CPNI
Centre for the Protection of National Infrastructure

National Cyber Security Centre

SECURE INNOVATION

SECURITY ADVICE FOR EMERGING TECHNOLOGY INVESTORS

FOREWORD

The UK is a world leader in research and innovation, and much of this is dependent on our strong international partnerships and international workforce. Our open and collaborative innovation environment has supported enormous advances across science and technology. The COVID-19 pandemic has shown the power and importance of international collaboration: governments, businesses, charities and universities from across the world united around a common goal, delivering the fastest vaccine development programme in history.

Due to the strength of this vibrant technology ecosystem, UK businesses have been a target for a range of actors who would seek to gain commercial, technological or military advantage from the innovations these firms have made. Protecting physical and information assets are essential parts of managing any successful business. Companies operating in this space should be mindful of these risks and consider how they can make their own organisations more resilient.

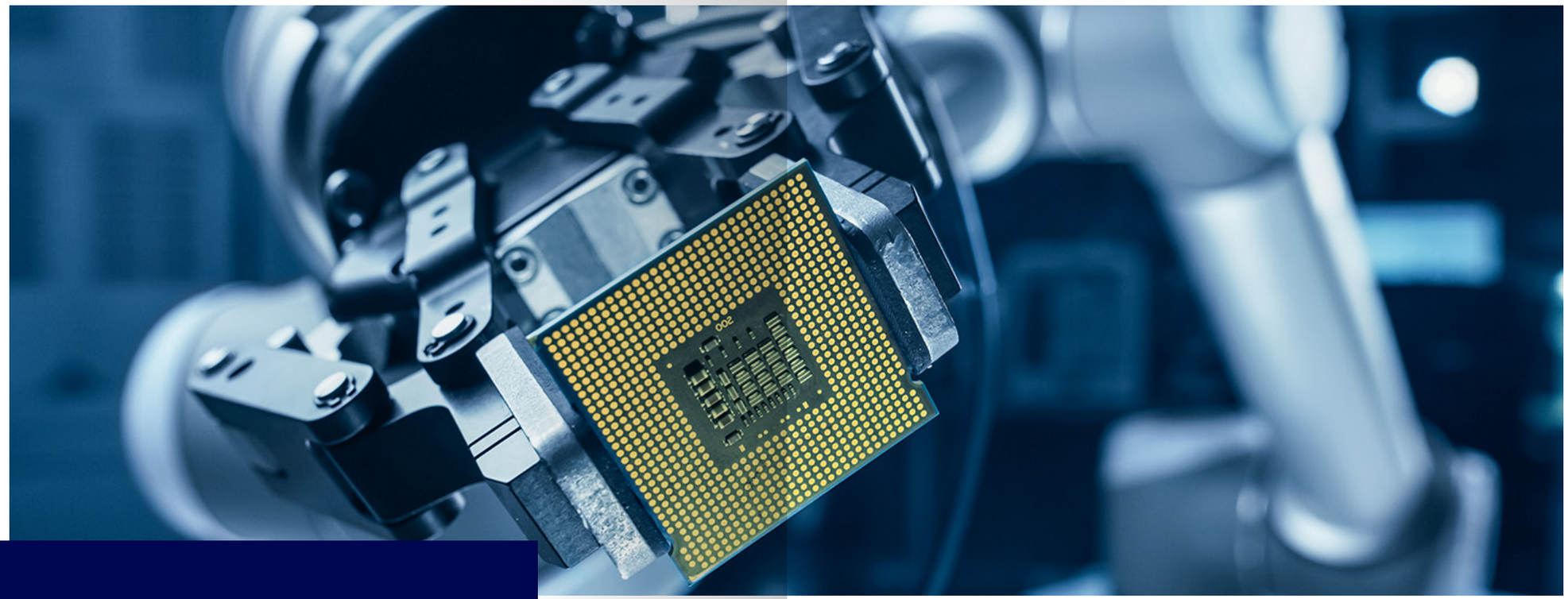
This booklet from the Centre for the Protection of Natural Infrastructure (CPNI) and National Cyber Security Centre (NCSC) sets out simple guidance for innovative start-ups and growing businesses, helping them to embed strong security practices and ensure that they collaborate with other organisations securely. I encourage all organisations – large and small – to review this guidance and consider the practical suggestions included within. Being open and collaborative also requires being secure.

Sir Patrick Vallance

Government Chief Scientific Adviser and Head of Government Science and Engineering Profession

SECURITY FROM THE START

SECURITY AS THE STARTUP GROWS



INTRODUCTION

This guidance is for early-stage investors in emerging technology companies. It suggests questions you can consider during the due diligence process and your early conversations with portfolio companies. Doing so will help you to make informed decisions that will increase the likelihood of seeing a return on your investment.

The UK's vibrant startup ecosystem and strong record in research and development bring plentiful opportunities for those investing in innovative startups. Secure Innovation aims to protect those startups from risks by providing practical steps to lay the foundations for strong security.

Startups struggling to establish themselves may find it difficult to prioritise security. These questions are also intended to help you to influence your portfolio companies' attitudes to security, helping them to succeed and to protect your investment.

Your ability to guide companies towards greater security and compliance may make you more attractive as an investor.

This booklet is divided into two sections: security from the start and security as the startup grows. This reflects the fact that both the threats faced by the startup and the company's resources to deal with those threats will change over time. You can manage this by continuing to discuss security for the duration of your involvement with the company.

