Business & Careers

Securing the gateway to confidential information

Luigi Benetton
Hi-Tech

Phones, tablets and notebook computers help lawyers be more productive, since they connect to the law firm network when the lawyer is out of the office. They also represent an information security risk because they connect to the law firm network while the device is out of the office. Compromise the device, compromise the network it connects to and compromise the data on that network.

That's why law firms need policies that govern mobile device usage and must find ways to help staff comply with those policies.

Drafting a mobile device policy is a complex practice. Dominic Jaar hasn't seen a policy yet that covers all the bases.

"You need the right people around the table," says Jaar, partner and national leader in information management and e-discovery for KPMG. "Most of the policies we see are either totally legal-oriented or a pure IT approach."

Mobile device policy can cover a wide range of topics, including:

- Required authentication (e.g. password usage) and other security controls;
- Ability to install software;
- Ability to download files to devices;
- Device encryption;
- Taking devices to other countries;
- Proper usage of mobile devices as Wi-Fi hotspots;
- Proper usage of location-based services;
- Reimbursement of fees paid for usage of personal devices for business.

Using his background in computer engineering and influenced by his work with technology clients, James Kosa wrote his firm's mobile device policy.

"A big part of my job is security, so I err on the side of security," says Kosa, who practises information technology and intellectual property law. Perfect security via policy "might not be worthwhile," says the Deeth Williams Wall partner whose 25-lawyer firm handles requests case by case.

"It isn't yes or no, it's a question of whether we can secure the device," he says, adding that overly controlled devices might lead to people "boycotting" them and using other, unauthorized (and potentially unsecure) devices to access the network. (Everybody in his firm opts for a BlackBerry on the job, though many carry other devices for personal use.)

Chuck Rothman has helped draft mobile device policies for clients and for his own company. To his eyes, the policies are mostly similar. Differences occur in details like what types of devices are authorized (e.g. BlackBerry, iPhone, Android, Windows) and whether staff can use the camera.

"A manufacturing company demanded the camera be disabled on phones to prevent industrial espionage," recalls Rothman, director of e-discovery services for e-discovery and information governance law firm Wortzmans.

Third-party applications could also pose problems. Ensuring staff only obtain apps from "authorized" app stores might mitigate potential risks. "That's the theory, anyway," Rothman quips.

Many policies are geared to phones, tablets, and sometimes notebooks. They rarely account for newer technologies like "wearables" (e.g. Google Glass and various "smartwatches" à la Galaxy Gear, Pebble and Apple Watch) that may contain data independently of other devices. And thanks to the blistering pace of technology innovation, it's a safe bet devices few people know about may soon burst into law offices.

For these and other reasons, Rothman advises firms review their policies annually to ensure they're up to date.

Ready for more policy wrinkles? Consider the bring-your-own-device (BYOD) trend where companies allow staff to access their networks and data using personal devices. The benefits can outweigh the costs for "non-risk" businesses, including cost savings to the company and allowing staff to use their preferred tools for work.

Jaar believes that any organization in a "risk" business should provide all work devices. Unsurprisingly, he considers the practice of law a "risk" business and advocates firms acquire full control over the devices employees use on the job.

"Even pushing e-mail through a personal device means you have a personal device that contains confidential information," he says.

Carefully chosen technologies can help firms make compliance easier for lawyers. For instance, the firm should be able to connect devices to a mobile device management (MDM) platform. From an MDM, IT staff can do things like remotely track missing devices, wipe a device's memory, push operating system or application updates to devices, and keep people from violating mobile device policy.

"You need the same capabilities on mobile devices that you have always had on PCs," Jaar says.

He also prefers devices that enable separate work and personal spaces. This entails the separation of business from personal e-mail, browsing, documents and other data.

"If an employee leaves, you can wipe corporate data from the employee's personal device without touching personal information," Rothman adds. "BlackBerry has already implemented this in the operating system and I think Apple and Android will do the same thing." Should a device be lost, the employee can ask IT to wipe the entire device.

All data traffic to and from a law firm's servers passes through the same gateway, so security there can be strengthened.

"We monitor traffic through the firewall and only allow authorized traffic in," Kosa says, noting that the firm has "whitelisted" (i.e. authorized) applications like GoToMeeting and certain desktop sharing tools.

Tools like MDMs and firewalls don't supplant the need for employee training. Staff rarely understand mobile device policies since they frequently aren't taught why they matter or how to follow them. "Even if you have the perfect policy, if it only sits on the Intranet, you may as well have no policy," Jaar says.

Since third-party apps are easy to install and can cause issues, Jaar suggests teaching staff how to search app terms and conditions for keywords like download, upload, confidential, personal, privacy, private, mining, analytics, sell and transfer.

Reading text in areas where these keywords appear can help lawyers avoid giving developers the right to do things like upload all contacts on a phone to developer servers or look at a device's contents.

Task: Challenge is to stay focused

Continued from page 20

ing to other human beings in other continents.

"It's not just hippie stuff about, 'Oh, let's all hold hands and have a global village," said Griffin. "It's just another way of saying the world is one family."

By embracing the spirit of Vasudhaiva Kutumbakam, lawyers will be more compassionate and never lose sight of the consequences of their actions.

Human rights lawyers, in particular, might benefit from adopting the concept, she said, because they're often involved in strategic litigation and trying to challenge or establish new laws.

Sometimes they get so wrapped up in the litigation process that they lose sight of who they're representing, said Griffin.

"I've seen that so many times in my work. Lawyers have to remember that they should be serving human beings, not setting legal precedents."

While it's not intentional, they focus too much on righting a legal wrong and lose track of the people who have been harmed, said Griffin.

"What can happen is that we don't act in the best interests of those that we're trying to serve."