CPNI
Centre for the Protection of National Infrastructure

RISK MANAGEMENT ADVICE:

DOING BUSINESS OVERSEAS

May 2012

This guide provides some basic information designed to help organisations understand the risks associated with travelling and operating overseas. As new and existing markets develop in non-western countries, companies are becoming increasingly vulnerable to the threat of economic espionage. The threat is greatest in countries where the State is pervasive, for example in communist and ex-communist states. Such countries might well use their intelligence agencies to further their national economic agenda.

Companies need to be aware that most states will have some surveillance capability, e.g. the ability to intercept phones, emails, eavesdrop on conversations, physical surveillance, tracking devices, etc. Many states also have the legislative framework and the motivation to deploy these surveillance techniques against you.

To inform further guidance in this area, CPNI would welcome information on companies' experiences whilst doing business overseas. If you suspect that you may have been targeted – using methods highlighted in this document or otherwise – please email enquiries@cpni.g.si.gov.uk

Contents

VISA applications 3
Electronic devices 4
Hotels and surroundings 5
Personal behaviour and conduct 6
State secrets and sensitive information 7
Background information 8

VISA Applications

Before travelling to most non-EU countries, you will complete a VISA application form. The details you provide on the application may include your photograph, email addresses, mobile phone numbers, details of family members, specific dates of travel, hotel locations, host organisation etc. If your company is of interest to a foreign intelligence service, they will have access to this information.

What is the threat?

Before you go:

- You may receive malicious (spear phishing) emails to any email address you have supplied. These emails are designed to deliver malicious software (malware) which will enable remote access to your computer.
- Using your VISA form together with open source information from online social media, your colleagues or family may be targeted in a similar way.
- Any information you provide to the authorities prior to travelling will afford an intelligence agency time to plan how, where and when to intercept you.
- If a phishing attack is successful, your work or home computer, tablet or smartphone could be accessible remotely and information stored or transmitted could be vulnerable to interception.

When you arrive:

- If you have provided your mobile phone number, this will make interception of voice and data stored or transmitted from your device relatively straightforward (see *Electronic devices* section).
- You will be easily identified and located on arrival making it easier for you and any of your devices to be intercepted.
- The location of your hotel will be known making it easier for eavesdropping devices to be planted (See *Hotel and surroundings* section).

Electronic devices

Travelling with mobile phones, laptops, tablets etc. enables you to continue working whilst overseas. However, they are perfect vehicles for hackers to access your company's network and information. Whilst the risk is minimal when travelling to western countries, the risks associated with taking electronic devices to countries with a history of espionage against the west are far greater.

What is the threat?

Mobiles and Smartphones

If you provide your mobile phone number on your VISA application, this will make interception of data stored or transmitted from your device relatively straightforward. Whether using a traditional mobile or a smartphone; phone calls, text messages, web browsing and stored information can all be accessed. Your phone can be used as a locational device. If you take the same mobile phone on subsequent journeys to a particular country, it can also be used to alert an intelligence service to your arrival.

If you leave devices unattended or they are taken by the authorities for inspection, data may be downloaded and devices/software installed onto them. As a result they could be used as eavesdropping devices and may be more vulnerable to remote attack whilst in the country and upon return to the UK.

Laptops

Connecting your laptop (or smartphone) to non-trusted networks, such as those provided by a hotel and conference centre, may enable your information and data traffic to be accessed since agreements are likely to be in place with local Internet Service Providers (ISPs)

Software which records your key presses could be installed on keyboards. Using hardware (e.g. a keyboard) which is provided by a hotel or third party may put your passwords or information you type at risk.

In some countries (e.g. Russia and China) encrypted information is prohibited. If you have used encryption (above that provided as standard) the authorities can force you to decrypt it.

If you leave your laptop unattended, data and information (including deleted files) may be accessed and it may be more vulnerable to attack on return to the UK.

Recommendations

Consider taking a 'single-use' mobile phone and a 'clean' laptop, i.e. one that does not hold company information. Whilst this doesn't remove the risk of compromise, it could limit the amount of information that could be accessed.

Assume that your conversations, email traffic and internet activity will be intercepted. Weigh up the risks before discussing or conducting any business of a sensitive nature.

Don't leave your phone or laptop unattended and be aware that conversations in the vicinity of your mobile phone may be compromised, particularly if it has been taken away from you at any point.

Only connect your laptop to your company's network via a secure virtual Private Network (VPN).

Disable functions you don't need such as Bluetooth and WIFI and limit the amount of information stored on your devices.

Use PINs to lock devices and to access voicemail and change these PINs regularly - particularly on return from travelling.

Hotels and surroundings

In most countries it is a legal requirement to provide details of your accommodation upon entry or as part of the VISA application process. Hotels will also notify the authorities as part of the check-in process.

What is the threat?

Your hotel room may be fitted with an eavesdropping device therefore any conversations or meetings you have could be listened to and recorded.

Intelligence services will be able to access your room and safe therefore any papers may be read and copied, and any electronic devices accessed or tampered with.

Using your hotel room's internet connectivity or wifi could make your data vulnerable to interception. If you use the connection to research bars and restaurants in the area, the intelligence services may be able to locate you. If you use the connection to access pornography, they may exploit this for bribery purposes.

