COMPANIES

National Protective Security Authority

National Cyber Security Centre

SECURE INNOVATION

SCENARIOS

INTRODUCTION

The UK has a strong record in research and development and a vibrant startup ecosystem. This can make innovative UK companies attractive targets for:

- State actors looking to steal your technology
- Competitors seeking commercial advantage
- Criminals looking to profit from companies with weak security

Emerging technology companies of all sizes, particularly those with weak security, are being targeted by certain states. Those states may steal your technology to:

- Fast-track their technological capability, undermining your competitive edge
- Target, harm, and repress their own people to prevent dissent or political opposition, damaging your reputation
- Increase their military advantage over other countries, risking our national security

There are many ways a state-backed or hostile actor could try to get hold of your assets.

This booklet provides scenarios to help illustrate the security threats and how to protect your business from them.

INSIDER

People are an organisation's biggest asset. However, in some cases they can also pose an insider risk. As organisations implement increasingly sophisticated physical and cyber security measures to protect their assets from external threats, the recruitment of insiders becomes a more attractive option for those attempting to gain access.

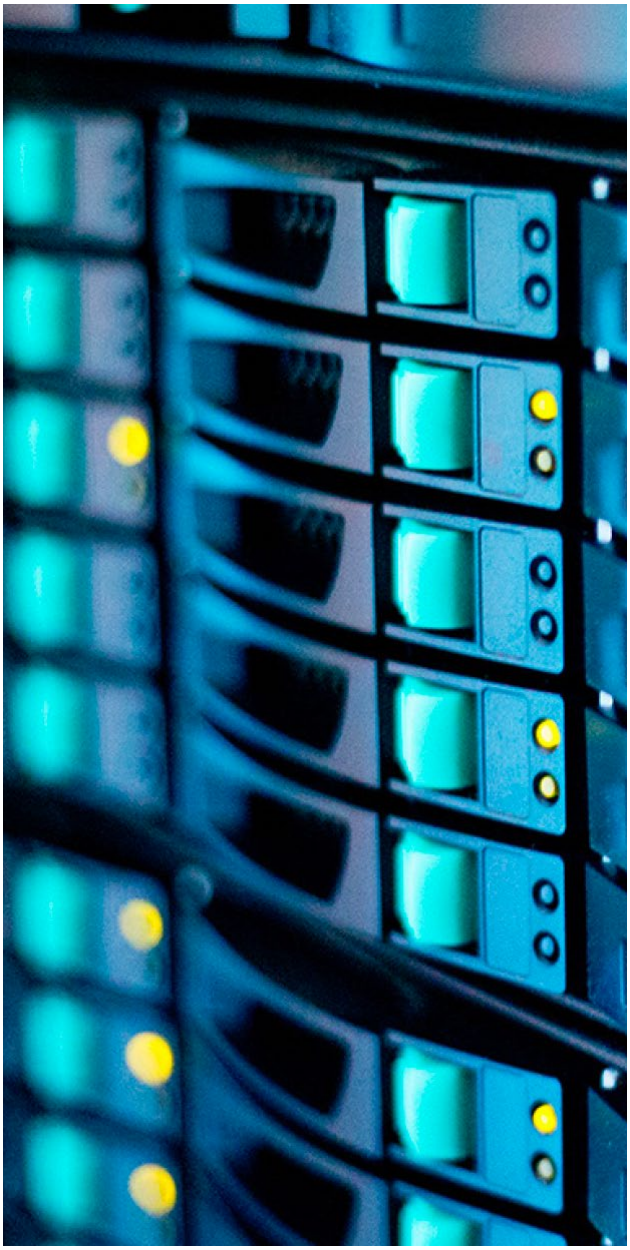
Risk

One of your employees is recruited by a foreign state actor to disclose sensitive information.

Scenario

An employee of a UK company previously worked in country X. Following several years employed in the UK, he became dissatisfied with his career progression and reached out to government officials in country X about potential jobs. He talked about his knowledge and skills, and implied he could duplicate his employer's intellectual property.

He resigned from his job, copied and downloaded the company's proprietary software to a memory card, and bought a one-way ticket to country X. His intention was to set up a rival, state-funded company in country X.



Actions to take can be found on the following page.

