
# Executive Protection: What can you do about corporate espionage?

- Published on July 7, 2016
- https://www.linkedin.com/pulse/executive-protection-what-can-you-do-corporate-joseph-goforth

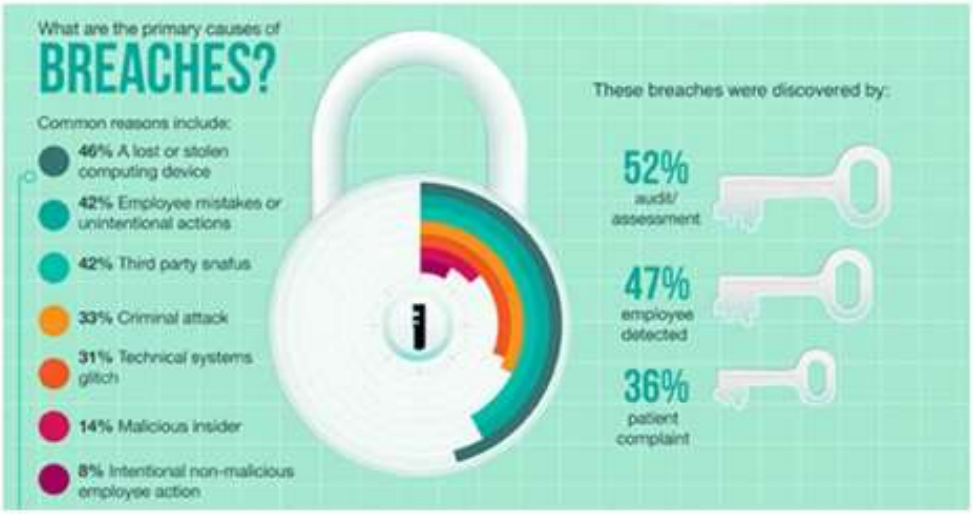
## Joseph Goforth

Security Professional | Corporate Security | Executive Protection | Protective & Criminal Intelligence

You have received the travel itinerary for your protectee.  You know the travel dates, members of the protectee's travel group, you've hired drivers, completed your list of essential equipment that will pass Custom's inspections, arranged for accommodations, and all the other myriad of tasks involved in preparing for the security advance. All aspects of the physical security plan are covered and set to be employed once you arrive. You feel comfortable your experience and training have prepared you for the series of fires that will need to be put out once the security detail is underway. You are lucky enough to have a team with you. You can split duties and rely on extra eyes and ears to keep a sharp look out for unexpected people and situations that will interrupt your security momentum.

There is one thing that continues to fester in the back of your mind however - the one variable you cannot control. Maybe you're there for an investors meetings. Maybe it's a confidential one-on-one executive meeting. Or maybe it's a vacation trip for the protectee and family. No matter what the purpose of the trip, you are not able to control the protectee's use of information or the information highway he may use to announce purpose, location, or material data. There is a security risk, and it is one you can't include in your advance or detail plans. The risk of corporate espionage.

In a recent study 42% of information security breaches were due to employee mistakes or unintentional actions. No C-suite employee is exempt from making mistakes while traveling overseas, whether it is from an overly informative conversation with a stranger to the "bond-style" search of laptops and files while they are away from their rooms.




Source: https://www.prot-on.com/tips-to-prevent-information-leaks-in-your-company

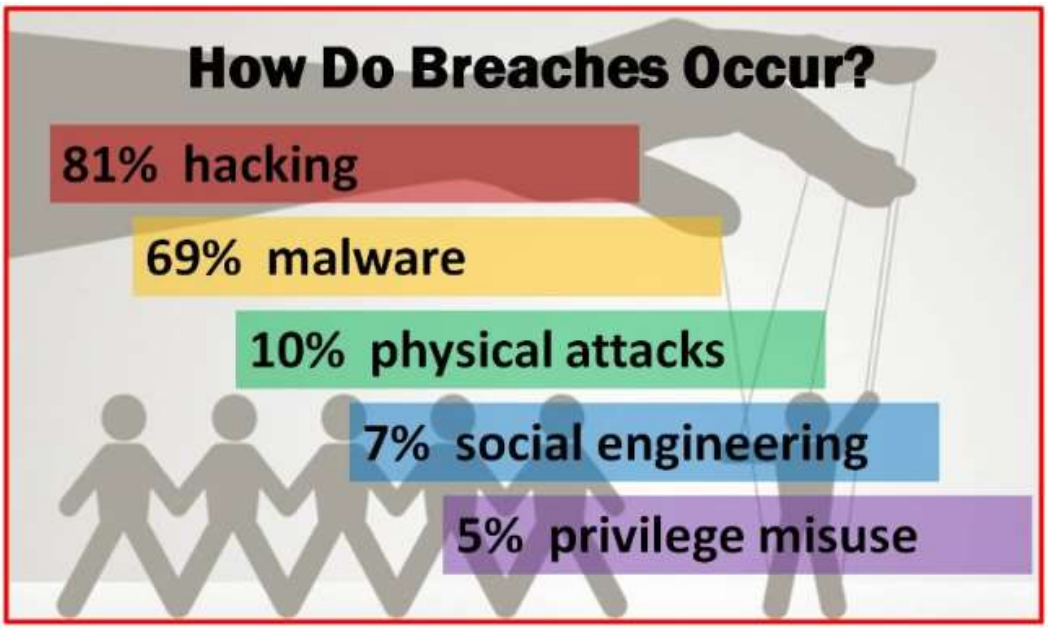
Executive travel, especially abroad, takes on critical risk levels when it comes to information sharing - especially when the "sharing" isn't voluntary. Trying to control this aspect of the security plan is difficult because it delves into the private habits of the protectee. We as Executive Protection professionals assume the risk for not only the protectee's person, but also their professional reputation. The security advance and the security detail must do their very best to protect *all* aspects of the protectee's visit. And this includes corporate or industrial espionage against your protectee.

