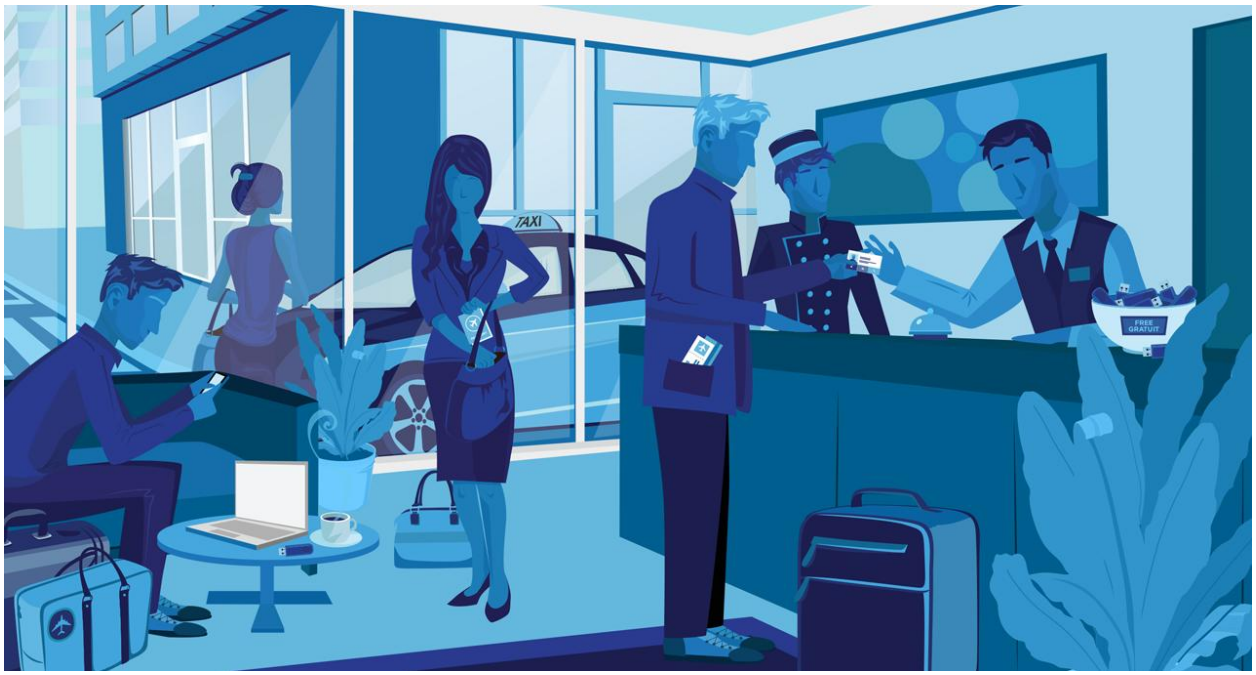
Risk · Pro

Information Security Risks for Business Professionals Traveling to China

Mangesh Sawant

Introduction



The growth of a globe trotting mobile workforce equipped with laptops and other devices is bringing many benefits to organizations. Businesses have become increasingly reliant on timely access to digital information even while travelling. Remote access to business information is generally facilitated through the use of portable electronic devices which can offer the traveler both communications services and access to information, even when this information is stored on internal corporate information technology infrastructure. But travelling with IT equipment also presents considerable risks from loss or theft of equipment/data to problems with security and customs. While most large firms have policies to guard against these risks, they are often ineffectively communicated or enforced. Many smaller companies have little or no protection in place.

All countries present a high risk for carrying IT equipment, especially equipment storing confidential data about the organization. Obviously those with lax security or law enforcement, limited intellectual property laws, a history of criminal activity, unfriendly or antagonistic feelings towards the traveler's country of origin, military hotspots or heightened criminal or terrorist activity present increased risk for data theft. You or your firm may be a target of a foreign country's efforts to obtain information or technologies in order to increase their market share, pass on secrets to indigenous businesses, build their economies or modernize their militaries. Targeting methods include luggage searches, eavesdropping, extensive questioning, and unnecessary inspection and downloading of information from laptop computers.