	ACTIONS TO TAKE
SECURITY CULTURE	➤ Start a conversation about security. ➤ Create an environment in which employees are confident that they can speak openly about security concerns.
PRE-EMPLOYMENT SCREENING	➤ Implement pre-employment security checks which include checking for employment history and any conflicts of interests.
SECURITY TRAINING	➤ Train your staff about security threats, and the policies and procedures in place to maintain security. ➤ Provide bespoke training for line managers so they can confidently assess security risks associated with their staff.
ROLE-BASED RISK ASSESSMENTS	➤ Conduct role-based security risk assessments so you understand which roles have higher security risk exposure. ➤ Provide additional training and support to employees in higher risk roles. ➤ Ensure staff accesses are role-specific – that they can only access assets and information they need and are trusted to use securely.
BEHAVIOURAL MONITORING	➤ Take steps to identify and address undesirable or concerning behaviours which might indicate increased insider risk. ➤ A supportive response can help improve the employee's relationship with the company, and therefore security.
TECHNICAL CONTROLS	➤ Develop appropriate identity and access management policies and processes to ensure only authorised individuals and systems have access to data or services. ➤ Implement technical controls to manage access and privilege, and introduce alerting on account creation, use, and modification. ➤ Implement technical measures to prevent, monitor, and audit data exfiltration by malicious insiders. ➤ Only use accounts with full privileges when absolutely necessary, and prioritise protecting accounts that have highly privileged access to systems, services and data. ➤ Review user accounts and systems for unnecessary privileges on a regular basis, and ensure privileged accesses are revoked when no longer required. ➤ Implement a robust credential management system, and ensure password reset processes are secure.

These measures will increase your chances of identifying insider threats early, but will also act as a deterrent to potential insiders.

RANSOMWARE

Ransomware is a type of malware that prevents you from accessing your computer (or the data that is stored on it). An attack of this type may result in your computer becoming locked, or the data on it being stolen, deleted or encrypted. Once data has been taken, you cannot assume that it will not be resold or published in the future. Some ransomware will also try to spread to other machines on the network, causing further disruption.

Risk

Cyber criminals prevent you from accessing your data and threaten to publish it online.

Scenario

A threat actor uses an unpatched vulnerability to gain access to a company's network. The actor moves laterally through the network to gain persistence and exfiltrate sensitive files, compromising the confidentiality of the organisations sensitive data.

The attacker then encrypts the files and demands payment in cryptocurrency to decrypt them; denying the availability of the organisation's data.

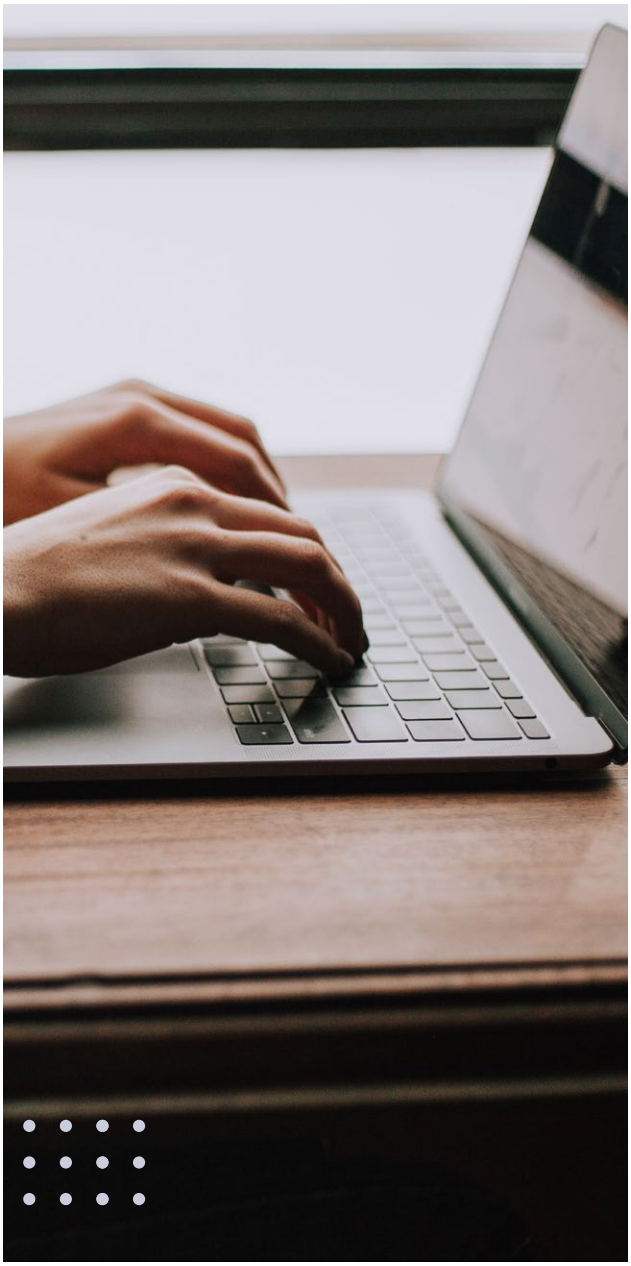
Because there are no recent back-ups, the encrypted files cannot be recovered (for a number of reasons, law enforcement discourage the payment of ransom demands). This results in the loss of many months' worth of work and causes significant reputational damage to the company.