Hardware such as keyboards may be provided in your room. If you use these, even with your own laptop, software installed within the keyboard could record your key presses putting passwords and the contents of any emails at risk.

Based on the location of your hotel and host, the intelligence services may seek opportunities to intercept you in local bars or restaurants providing opportunities to exploit anything left unattended or eavesdrop on conversations.

If you are visiting a tradeshow or conference, intelligence agencies may use these opportunities to introduce themselves to you under the cover of a different organisation in order to cultivate a relationship. Whilst you may believe this relationship to be genuine, they may subtly start to use this relationship to extract key information about you and your business.

Recommendations

Avoid sensitive discussions in your hotel room or in public places, e.g. bars and restaurants.

Limit the amount of information you take overseas, both in paper form and stored on electronic devices, noting that deleted files can be recovered.

If you do need to connect to the internet, use a VPN from your work server.

If you have chosen to take a Smartphone, use free Wi-Fi in random coffee shops, taking care not to return to the same one.

Keep important documents and electronic devices with you at all times. Do not leave them unattended in your hotel room or in your room safe.

Be cautious when approached at events such as trade fairs and conferences, particularly if people subsequently try to establish personal relationships. Think carefully about the information you exchange with them and avoid casual meetings in non-work environments.

Personal behaviour and conduct

If you or your company is of interest to a foreign intelligence service, they may choose to exploit or introduce personal vulnerabilities to either overtly or covertly gain access to your company's information.

What is the threat?

Personal information regarding your family, social life and relationships can be used to identify 'hooks' and 'levers' which could be used to manipulate and control your behaviour.

Any personal indiscretion which places you in a compromising situation or leads to an accusation of criminal behaviour may be used for blackmail purposes. Situations can be engineered by the intelligence services to entrap individuals.

Some intelligence services may try to 'plant' items on individuals of interest, e.g. large amounts of money, which can be used to coerce agreement or action.

Any criminal behaviour whilst visiting a country will provide local authorities with a reason to detain individuals and confiscate equipment and papers.

It is not unusual for some intelligence services to introduce a romantic interest to covertly gather information regarding your business.

Accepting gifts and hospitality may provide opportunities to provide you with electronic equipment, such as cameras and USB sticks, which may contain malicious software designed to enable remote access to any connected device.

Recommendations

Limit the amount of personal information which can be accessed via open source media, e.g. Facebook, LinkedIn.

Keep a low profile whilst travelling and be particularly cautious whilst in social situations and whilst being entertained.

Be wary of packages and electronic gifts. Do not plug any electronic gifts into your own devices.

State secrets and sensitive information

Conducting and gathering market research overseas could put you at risk of infringing commercial or state secret laws, particularly in China. It is important to fully understand the laws with which your company needs to comply overseas and to also note that the interpretation of the law can flexible, particularly should a state wish to disrupt your activities.

What is the threat?

Identifying what is a state secret and what is sensitive information is not straight forward and is subject to interpretation by the authorities- if you are found to have infringed the law, this could result in significant fines and a prison sentence.

Business information in a state owned enterprise can be protected by state secret protection laws, particularly when it relates to information regarding a state's strategic industries i.e. defence and high tech. In most cases, state secrets are marked as such however a classification can be added retrospectively.

Gathering information which affects the competitiveness of your company, even from open sources, may result in accusations of storing or possessing state secrets or sensitive information, particularly when it may weaken the position of a particular company or state.

Recommendations

Be aware that the following types of information are often classified as sensitive: maps, survey and geological data; personal information relating to government officials which is not publicly available; detailed corporate information regarding state-owned enterprises.

Be aware that the following types of information may be classified as a state secret: anything to do with or that could be detrimental to state security, social stability or economic development.

Do not keep sensitive information on any portable devices, do not share or disclose such information via email or other online communication or attempt to export from the country without discussion with your legal department.

Do not disclose sensitive information to any third party.

Do not seek to obtain state secrets.

Do not store or possess state secrets in either physical or electronic format.

Background information

Russian intelligence services

The UK remains a priority target for the Russian Intelligence Services.

Russia's intelligence requirements are largely in the following areas: political, military, technology, biotechnology, communications and energy.

There are three main intelligence services which operate against UK interests:

- FSB - the internal security service
- SVR - the external intelligence service
- GRU - the military intelligence service

Chinese intelligence services

Increasing trade with China means that the threat of espionage against the UK is on-going.

Corporate espionage is common and widespread in China.

There are three main intelligence services in China:

- The Ministry of State Security, MSS – a civilian organisation responsible for collecting foreign intelligence and investigating foreigners involved in subversion and espionage.
- The Second Department of the People's Liberation Army (2PLA) - a military organisation responsible for collecting military intelligence.
- The Third Department of the People's Liberation Army (3PLA) - another military organisation 3PLA collects intelligence through remote technical operations.

In addition to these intelligence agencies, the Ministry of Public Security (MPS), the principle Chinese law enforcement authority, plays a major role in monitoring foreign visitors to China, often in support of the intelligence services.