In previous columns, we described innovative practices that Advanced Practices Council (APC) members shared with their colleagues at recent meetings. In this column, we present sobering security advice shared by Mischel Kwon, Chief IT Security Technologist at the Department of Justice, at the May 2008 APC meeting. She was invited by APC member Skip Bailey, CIO of DOJ’s Bureau of Alcohol, Tobacco, Firearms and Explosives.

Mischel acknowledged that APC members, already knowledgeable about IT security by virtue of their roles as CIO, have long been aware of IT security threats from viruses and hackers. APC members may not be as aware of the explosion of organized groups targeting organizations as well as individual executives. These include other national governments, organized crime, industrial spies and terrorists. “These people are not trying to bring systems down, as in the past,” she explained. “They are trying to get information.”

Unfortunately, many organizations are not as well protected as they think. Seventy percent of a typical security budget is spent on compliance matters, not on protecting and defending the organization. “This is not enough,” she stressed. “The balance must move the other way.” Two of the biggest gaps in protection are email and access to social sites. “While you often hear that insiders are responsible for most security breaches, this is not quite true,” she noted. “What usually happens is that an insider unknowingly clicks on a website or email containing malware and infects the whole organization.”

---

1 This is the fifth in a series of columns from the SIM Advanced Practices Council, an exclusive forum for senior IT executives who value directing and applying pragmatic research, exploring emerging IT issues in depth, and sharing different perspectives with colleagues in other industries.
A key responsibility of the CIO is to ensure a balance between what staff can and can’t do. “You can’t always say ‘no’,” she explained. A portfolio of tools and approaches is required to manage both organizational and personal security.

Mischel focused the rest of her talk on specific security risks to executives, identifying actions APC members could take to improve the security of their personal information:

- **Don’t publish your email address in a useable form.** Much spam originates from hackers who pick up addresses from corporate websites or address books. A number of malware programs can make an email look like it comes from an executive, and people in organizations are much more likely to open an email if it comes from a company executive. She therefore recommended obfuscating one’s email address (e.g., name[dot]last name[at]organization[dot]com).

- **Avoid surfing the net with the same computer used for company or personal business.** Sports and social networking sites are notorious places for harboring keystroke logging malware. Once an individual clicks on one of these sites, a keystroke logger can access whatever is done on a computer, such as passwords. One method of protecting oneself while surfing is to use a “virtual machine” every time one logs on to the internet. While less user friendly than other forms of access, this software essentially cleans and reimages a computer every time it is used. “Cookies” are a good place to store malware, she noted. It’s therefore best to erase them after every internet use.

- **Don't open attachments from people you don’t know.** Phishing and website redirects have become considerably more sophisticated, to the point where it is almost impossible to distinguish between the real and the bad site. Often, hackers will send an email with an attachment that looks like it’s come from inside the company. Once the attachment is clicked, malware is downloaded automatically. “Many people think that previewing an attachment will prevent this,” said Mischel. “This is not the case. Previewing is the same as opening from a security point of view.” This type of malware is often not detectable by a virus checker.

- **Delete personal identification information from your cell phone.** It is extremely easy to hack into a cell phone and obtain an individual’s home phone number, address and family names and photos. She illustrated this with a video that is available on the internet. Many executives also keep company phone directories on their cell phones. Mischel advised putting only first names in your phone directory so that individuals cannot be traced if the phone is hacked or physically lost. Similarly, she recommended not posting one’s home address on the LinkedIn website. “Passwords can be easily broken,” she stated. “Encryption is harder to break, but it’s only as good as one’s password.” In short, cell phones should not be considered private and users should have no expectation of privacy when using them. This expectation should also extend to text messages.
• **Ensure Bluetooth connections are in “non-discoverable” mode.** Most Bluetooth devices (e.g., Blackberries, cell phones, and in-car computers) are pre-set to “discoverable” mode, which enables a hacker to find and easily hack into them with their own cell phones. Once in, they have full access to all information on the device and can also make calls through others’ devices. If you need to be in “discoverable” mode for some activities, for example to connect, Mischel recommended changing the mode only for the few seconds needed to do this and not naming the device with your full name. “Naming your device with your full name makes it much easier to connect your information with you,” she explained.

• **Don’t assume hotel internet connections are safe.** Even if there is a wall connector in a hotel room, chances are that hotel internet connections are made wirelessly between floors. Thus, a hotel is really a huge, unprotected wireless cloud with wide open connections. “You should treat everything you do online in a hotel as not private,” she warned and also strongly recommended *not* doing online banking while away. Ideally, business travelers should use a separate laptop from the one they normally use. Even encrypted networks, while safer, are not immune from attack.

• **Use a separate machine for personal business.** Doing online banking, online shopping and filing taxes online must be a risk-based decision and should be done with caution. Mischel herself avoids these activities because of her personal experiences and knowledge. However, if an individual does decide to undertake these activities, he should use a different machine for personal business from the one used for surfing the net. Furthermore, if a home router is used for wireless access, it should be less than two years old because earlier models have poor firewall protection. She also recommended turning the “file sharing” features of a computer off. Finally, most new computers come with an infrared data access (IrDA) feature turned *on*, which effectively opens up any computer to the world. Mischel recommended covering up this access point with a small sticker.

• **Be careful with all moveable computing devices and storage.** Never leave a laptop in a car or “asleep.” Even if it is encrypted and password protected, it is relatively easy for a hacker to pick up passwords and files. Similarly, memory sticks can be used to quickly download key information simply by putting them in a USB port for a few seconds. “Never put an unknown USB device in your machine,” she recommended.

• **Use shields for all RFID-enabled cards.** Many organizations, such as Amex, the Passport Office, and hotels, are adding RFID chips to their cards and other documents to improve identification and authentication. However, these chips are very hackable from a wide range. Mischel illustrated this problem with a video showing how a dummy with an RFID-enabled passport could be targeted by terrorists and the chip used to trigger an explosive device. The best way to protect against this is to always use the shield provided or to disable the chip.
• Get a separate computer for your children. Children tend to be big users of the most commonly infected websites, such as Facebook, YouTube, and university sites. No executive should ever allow his children to use his personal or business computer for these activities.

• Create an algorithm for your passwords. While it’s inconvenient to change passwords routinely, this is the safest practice. Mischel therefore recommended that each person create an eight character password creation algorithm that can be easily remembered and used.