THE BUSINESS OF WEALTH

FAMILY OFFICE MAGAZINE

AUTUMN 2018 ISSUE

ART & MUSEUM MAGAZINE INCLUDED

FAMILY OFFICE INSIGHTS

ARTHUR A. BAVELAS

FAMILY OFFICES - UHNWI - WEALTH MANAGEMENT- PHILANTHROPY- LUXURY - LIFESTYLE

Subscription €99 per year

www.familyofficemag.com

CEO COUNTERESPIONAGE

by Michael O'Rourke

You possess valuable business secrets and unscrupulous people, even nations, want them. Knowing this, your family office takes measures to protect your intellectual property and other critical data on home soil. However, if you're reading this at 30,000 feet, or in your foreign hotel suite where your trade secret-filled laptop is connected to the Wi-Fi, please read on.

Entrepreneurs and executives face a more significant economic espionage threat while travelling than ever before, and the family office is no exception. When a foreign intelligence service is your adversary, the deck is stacked against you. Negotiating a manufacturing deal in China? The Chinese government goes after intellectual property on an industrial scale. Did you enjoy the World Cup in Russia? You might have scored an own goal with your trade secrets in the number two international threat. Nations traditionally considered as friends don't always play nice when it comes to economic espionage. To avoid offending allies, I will refer to two of the worst offenders as France and Israel. Intellectual property is the lifeblood of innovation. Many companies, perhaps yours, will have sixty-five per cent or more of their total value directly tied to their information, technology, or another proprietary competitive advantage. The latest market disrupting product will have tens of millions of pounds or dollars in research and development costs before release. All of this could be lost unless you learn how to protect your trade secrets while travelling.

Before you dismiss the following advice because your family office does not deal in military technology, let us briefly discuss the possible economic espionage targets in your laptop right now. Proprietary formulas and processes, prototypes, technical plans, research, passwords, client and employee data, manufacturing plans, specifications, mergers and acquisitions plans, negotiating strategies, customer data, and investment plans merely begin a long list of business secrets you may carry during your travels. If you run a multi-family office, the potential cost of compromise is further magnified.

Defeating the world's spies requires you to think like one. The number one way to protect your secrets on the road is to leave them at home. Since that makes doing business difficult, here are some ways you can go spy versus spy and come out on top.

Leaving your regular laptop and smartphone behind, travel with clean devices. Preload only the phone numbers and encrypted files needed for that trip. Do not connect any device with sensitive data to the internet. Since many of you will connect in any event, the next two bits of advice will put you head and shoulders above most travelling executives. Establish secure email accounts for you, trusted staff, and advisors that are not connected to your company network. Switzerland-based Proton Mail is a solid option that provides end-to-end encryption. Encrypt your text, voice and video calls with the Signal app by Open Whisper Systems. I've used both in Iraq, Afghanistan and other high threat environments to relay information vital to my security clients securely.

A Virtual Private Network for all internet connections is an absolute must. Airports and hotels host some of the most compromised networks. Install the VPN on your laptop and phone before travelling to the most privacy-phobic countries, then virtually place yourself in a country that allows information to flow unregulated. Think of the VPN as your escape tunnel to freedom through dangerous networks.

Never work on sensitive projects in public spaces like coffee shops, airport terminals, or while in flight. A shoulder surfer could be sitting behind you or zooming an overhead security camera onto your screen. When you ignore this advice, and many of you will, at least make the spy's life more difficult. Placing a privacy filter over your screen severely limits the viewing angle. For less than forty dollars you help protect intellectual property worth millions.

Take your computer whenever you leave your hotel room. More specifically, do not leave the hard drive unattended. Yes, it is inconvenient when you're just heading out to dinner or to the hotel bar. Intelligence services in many countries have ready access to the rooms foreign business travellers occupy. When you step out, they could slip in and surreptitiously harvest your data from the source. Forget about the in-room safe for data security. Most have an easy way to bypass the code you set. Don't believe me? Call the front desk and tell them you forgot the code, then watch what happens.

Once home, have your IT department check everything. They're searching for signs of tampering and malicious activity, whether intrusions or malware. After safely removing needed data, all devices are wiped clean and ready for the next trip.

These techniques sound relatively simple because they are. Even at this basic level, deploying counterespionage procedures makes you more secure by far than most business travellers. Mastering advanced level CEO Counterespionage places you in a different league altogether, requiring a commensurate level of commitment on your part, and intentional vagueness on mine. A detailed discussion in print would only benefit our mutual adversaries.

Specific protocols for composing, sending, and receiving email are required. Specific steps for accessing and working with your sensitive data must be followed. Depending upon your travel destination, even where you sit in your hotel suite while logging into your computer is carefully considered. Details concerning your devices and possible security modifications are better discussed in person.

We have not descended into paranoia. Instead, we frankly acknowledge the multibillion-dollar economic espionage threat against which global executives must conduct business. It is a discussion in which more of us must engage.

Michael O'Rourke is CEO of Advanced Operational Concepts, an international security consultancy. He leads his firm in providing bespoke advice and personalised training to counter economic espionage in the modern threat environment. Michael may be reached at

mike.orourke@adopcon.com
https://adopcon.com.