China's massive market is attractive to Indian businesses as it may become one of India's largest trading partner with an increasing trade deficit. China's brazen use of cyber espionage stands out because the focus is often corporate and a part of a broader government strategy to help develop the country's businesses and economy. Many Chinese companies are state owned enterprises linked to the government and security agencies. MNCs are increasingly concerned about

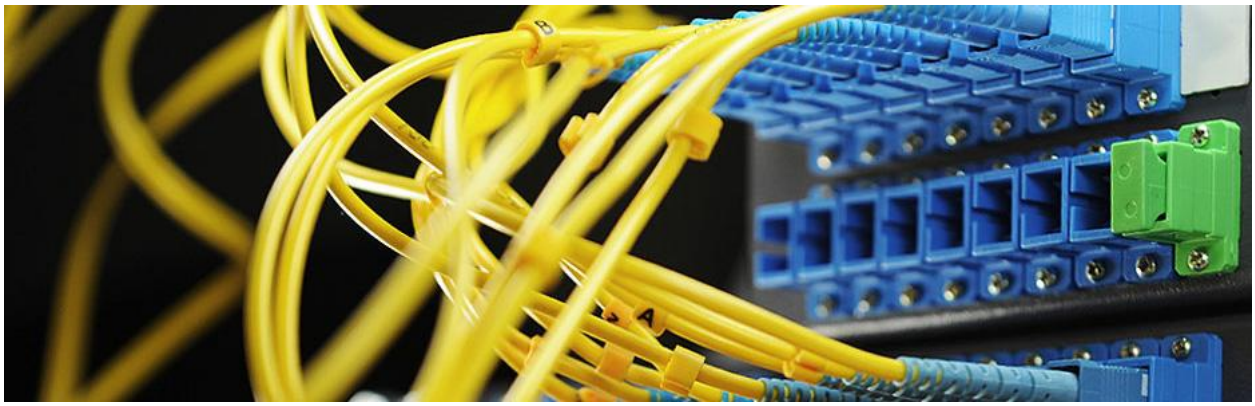
working amid electronic surveillance that is sophisticated and pervasive. Networks in every major hotel are monitored by Chinese security agencies. Foreign governments have uncovered a sophisticated industrial espionage campaign that targets business executives in luxury hotels across China once they sign on to computers using in-room wireless connections they consider private and secure. There were recent instances of travelers' laptops being infected with malicious software while they were using hotel Internet connections. Many high profile US organizations require their employees to take extensive precautions when traveling to China.

Threats to the cyber security, both physical and technical, can increase significantly when travelling. A user is normally taken from a known and relatively secure environment to one that is open, unknown and, in some cases, where threat actors have the power of government behind them. A heightened sense of cyber security awareness is required when travelling to protect personal and corporate assets. Employees should be made aware of the risks that they and the information they take with them may face while travelling as well as understand measures that they can take to reduce this risk. This report provides cyber security information to increase the traveler's awareness of potential risks they face while travelling with electronic devices. In this report Riskpro offers the advice and provides guidance to help ensure the protection of electronic information of importance to Indian businesses. Riskpro also recommends a set of best practices while travelling to China. These best practices are for use by both the business professional and information technology staff.

Threats

- Foreign government officials, journalists and business professionals with access to advanced proprietary information are particularly likely to be under surveillance in China
- Individuals holding senior positions within an organization and/or those who work with valuable information may be at higher risk of being targeted through their mobile devices
- Wireless access services have been monitored by third parties to gain information transmitted through WiFi service.
- Unauthorized full disk copies have been made while the laptop owner was out of the hotel room in China
- Security personnel may at times place foreign visitors under surveillance
- Data security hazards include the loss or theft of equipment, spyware on PCs in hotels and airports, data theft through WiFi and border or customs officials
- Capabilities exist which allow threat actors to:
    - identify and target mobile devices
    - deliver malicious code to the device
    - use device network connections (e.g. wireless, Bluetooth, etc.) for their own purposes
    - leverage the device as a means of infecting other networks
    - access the device as a means to track your location (e.g. GPS)
    - activate the microphone on a device
    - intercept communications that are sent electronically