Actions to take can be found on the following page.

	ACTIONS TO TAKE
MAKE REGULAR BACKUPS	➤ Make regular backups of your most important files. Ensure you create offline backups that are kept separate from your network and systems, or in a cloud service designed for this purpose, as ransomware actively targets backups to increase the likelihood of payment. ➤ Check that you know how to restore files from the backup, and regularly test that this works as expected.
PREVENT MALWARE BEING DELIVERED AND SPREADING	➤ Install security updates as soon as they become available to avoid running vulnerable software. ➤ Introduce mail filtering and spam filtering, which can block malicious emails and remove executable attachments, which are common methods of delivering ransomware. ➤ Provide security education and awareness training to staff, including the risks of clicking unknown links and opening attachments from unknown sources, and the importance of immediately reporting incidents ➤ Prevent malware spreading across your organisation by following NCSC guidance on preventing lateral movement. ➤ If your organisation has been infected with malware, limit the impact through immediately disconnecting infected devices from the network.
PREVENT MALWARE FROM RUNNING ON DEVICES	➤ Centrally manage devices in order to only permit applications trusted by the enterprise to run. ➤ Consider using antivirus or anti-malware products.
PREPARE FOR AN INCIDENT	➤ Identify your critical assets and determine the impact to these if they were affected by a malware attack. ➤ Create and exercise an incident management plan.

EMAIL COMPROMISE

Through well researched phishing attacks or gaining access to credentials of business email accounts, attackers can craft believable emails asking for executives or budget holders to transfer funds or reveal sensitive information.



Risk

Valid payments are diverted, or sensitive information is revealed.

Scenario

Poor password security leads to a successful brute force attack of an email account for a member of finance staff at an organisation that supplies computer components. This provides the attacker full access to the inbox, including sensitive emails – compromising confidentiality.

The attacker uses this access to email a company who they do business with, explaining they have had an issue with their bank and asking that the details for payments are changed. The email is crafted with a solid understanding of business language and tone, and the recipient proceeds to amend the payment details, diverting payments to the attacker.

The compromise is not discovered until the supplier contacts the company asking why they haven't been paid. This results in significant financial loss and reputational damage.

Actions to take can be found on the following page.

	ACTIONS TO TAKE
MAKE YOURSELF A HARDER TARGET	➤ Limit the information about yourself publicly available (eg across social media and your organisation's website) to reduce the amount of data criminals can use to create convincing phishing emails.
EDUCATION AND AWARENESS	➤ Provide staff education on common cyber threats and how to spot phishing emails. ➤ Ensure staff use strong passwords and turn on 2-step verification (2SV). ➤ Create a culture where staff feel confident questioning if something is genuine and report immediately if they think they've been a victim of an email compromise or phishing attack.
SECURE WORKING PRACTICES	➤ Make processes more resistant to email compromise or phishing by ensuring that all important email requests are verified using a second type of communication (such as SMS message, a phone call, logging into an account, or confirmation by post or in-person). ➤ Have a method whereby staff can check the authenticity of suspicious emails through your IT department.

PHYSICAL

Anyone with physical access to your assets could steal or compromise them. This could be theft of a prototype, laptop, or physical documents; or gaining physical access to a server or computer to download content or compromise it in some other way.

Risk

Someone accesses or steals your technology from your premises.

Scenarios

Several months after a high-profile visit by a delegation from country X, several laptops were stolen from a UK company. Several years later, pictures began emerging showing a firm in country X making a product virtually identical to the UK company's device. The UK company lost their competitive edge and struggled to survive.

