Chukwuma.

The specific controls around those issues may be different from those examined in other types of audits, and there may be more of them to review, but they are assessed the same way. "There could be 600 controls for a Blackberry alone," Chukwuma points out. "You've got to go through item by item to determine which are applicable to the organization." And auditors have to figure out who controls the control in question — specifically, whether mobile computing is considered an enterprisewide operation or a function of your organization's IT shop. "Is it a strategic initiative that management wants to put in place?" he asks rhetorically. "Does management want to get away from laptops and migrate to iPads, for example, to free up people to do more off site work?" Is it thus enterprisewide, or is it something that IT has put in place because it's an IT issue? If it's in the hands of IT, then IT security policies kick in. If not, it's a corporate governance issue. Knowing which it is helps to determine who controls it.

Once auditors determine who controls mobile computing and what specific operational controls are in place, a controls assessment should proceed pretty much as it always does. One specific tactic Thomas suggests is gaining access to some people's phones, iPads, or Blackberries, especially from different types of user groups — the C-suite versus sales versus financial operations — for a physical inspection. "Employees will be reluctant," Thomas concedes. "So try something just shy of a surprise, something like, 'Next week we're auditing phones. We want to see if they're being used the way they're supposed to be.' Then schedule a time for people to bring the phones by."

Lourens, too, suggests a real-world-effectiveness standard for mobile computing controls. "The effectiveness of the controls should involve a test of the correlation of security configuration to defined, approved, and communicated IT security policies and procedures," he says. "They should be bespoke, defined in a manner that the business deems appropriate to secure its environment, and taking industry good practice into consideration."

Auditors may never be able to assess mobile computing device controls completely, because, as Martinez points out, it's too nebulous — the technology can change so rapidly. "Can you have a preventive or detective control that's comparable to a traditional control?" Martinez asks. "You can determine that there's some inherent risk, but you can't gauge the level of it because the dynamics

are so fluid." In fact, he stresses, it may be that the only usable control is simply putting a name on each product. "If I'm issued a Blackberry, I'm responsible for it," he suggests. "The main control then is 'I have to be accountable for its use.' That's really the only control you can put in place with any confidence" — if, that is, the company actually has confidence in its employees' ability to use mobile computing devices responsibly.

What About Personal Devices?

One of the trickiest issues around mobile computing risk is the blurry line between "business" and "pleasure." For many companies, smart devices are still personal assets, notes Philip Chukwuma, chief technology officer at consultants Securely Yours LLC, in Bloomfield Hills, Mich. "There is a financial decision to be made here because providing smart devices to all your employees can become very expensive very quickly." Many companies find it's cheaper to allow employees to use their personal smart devices, but to provide safeguards and access control. The job of internal auditors is making sure there are safeguards to protect the organization while allowing employees to use their personal devices.

"The organization may allow email, but not data,"Chukwuma says. Or it may provide access to email and data through a company-provided virtual private network tunnel, or it may disallow the transfer or viewing of some data on a smart device based on data classification. "For each company, there will be a variation to support the business," he says, "but internal auditors are responsible for making sure that the way the organization uses personal smart devices is fully defined and documented."

The IIA's Global Technology Audit Guide 15: IT Security Governance can provide valuable assistance, notes Cesar Martinez, a former municipal internal audit executive. So can a conversation with the enterprise's IT staff. "IT should analyze the different types of technologies out there and determine which the company feels comfortable allowing to connect to internal systems and carry company information, says Brian Thomas, a Houston-based partner in the advisory services department at certified public accounting firm Weaver LLP, in Fort Worth, Texas. "Therefore, internal auditors should seek to understand from IT whether it allows noncompany-issued devices to attach to the network and how it deals with the various threats associated with certain platforms."

In the view of Thagrai Moodley, audit manager for information security at Nedbank Ltd. in Sandown, South Africa, "the storage of company data on personal mobile devices should not be permitted; however, that may not be feasible within most organizations." In any case, Moodley adds, "we need to ensure that controls are defined and implemented to facilitate sound governance and security practices." Only technology adopted by the company in question should be permitted on the network, for example, and drives should be disabled on laptops and desktops, with a mechanism to enable for approved mobile devices. A means of encryption should be implemented to ensure all devices with confidential information are protected from unauthorized access and malicious intent. And if that's not the way staffers are used to doing things, internal auditors need to step back and let management do its job. "This is a cultural thing," says Thomas. "IT and the organization overall must condition employees to realize that if they want to connect personal devices to the network, certain conditions apply."

To comment on this article, email the author at russell.jackson@theiia.org.