- Hotel business centers and phone networks are monitored and in some locations, rooms may even be searched. As a general guideline, assume that there is no expectation of privacy in offices, hotels, Internet cafes, or other public areas.
- Mobile devices are a prime target for theft. If stolen, the information contained within may be accessed and/or used for malicious purposes.
- Business professionals traveling in China and Russia should expect continuous surveillance and Internet traffic monitoring. Mobile computing devices are routinely compromised.
- The information contained on your organizations systems relating to high profile events whether classified or unclassified can be of strategic interest to adversaries.
- A keylogger records information typed by the user on the computer such as passwords and credit card numbers. They can be either covert software applications, or physical devices attached to computers.
- Electronic eavesdropping has been reported on airlines, in hotel rooms, taxis and meeting rooms.
- Business and government travelers have reported their hotel rooms and belongings were searched while they were away. Sometimes there was no effort to conceal the search
- Software and hardware was offered to participants while attending conferences and training events. These materials can either be free of charge or part of the paid content for the event. Even when provided during the course of a planned activity, it is possible that these materials may inadvertently or purposely contain malicious software. For example, a recent conference on computer security mistakenly distributed USB sticks that contained viruses that were installed during the manufacturing process



Risk · Pro

Recommendations

Before you travel

- If possible, do not take your work or personal devices with you. Use a temporary device, such as an inexpensive laptop and/or a prepaid throw away cell phone purchased specifically for travel. If you must take your electronic device(s) with you, only include information that you will need for your travel.
- Be sure that any device with an operating system and software is fully patched and all the institutionally recommended security software in installed
- **Loaner devices**
  It is common practice for travelers to have their organization provide devices that are used specifically for travel purposes. These are "clean" devices that allow the user to continue to perform their duties while travelling. These devices are often older or cheaper assets configured to provide basic computing abilities and may or may not include the ability to connect to corporate networks. They are exclusively used for travel purposes. After travel, the information on the device is securely deleted and at times the device itself is destroyed. Organizations with an advanced forensic analysis capability may choose to examine the device for evidence of compromise. No matter the state of the device, awareness of the risk while travelling is important. If the loaner device connects back to the organizational network, or the organization's information is processed on the device, risk of compromise remains. Loaner devices may therefore be restricted from accessing critical or sensitive networks.
- If you can travel without the device, do so. If you must take a device, use one minimally configured for travel
- Beware of emails received prior to the travel especially if they are related to large international events. These emails may have links to malicious compressed archive or executable files, other malicious attachments, or web links. Verify the source to the extent possible
- Install up-to-date anti-virus protection, spyware protection, operating system security patches, and a personal firewall. Set the web browser to the highest security setting possible. Ensure that the user cannot disable these features
- Consider the impact to your organization if the information on the travel device was lost or stolen. Remove unnecessary information from the travel devices and ensure backups of this information are made and left at your local facilities. Consider whether using encryption to protect files is allowed in the visited country.
- Configure devices to run anti virus software on storage devices on access (e.g. USB) upon installation
- Limit and restrict administrative privileges. Have the traveler change passwords prior to travelling. Ensure any passwords meet the organization's security policy requirements for password complexity.
- Ensure that proper network security settings are implemented for all devices. Disable unnecessary connection capabilities such as Bluetooth, Infra-Red, NFC and Wi-Fi.
- Ensure proper security settings are implemented for Virtual Private Network (VPN) access (if applicable).

- Verify that mobile devices are not able to access the Internet at the same time that the user is accessing the organization's internal network.
- Increase logging and monitoring capabilities (when applicable).
- Install a mobile device management (MDM) application to assist with the identification of security compromises. MDMs allow organizations to compare device images before and after travel to identify discrepancies
- Disable all file-sharing, peer-to-peer communications and vulnerable ports
- Consult your IT security staff prior to departure. They can confirm that your device's configuration is correct and that all updates, patches, encryption and antivirus software have been installed. They may also advise on further security measures such as emergency information sanitization procedures if you are travelling to a high risk location.
- Remove all non-essential data from the device, in particular, reconsider the need to take classified information overseas.
- Disable any feature or software that is not required for the trip. The lesser software on the device, the smaller the opportunity to exploit and gain access to the device through software vulnerabilities.
- Encrypt all the files on your laptop computer, so they become unreadable for anyone other than the user with the correct password