A company worked in a shared office space where there were frequent visitors. They did not have a segregated area, or any access controls protecting their sensitive assets. A visitor to their premises stole various documents which were left at an unoccupied desk. These documents showed sensitive information about the company's manufacturing process which would be invaluable to a competitor.

Actions to take can be found on the following page.

	ACTIONS TO TAKE
IDENTIFY YOUR CRITICAL ASSETS	➤ Identify the physical assets that are critical to your business' success, or could allow access to critical intangible assets (eg prototypes, computers, servers).
CENTRE SECURITY AROUND YOUR CRITICAL ASSETS	➤ Place barriers (physical or virtual) around those critical assets. ➤ Control access to the asset only to those employees who need it and are trusted to use it securely. This should include visitor management policies. ➤ Implement measures to detect and respond to unauthorised activity. ➤ Consider putting proportional procedures in place to manage camera or phone usage and conduct bag checks.
PREPARE FOR SECURITY INCIDENTS	➤ Plan and exercise your security incident response procedure so you can respond quickly and effectively when required, and limit the damage caused by a security breach.
TECHNICAL CONTROLS	➤ Use full volume encryption software to ensure that all user data, including sensitive user files, is encrypted at rest. ➤ Introduce a risk-based policy and technical controls on the use of removable media.

INTERNATIONAL TRAVEL

Travelling internationally could increase your exposure to security risks. Certain countries are actively targeting UK innovation. Travel to those countries, or third-party countries where they can operate without scrutiny, could put your people and innovation at risk.

Risk

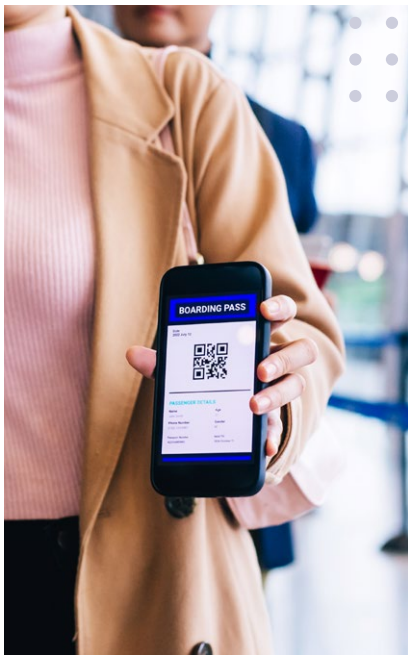
Someone accesses or steals your innovation, or attempts to recruit your employee whilst they are travelling internationally.

Scenarios

A company was invited to country X to speak at a conference. The employee who attended took their work laptop with them so they could work whilst overseas. During the conference, they left their laptop in their hotel room. IT monitoring on their return identified that an external drive was attached to the laptop and sensitive files had been downloaded.

An employee was required to travel to a country Z regularly for work. Whilst attending a conference in country Z, they were approached by another delegate who asked increasingly probing questions about their latest technology. This interaction was followed by engagement on a professional networking site and offers of expenses paid travel, in an attempt by country Z to cultivate and recruit the employee.

The employee was successfully recruited and, over the course of three years, stole dozens of confidential documents and datasets. The stolen material was used to set up a rival company in country Z, costing their original employer its competitive edge in an emerging market.



Actions to take can be found on the following page.

	ACTIONS TO TAKE
INTRODUCE A TRAVEL SECURITY POLICY	➤ Develop a travel policy which helps mitigate the risks associated with international travel. ➤ Consider whether the travel is high-risk and necessary; protect electronic devices taken overseas; remove non-essential data from them; ensure travellers know what business information is sensitive and what can be shared; encourage the reporting of any security incidents to security leads or line managers. ➤ Consider the use of burner technology (eg. laptops, phones) for staff travelling internationally.
CONSIDER EXPORT CONTROL	➤ Consider whether the work being conducted overseas is subject to export controls, and apply for appropriate licences.
CONSIDER LOCAL LAWS	➤ Ensure the traveller and wider business understand the rules and laws staff are required to comply with in their destination country.
SECURITY TRAINING	➤ Train your staff about the security threats associated with international travel, and the policies and procedures in place to maintain security. ➤ Train your staff about safe and secure practices when using social media. ➤ Provide bespoke training for line managers so they can confidently assess security risks associated with their staff.
TECHNICAL CONTROLS	➤ Use full volume encryption software to ensure that all user data, including sensitive user files, is encrypted at rest. ➤ Develop appropriate identity and access management policies and processes to ensure only authorised individuals and systems have access to data or services. ➤ The use of VPN technology should also be considered when using devices abroad.

