INVESTMENT COMPANY INSTITUTE®
ICI Global
WASHINGTON, DC • BRUSSELS • LONDON • WWW.ICI.ORG

ICI VIEWPOINTS

FEBRUARY 17, 2017

Cybersecurity at Work: Keeping Secure When Away from the Office

By Peter Salmon

Part of a series of ICI Viewpoints *covering cybersecurity issues.*

In the previous installment of this series, we discussed the risks associated with information sharing. One aspect we did not touch on is the inadvertent sharing of information, or data, when traveling for business or pleasure. For example, anyone who has flown lately can clearly observe that planes are full with business travelers, often made obvious by their black ballistic-nylon laptop bags.

A 2008 Ponemon Institute survey revealed that up to 12,000 laptops are lost at airports each week, with roughlytwo-thirds of these devices going unclaimed. Though you would think that people might try to reunite with their missing laptop, some companies will now remotely disable lost laptops, making recovery less important. And these road warriors carry more devices than just a laptop computer—business and personal travelers also bring along phones, USB sticks, tablets, and other devices that may be even easier to overlook or lose.

Stay Vigilant, and Travel Light

So, when it comes to cybersecurity, step one when you travel is to keep track of your electronic devices. This raises a couple of interesting questions. First, what devices do you really need to take? And second, what data are on those devices?

Let's address the second question first. If you were planning a trip abroad, you almost certainly would take a suitcase—but would you put your entire wardrobe in that bag? Certainly not. So why would you carry a device or devices that contain *all* of your business and personal data? The answer is, you shouldn't.

There is a way to reduce this risk. For business travel, if available, carry a "clean" device(s)—one that your employer provides specifically for the purpose of working while traveling. When traveling for pleasure, consider removing data that you don't need with you. The benefit of these tactics should be obvious: if your device is lost or stolen, the impact is minimized. Limiting the number of devices you carry—tablets, phones, laptops—also reduces the risk of loss.

Let's assume you are on a business trip, you have your clean device(s), and you have taken the additional steps of making certain your antivirus software and applications are up to date. Being a security-conscious traveler, you also lock your devices with a strong password or passphrase, use software that enables you to remotely track your device (and wipe it clean) if it is lost or stolen, turn off Bluetooth, and have backed up your device(s). Now we can just connect to Wi-Fi and get to work, right? Not so fast. If accessing the Internet while traveling means using free public Wi-Fi at your hotel, an airport, or coffee shop, you should be leery, because you don't know who else is connected to them. It's basically a case of, "you get what you pay for"—the security you get from free public Wi-Fi is directly proportional to what you (didn't) pay to access it.

Control Your Device and Connection

Fortunately, there are some steps you can take to minimize the risk of connecting to the Internet while traveling. Firms typically provide employees traveling on business with a way to use a virtual private network, or VPN. The benefit of enabling a VPN is that all of your online activity will be encrypted. If traveling for pleasure, you can purchase VPN services from providers such as Tunnel Bear or Private Internet Access VPN. If possible, you should avoid using public computers, such as the ones in hotel lobbies or Internet cafes. Quite simply, you do not know who was on the computer before you and whether they have infected the device. This is all about control and trust of the device and the connection, to remain as safe as possible.

If you are starting to notice how physical security and information security are linked, it is because they complement each other. This brings me to the ubiquitous hotel room safe—a misnomer if ever there was one! Most hotel room safes use an electronic number pad that require you to enter a “secret” four-digit code to lock and open the safe. Common sense would tell you that there must be more than one way to gain access to the contents of these safes—for example, if there is a malfunction with the safe’s electronics. Next time you check in to a hotel room that has a safe, look to see if it has a metal nameplate on the front, with the safe’s logo. These are usually screwed on and can be removed to reveal a keyhole that can be easily manipulated to unlock the safe. Importantly, the safe can be relocked the same way and the nameplate replaced without you ever suspecting an unauthorized entry.

You can, however, enjoy the mint on your pillow—I think. But if you need to store something valuable—information or devices—take them to the front desk to be locked in their safe. There are no guarantees there either, but the chances are better that security is tighter!

The next post in this series will examine what to do if you’ve been hacked.

Additional Resources:

Information Security Resource Center

Other Posts in This Series:

- Cybersecurity at Work: Creating Passwords That Are More Secure
- Cybersecurity at Work: Incident Response Plans and What They Entail
- Cybersecurity at Work: Exercise Is Important
- Cybersecurity at Work: The Benefits of Information Sharing Networks
- Cybersecurity at Work: The Risks of Information Sharing
- Cybersecurity at Work: Keeping Secure When Away from the Office
- Cybersecurity at Work: I Know What You Know!
- Cybersecurity at Work: To Confront Evolving Threats, Flexibility Is Key

Peter Salmon is ICI's senior director of operations and technology.