During your stay

- If information might be valuable to another government, company or group, you should assume that it will be intercepted and retained.
- Beware that your conversations may not be private or secure. China does not legal restrictions against technical surveillance. Most foreign security services have various means of screening incoming visitors to identify persons of potential intelligence interest. They also have well established contacts with hotels and common hosts that can assist in various forms of monitoring you. Electronic eavesdropping has been reported on airlines, in hotel rooms, taxis and meeting rooms.
- Do not use non-company computers to log into your company's network. Always consider any information conveyed through a non-company computer to be compromised, even if encrypted.
- Do not allow foreign electronic storage devices to be connected to your computer or phone. They may contain malware or automatically copy your stored electronic data. Do not use thumb drives given to you – they may be compromised.
- All information you send electronically can be intercepted especially wireless communications. Assume that anything you do on the device, particularly over the Internet, will be intercepted. In some cases, encrypted data may be decrypted
- Security services and criminals can track your movements using your mobile phone and can turn on the microphone in your device even when you think it is turned off.
- Do not invite strangers into your room
- Beware of new acquaintances who probe for information about you or who attempt to get you involved in what could become a compromising situation.
- When not in use, turn off the device(s). Do allow them to be in "sleep" or "hibernation" mode when they are not in active use
- Never use shared computers in cyber cafes, public areas, hotel business centers, or devices belonging to other travelers, colleagues, or friends

- A malware family known as “keylogger” is commonly used to steal personal information. Keyloggers are covert software applications or physical devices attached to computers that capture any information that is entered into the device. Always be skeptical of the security of an unfamiliar network or device; use free computing resources with the assumption that any information you enter could be seen by an unauthorized third party
- Maintain physical control of the device at all times. Do not check the device with checked baggage or secure in airport, train or hotel storage lockers. If you must store the device, remove the battery, memory expansion and SIM card and keep them with you
- Avoid connecting untrusted or unknown digital devices such as USB keys, media cards and USB chargers to your own devices. Avoid connecting your USB keys, etc. to untrusted devices
- Be aware of your surroundings and who might be able to view your screen/keyboard especially in public areas (e.g. shield passwords from view) and terminate connections when you are not using them.
- Where appropriate for security teams, maximize monitoring capabilities for devices that are associated with international travel and look for unusual activity and anomalies such as:
    - unauthorized connection attempts
    - connection attempts which occur at unusual times
- Unless there is a strict need, do not offer or allow another unauthorized person to insert any removable media on an IT system that connects to important information or a government network.
- Implement “full disk” encryption for portable electronic devices when traveling abroad.
- Many facilities offer travelers devices that they can use to connect to the Internet. This service is often available in business centers at hotels and airports. These devices should not be considered to be trusted access points. They are subject to the security practices and management of the providing organization. Malicious software and hardware may be inadvertently installed on these devices and made undetectable by its users and the provider. One example is that of a keylogger. A keylogger records information typed by the user on the computer, such as passwords and credit card numbers. They can be either covert software applications, or physical devices attached to computers. Travelers should not use these publicly accessible devices to view or transmit information that, if disclosed, could harm either the traveler or the traveler’s organization

Tablets/laptops

Tablets and laptops can also be attractive targets for malicious actors. The following tips may help secure these types of devices during travel

- Enable a password on the device and change the password prior to travel. Ensure the password meets the complexity requirement defined in the organization's security policy. Change the password at regular intervals and when the travel has been completed.
- Update the antivirus software before travelling.
- Install and enable a firewall on the device.
- Install software updates applicable for the device operating system and applications. If using a corporate laptop or tablet, consult the IT department to ensure such updates are applied.
- Disable wireless (Wi-Fi, Infra-Red and Bluetooth) connections when not in use.

- Ensure that all the required software/hardware is installed to avoid purchasing or downloading them while travelling.
- Avoid connecting USB devices and storage media obtained from unknown sources to the tablet or laptop.
- Encrypt the data stored on the device. Note that some countries do not permit entry of a device with encrypted data. This should be verified prior to travel
- If possible, set web browsers to their highest security setting

Wireless access points

- Travelers will encounter various Internet wireless access points, some of which are free to use. Examples of such services include free Internet provided during conferences, in hotels, in airports, or in other public locations. These access points are often unsecure networks that can be accessed by anyone. A network that requires a password to connect to may not be secured. While any wireless communication faces the risk of interception, the use of strong encryption can reduce the risk of information disclosure.
- As a best practice, avoid connecting to public wireless Internet and avoid transmitting information that you do not wish to be disclosed to an undesired or unauthorized party
- Avoid connecting via public Internet access point and open wireless access point

Data encryption: protecting your digital assets

When travelling, users may also employ encryption mechanisms to protect their data. In short, encryption transforms data in order to make it unreadable without a decryption key. Encryption may be used by travelers to send emails or to secure the content of storage media such as laptop hard drives and USB memory sticks. When properly implemented, encryption protects information against theft and interception. Email and file encryption software is available commercially from a number of reputable vendors. PGP, or Pretty Good Privacy, is an example of a commonly used tool for effective email and hard drive encryption. Travelers should consult their IT department regarding supported encryption options. Encryption is a very powerful and can be a somewhat unforgiving method of data protection. Depending on the nature of the encryption, should the decryption key required to unlock the encrypted data be lost, the data may not be retrievable.