This task becomes tremendously complex and problematical when the Executive Protection professional cannot monitor what the protectee gives out over a personal phone, internet, email, or even in a crowded airport or hotel lobby. A good company IT team should have technical solutions for this dilemma when it comes to company phones, tablets, or laptops. But breeches happen all the time. In spite of what most countries would have you believe, corporate espionage is alive and doing well. Our new age of information sharing is prime breeding ground for this type of security intrusion, and can possibly do more harm than an old school physical attack or physical intrusion.

A recent study from the U.S. Department of State (Diplomatic Security Research and Information Support Center) announced that Chinese cyber espionage campaigns against U.S. companies have decreased. That's good news right? Reading further, one of the factors which this is attributed to are the success of Chinese hackers in refining their ability to evade detection. Chinese espionage campaigns "are ongoing" as the study points out and emphasizes China is still a motivated cyber threat. China isn't the only culprit however. In 2011, the FBI estimated the U.S. lost between $2 billion and $400 billion or more from economic espionage. The range was so extreme due to the scarcity of data and the various methods that can be used to extract information.

So what is worth stealing? Depending on what sector your executive works in, there can be many advantages for state-sponsored actors and the information they can collect. Intellectual property is often associated with research and development (R&D) data. This may be because it's more often portrayed in movies, and consequently some traveling executives and their security team may conclude that they have nothing worth stealing. In reality, any information which would give a competitive edge in the market place is a target of intellectual property theft. The United States has been reported to have conducted at least 50% of the world's research and development, so this fact alone makes traveling executives prime targets for industrial espionage.


So what should we as Executive Protection professionals be looking for? How do breaches occur and is it worth worrying about from a security detail standpoint? After all, our profession is a small niche' and we can't be responsible for every lapse in operational security, right? According to the 2012 Data Breach Investigations Report by the Verizon RISK team, 7% occur from social tactics and 5% occur from privilege misuse. Both of these methods can be influenced by the savvy and motivated Executive Protection professional. (more on this later)



Methods such as "watering holes" exploit vulnerabilities in websites that would normally be used by company personnel traveling abroad. These websites include news websites, industry-specific portals, partner sites, and even menus of restaurants nearby to commonly used hotels. In other words, websites anyone of us may use while traveling abroad - including executives.

Old school social engineering is also a continuing threat. While the Executive Protection professional cannot cancel meetings or deny access to invited guests, foreign collectors of intellectual information can take the form of personal contacts through arranged meetings, telephone calls, emails or any other form of direct contact where information can be elicited. Conferences and trade shows are productive opportunities for access to executives and competitive information. Tour groups are also lucrative opportunities to engage company personnel and extract information.

Trash runs are also high-return/low - cost methods used by foreign actors to collect information. Trash in the hotel rooms, post-meeting rooms, and dinner meeting sites are all great sources of clandestine harvesting of intellectual property. So with all the standard security precautions we take as Executive Protection professionals, how do we have time to then worry about what the executive does with his or her own equipment or conversations? The simple answer is - *we don't*. Nor would our cautioning or admonishing be a welcome interruption to them as they conduct business "as they see fit."

The solution is **mitigation by education**. C-suite personnel should be briefed *on a regular basis* about the dangers and easy pitfalls associated with falling prey to corporate espionage. The Office of the Director of National Intelligence has outlined several key suggestions to make traveling executives better aware, and thus better understand, the importance of safeguarding the information they possess. Whether that information is written down, stored electronically, or on the tip of their tongues, regular reminders should be conducted through briefings, especially before undertaking international travel, to keep risk levels at a minimum. Below is an infographic representing some of the top suggestions advocated by the National Directorate of Information Intelligence.


Protecting reputations are just as important as protecting the executive's life. While there are limitations to what we can do in either case, as Executive Protection professionals, thinking outside of the box and creating opportunities to complete our mission is where we make our money. I urge anyone in this profession to seek out opportunity *before scheduled travel* to brief protectees on the social aspect of corporate espionage. Remind them they are certainly targets for this type of clandestine activity. Also offer advice on early mitigation techniques to minimize any damage that may be suffered to not only the corporation itself, but the personal reputation of the executive.