INVESTMENT

In a minority of cases, the investment that you are seeking may unintentionally pose a risk to your company's security. Certain states may use domestic or foreign investment to gain access and influence, either to harm your company's interests or the UK's national security. This could include using information from your company to undermine your competitiveness.

Risk

Someone with hostile intent gains access to your sensitive assets, and/or influence over your business, via investment.

Scenarios

After agreeing a takeover from an investor from country X, a UK company signed several technology-transfer agreements with their would-be acquirer. These entailed providing training and revealing technology in return for a proportion of the company's agreed sale price. Several years later, the investor failed to complete the deal citing difficulties obtaining approval from country X's government. The UK company was left facing administration.

	ACTIONS TO TAKE
BACKGROUND CHECKS	➤ Conduct background checks on prospective investors to assess the risk of working with them. ➤ Verify they are who they say they are; check there are no obvious sources of unwanted control or influence; confirm that their values and intentions align with your own.
LIMIT EXPOSURE	➤ Limit data sharing to just the data or information which is appropriate. ➤ Ensure third parties are handling any sensitive data appropriately and securely.
PROTECT YOUR ASSETS	➤ Compartmentalise your most sensitive data or projects. ➤ Include protections for your assets and data within investment documentation, and ensure they are enforceable in the country where your investor is based.
CONSIDER THE NATIONAL SECURITY AND INVESTMENT ACT	➤ Check whether you are required to submit a mandatory notification of the investment to the UK Government. ➤ If not, consider the benefits of submitting a voluntary notification, which includes significant due diligence of the investor by the UK government.

OVERSEAS JURISDICTIONS

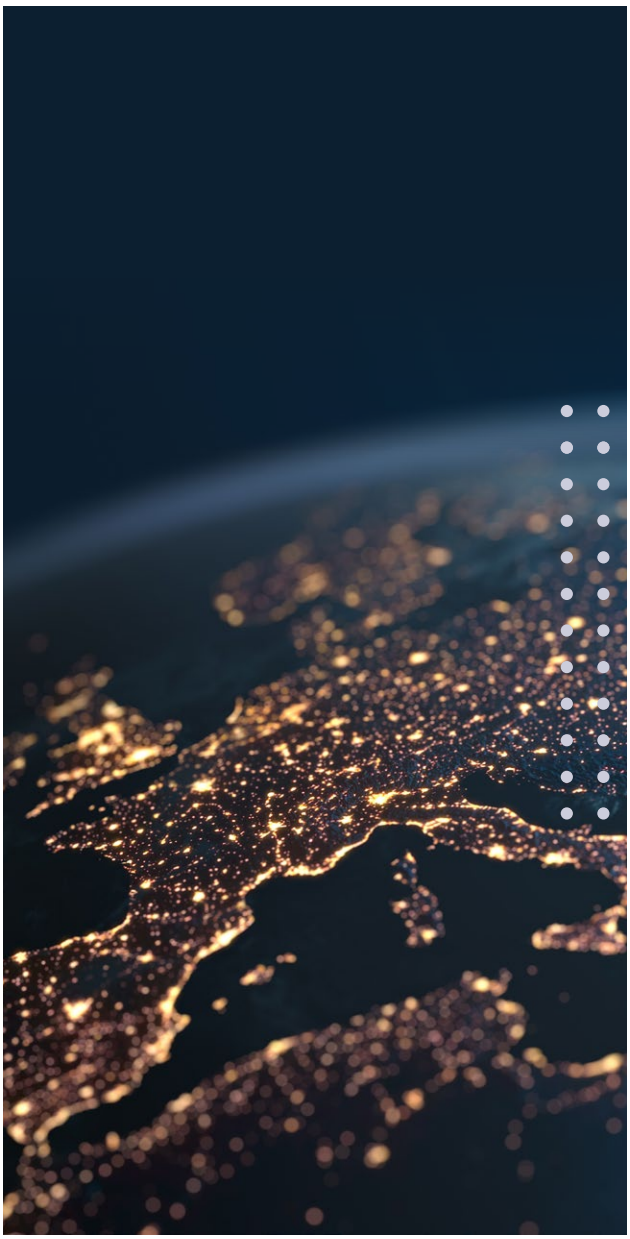
Different countries have different export control laws, as well as laws regarding the handling and storage of intellectual property (IP) and data. National security laws in foreign countries can allow that country's government to access data or information stored in, or transmitted via, that country.