Be aware of event related targeted emails

Targeted email attacks or spear phishing rely on exploiting the trust of the intended recipient. Before, during and after travelling to a scheduled even, a traveler may be subjected to targeted email attacks. These emails are designed to appear authentic and may entice the recipient into providing sensitive information or may unknowingly install malicious software on their device through a malicious attachment or web link. Travelers attending international conferences on topics of strategic and economic significance such as energy, environment, finance and military are common targets of spear phishing attacks.

Conference gifts

While attending conferences and training events, software and hardware may be offered to participants. These materials can either be free of charge or part of the paid content for course

delivery. Even when provided during the course of a planned activity, it is possible that these materials may inadvertently or purposely contain malicious software.

Travelers should be aware of all storage devices that they attach or load into the devices they carry. Do not attach or access any device that was received as a result of travel until it is properly evaluated by the organization's information technology team.

Upon your return

- Review your system access with your company's Information Security Officer. Access that is not accounted for should be investigated.
- Upon returning from your travels, immediately discontinue use of the device(s). The hard drive of the devices should be reformatted, and the operating system and other related software reinstalled, or the device properly disposed of.
- Reset all credentials including both remote and local accesses and other accounts, including personal accounts, even if not accessed during the travel
- Consult the user to obtain information about any reported issues or any other security concerns
- Apply due diligence and handling procedures prior to reusing the traveler's device
- Examine the device for the presence of malicious software before connecting to the corporate network.
- Continue to monitor the remote access accounts of employees who returned from travel to ensure unauthorized accesses are not occurring.
- Compare the current image with the baseline image (if available) to identify signs of compromise.
- Re-image the device before returning it to the travel inventory.
- Test removable memory devices such as CD-ROMs, DVDs and USB sticks that were received during travel before plugging them into the corporate network.
- Handle and report suspected incidents in line with organizational procedures and policies.

Risk · Pro

Conclusion

Cyber threats to your organization are becoming increasingly sophisticated and targeted. An information security breach can have a direct impact on your organization. The information held on your networks can accessed by intruders for their economic gain. There are many state and non-state actors who would benefit from having access to information which is essential to the functioning of your organization. Every organization faces different threats and security risks and needs to deal with them in different ways.

The information that someone travels with or the data accessed while travelling could be compromised by threat actors and used against the traveler or the organization represented. Potential threat actors include hostile and foreign intelligence services, criminals and competitors. The information targeted by the threat could be technical, military, financial or personal and a compromise of this information could provide the threat with a political, strategic, economic or competitive advantage.

Countries with significant state control of private industry, especially in telecommunications, may also be higher risk. Information, including customer data, product development documentation, countless emails and other proprietary information of value will be exposed to the Chinese government and competitors. The risk associated with the potential information disclosure depends on the nature and/or sensitivity of the information itself. Chinese are very good at installing keylogging software on your laptop. If a company has significant intellectual property that the Chinese are interested in and when you go over there with mobile devices, your devices will be penetrated.

Consumers and custodians of proprietary and sensitive information need to be aware of the potential harm if the information is lost or stolen. The best way to prevent information loss or compromise is not to travel with it in the first place, not to access it remotely and not to bring back external data files or devices and introduce these to the organization's information systems Its advisable to bring a temporary laptop or other computing device when going overseas. Upon returning home, the devices can be wiped to remove any malicious software. These preventative measures may not always be feasible. Therefore an organizational understanding of the risk travelers face, increased awareness by the travelers themselves and the implementation of technical and procedural measures to reduce the risk associated with the loss, theft, compromise or corruption of digital information and devices are essential enablers of business or mission objectives.

Business travelers should take measures to ensure not only the safety and security of themselves but also their business information while traveling to China. The security and safety measures suggested here will help protect you from data theft by Chinese intelligence and security organizations while traveling for business.

Manoj Jain
Managing Director
Riskpro
Email: manoj.jain@riskpro.in

Mangesh Sawant
Senior Vice President
Security Consulting & Risk Management
Riskpro
Email: mangesh.sawant@riskpro.in

www.riskpro.in

Risk · Pro

Be Secure

Stay Secure