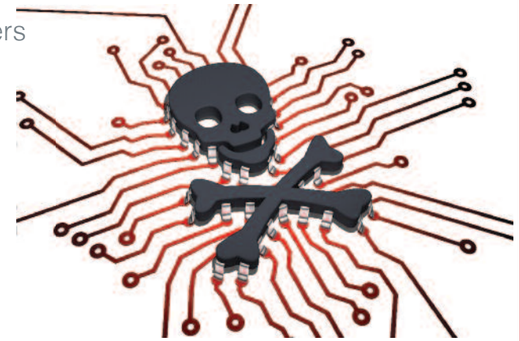
Virtual RISK

Cyber threats are not just in the movies – they are real and they are out there with your travelers

By Fatima Durrani Khan



Sometimes it's hard to pick what constitutes the bigger threat to organizations that send business travelers around the globe: Is it their physical security – protecting employees from harm while they're on a trip? Or is it their digital footprint – the proprietary information they carry on their mobile device or laptop? The answer of course is both.

While it may seem obvious, many companies are still trying to understand how and to what extent cyber security plays an essential role in protecting both travelers and organizations.

From overt attempts to hack confidential information to something as simple as a misplaced device, risk managers are quickly learning that any weakness in an organization's cyber security protocols can create a huge mess. The weak link could be a business traveler who leaves his laptop unsecured in a hotel lobby or who discloses sensitive information over his phone during a taxi ride.

In other words, not educating your traveler on the risks associated with navigating the cyber world leaves your organization at risk of having proprietary information stolen or leaked.

What's the Bottom Line?

Data security, in addition to physical security, is an essential component of a holistic travel risk management (TRM) program. Unfortunately, data security is laden with complex risks, and once compromised, can destabilize businesses and affect assets and productivity.

"Because no organization wants their data security breached, there should be policies and procedures in place that help business travelers understand what their role is in maintaining the integrity of their data," explains Tim Daniel, group executive vice president at International SOS, who has been involved in the company's business of Information and Tracking Services, including the digital enablement of related company product lines.

For example, travelers should be aware that threats to data security can increase or decrease based on the their destination. For example, many countries conduct "surveillance" with benign intentions: they simply don't want inappropriate information and/or viruses to enter their countries.

However, in higher risk destinations, intellectual property can be targeted for more sinister reasons. According to the US Overseas Security Advisory Council (OSAC), "Business travelers should be particularly mindful that trade secrets, negotiating positions and other business-sensitive information may be taken and shared with local interests."

"The threat isn't always criminal. In many cases it's as simple as a traveler misplacing a laptop, phone or tablet while on a trip," Daniel clarifies. "That still creates the uncertainty of where the device ended up, as well as a headache for not only the traveler, but the organization. International SOS also routinely hears about travelers whose devices are searched at border checkpoints. Compromising information and content considered illegal can lead to the confiscation of the device and even jail in extreme cases."

Keeping Travel Cyber Safe

According to International SOS, in order to protect a traveler's physical risks:

- Keep laptop, tablet and phone on your person at all times
- If carrying memory sticks make sure they are clean encrypted and on your person at all times (but the preference is not to use them at all)
- Carry a cable lock with you and use it whenever you are likely to step away from your computer (including in your hotel room)
- Use a screen protector and do not work on sensitive documents in public areas
- Ensure devices are password protected, that laptops have whole disk encryption and that lock settings on phones and tablets are immediate or have a short duration

In order to minimize a traveler's cyber risks:

- Establish a VPN when using any publicly accessible WiFi
- Ensure your anti-virus protection is up to date
- Use Web Content Filtering if that is available in the organization
- Use strong passwords and ensure that these are not recorded in any paper or media you are carrying
- Do not visit sites that host illegal or potentially compromising materials (pornography, political issues, hate speech, violence)
- Do not bank or shop online from a public hotspot
- Exercise caution in any correspondence you send via e-mail/chat
- Turn off wireless when you are not using it
- Set wireless to connect manually
- Turn off any file sharing
- Do not carry any sensitive data with you – remove it from your devices and store on your personal network drive or encrypted back-up. Files containing PHI, PII, and CSI should not go with you on your travels
- Ensure that you are not carrying any content that has been illegally downloaded

The Cyber Shift

It's important for risk managers to conduct cyber security research in areas of the world where organizations are doing business, looking at the "who, what and where" when it comes to data security.

Who: Is the traveler someone who is perceived to have valuable information? While on the surface, a senior manager may appear the most likely target, a mid-level engineer or scientist who carries highly proprietary and technical information on their laptop may be a greater risk.

Where: Does the destination country have a history of cyber theft? Or even a track record of petty theft like pickpocketing, purse snatching and other crimes?

What: Does the purpose of the trip hinge on topics that involve a lot of sensitive corporate information?

Because stolen data can create such a negative impact on an organization's business continuity, some companies are instructing employees not to bring a laptop or business phone unless these devices are absolutely necessary.

However, if an organization makes a strategic decision that a laptop or phone is mission critical to meet the objectives of the trip, then a layered approach to data security is necessary. For example, ensuring strong password management is applied to mobile phones is one layer; placing a tracking tool on the device is yet another.

This tool keeps track of everything from validating that employees have checked out a "clean" device from their IT department to making sure it's not infected with viruses upon its return. Simultaneously it acts as a compliance tool and helps automates the traveler's data security processes.

Duty of Care in the Cyber World

"We support companies in order to help them meet their Duty of Care," continues Daniel. "However, the traveler is an important focal point in that they must be taught how to act appropriately with regards to data security. They must understand they have a Duty of Loyalty to act responsibly. For example, there may be a high profile executive who maintains a high level of secure travel – from private transportation to and from the airport to nondisclosure of his itinerary. Nonetheless, it's possible that this same executive can land in a foreign destination, and immediately upload a selfie to his Facebook account, thereby giving away his location."

Organizations must provide a pre-established policy which clearly explains the employee's parameters of privacy and accountability while on business travel.

> Travelers should be aware that threats to data security can increase or decrease based on the their destination.

This includes educating travelers about what constitutes "responsible behavior" and understanding that their online "persona" must be left at home during business travel.

"It's all about managing expectations," says Daniel. "While we would be hard pressed to find a multinational company that doesn't have policies and procedures in place regarding data security, it's a process that's continuously evolving. International SOS helps clients throughout the education and compliance process."

As part of this process, Daniel points to International SOS' own in-house procedures. "We ourselves have strong data security policies, such as requiring full encryption on our own devices and laptops even while they are in transit, in addition to 'check-in' compliance tools during international travel."

The concerns about data security are going to be around for a long time to come, Daniel says. "In fact, as the intersection of the digital world and business travel becomes sharper, cyber security will become an even bigger consideration." BTE