Risk

Local laws in a country you are operating in result in the loss of your sensitive assets to the state or a local business.

Scenarios

A company wanted to expand into country X. They entered into a joint venture (JV) with a company in country X to enjoy national treatment. The UK company was the majority shareholder, but agreed that the JV's CEO would be from, and domiciled in, country X. Country X's laws meant that the CEO dictated the company's operations and could act without supervision from the Board. The CEO transferred IP ownership from the JV into another company in their name. The UK company had no legal recourse and lost their IP rights in country X.



Actions to take can be found on the following page.

	ACTIONS TO TAKE
CONSIDER LOCAL LAWS	➤ Familiarise yourself with the IP framework and enforcement processes in overseas markets. Register for IP rights in advance of entering the market, and ensure you are resourced to defend those rights if required. ➤ Research the national security and data protection laws in countries you are looking to operate in. Consider how those laws could impact on the security of your assets, people, and business.
COMPLY WITH UK LAWS	➤ Consider whether the work being conducted overseas is subject to export controls, and apply for appropriate licences. ➤ Comply with UK GDPR when transferring data outside the UK.
BACKGROUND CHECKS	➤ Conduct background checks on prospective partners to assess the risk of working with them. ➤ Verify they are who they say they are; check there are no obvious sources of unwanted control or influence; confirm that their values and intentions align with your own.
LIMIT EXPOSURE	➤ Limit data sharing to just the data or information which is appropriate. ➤ Ensure third parties are handling any sensitive data appropriately and securely.
PROTECT YOUR ASSETS	➤ Compartmentalise your most sensitive data or projects. ➤ Include protections for your assets and data within legal documentation, and ensure they are enforceable in the country where your partner is based.

SUPPLY CHAIN

Businesses are targeted via their supply chain for two core reasons:

1. *Their suppliers have weaker security measures in place so are easier to attack; or*
2. *One of their suppliers serves various organisations of interest, so targeting that supplier gives a hostile actor access to several targets via a single attack.*

By giving suppliers access to information without setting expectations about how it should be protected, you are exposing your business to a range of security threats.

Risk

Your sensitive information or assets are stolen or compromised by a vulnerable or malicious supplier.

Scenarios

A technology company was procuring a new cloud service. The cloud service provider was granted privileged access to the company's IT systems, which gave them access to a wide range of sensitive data. The service provider held the company's data in servers in country X. Country X is actively pursuing technological advances. Country X's national security laws meant that it could demand the cloud service provider shared the technology company's data with the state, without disclosing it to them.

A software provider was working with a range of small businesses in the technology sector. The intelligence service of country Z, who are actively pursuing technological advancements, targeted the software provider as a route into several organisations of interest. They successfully implanted malicious code within a software update, facilitating their access to the computer networks of the software provider's customers.

Actions to take can be found on the following page.

	ACTIONS TO TAKE
BACKGROUND CHECKS	➤ Conduct background checks on prospective suppliers to assess the risk of working with them. ➤ Verify they are who they say they are; check there are no obvious sources of unwanted control or influence; confirm that their values and intentions align with your own. ➤ Identify whether your prospective supplier falls under another country's jurisdiction by virtue of its geography or ownership structures. If so, understand the laws by which your supplier may be bound.
LIMIT EXPOSURE	➤ Limit data sharing to just the data or information which is appropriate. ➤ Ensure suppliers are handling any sensitive data appropriately and securely.
PROTECT YOUR ASSETS	➤ Compartmentalise your most sensitive data or projects. ➤ Include protections for your assets and data within supplier contracts. Include minimum requirements for suppliers' protective security measures. Include requirements for notifications, and provisions for termination, of offshoring of your data, changes of ownership, investments, or any other change which could impact on the security of your information and data. ➤ Check that suppliers are meeting their protective security requirements and are testing that the protective security measures they have in place are effective.