WHAT IS THE RISK?

IN THIS SECTION:

- Recognising the security risks to your investments and the groups that pose them

The UK has a strong record in research and development and a vibrant startup ecosystem. This can make innovative UK companies attractive targets for a range of actors, such as:

Competitors

Seeking commercial advantage.

Criminals

For instance, cybercrime is a major threat to businesses of all sizes, as criminals will try to and access any vulnerable network.

Hostile actors backed by a foreign state

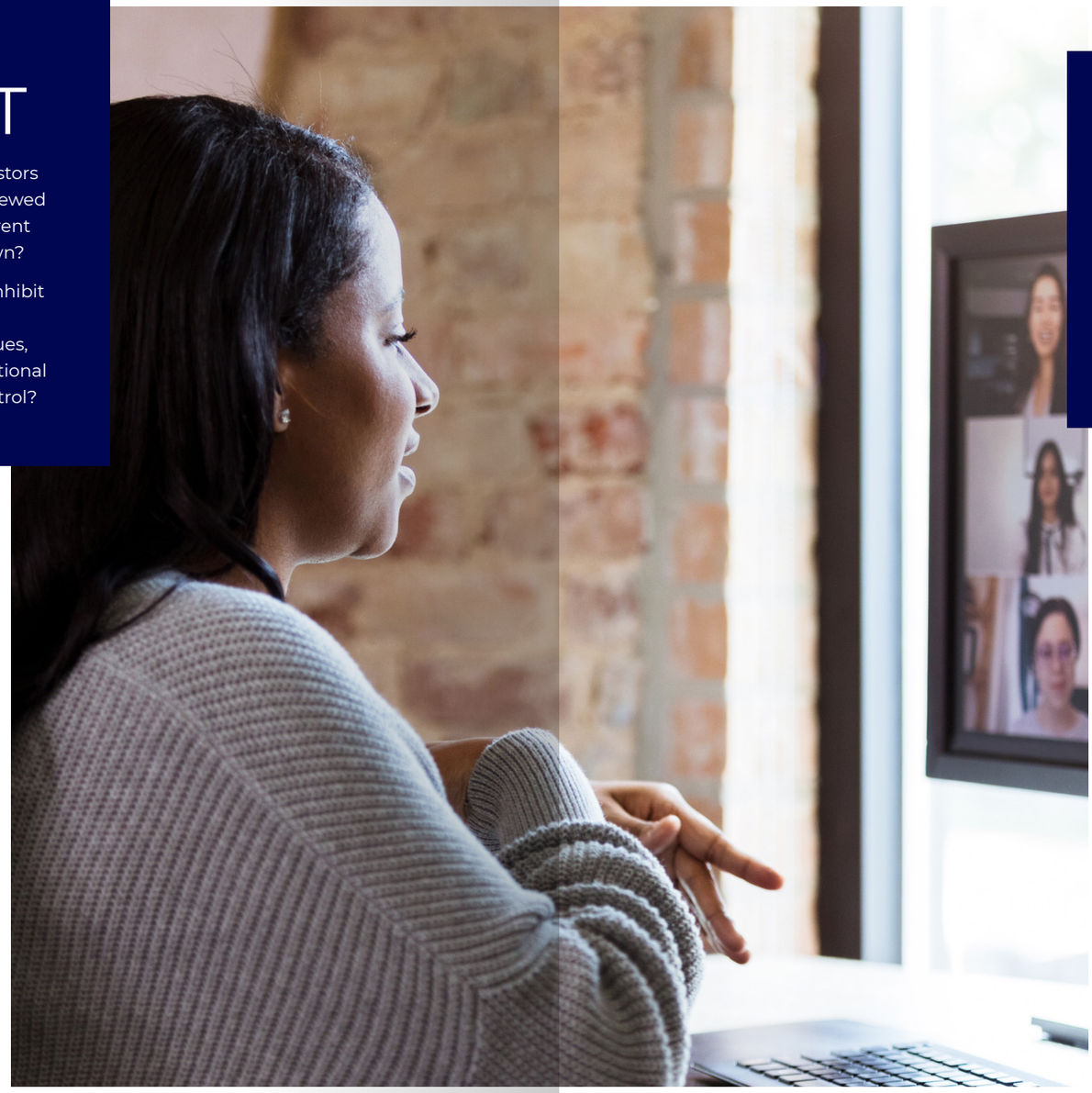
These actors may seek access to emerging technology for reasons that risk undermining the company's success or are at odds with the UK's interests and values. The latter could include:

- to develop a research and innovation base to increase military and technological advantage over other countries
- to deploy their technological and military advantages against their own population to prevent internal dissent or political opposition

PRE-INVESTMENT

- Does the company have any overseas investors associated with a country which may be viewed as hostile to the UK or one which has different democratic and ethical values from our own?
- Could the involvement of other investors inhibit future fundraising or sale of the company, because of legal, ethical or compliance issues, particularly in relation to sanctions, the National Security and Investment Act or export control?

The above questions should form part of your due diligence investigations into the startup and any other investors involved. They are intended to help protect your reputation as well as improve the chances of gaining a successful return on your investment.



LEADING BY EXAMPLE

IN THIS SECTION:

- Is security owned and discussed at Board level?

ENDURING ROLES AND RESPONSIBILITIES FOR SECURITY NEED TO BE ESTABLISHED EARLY.

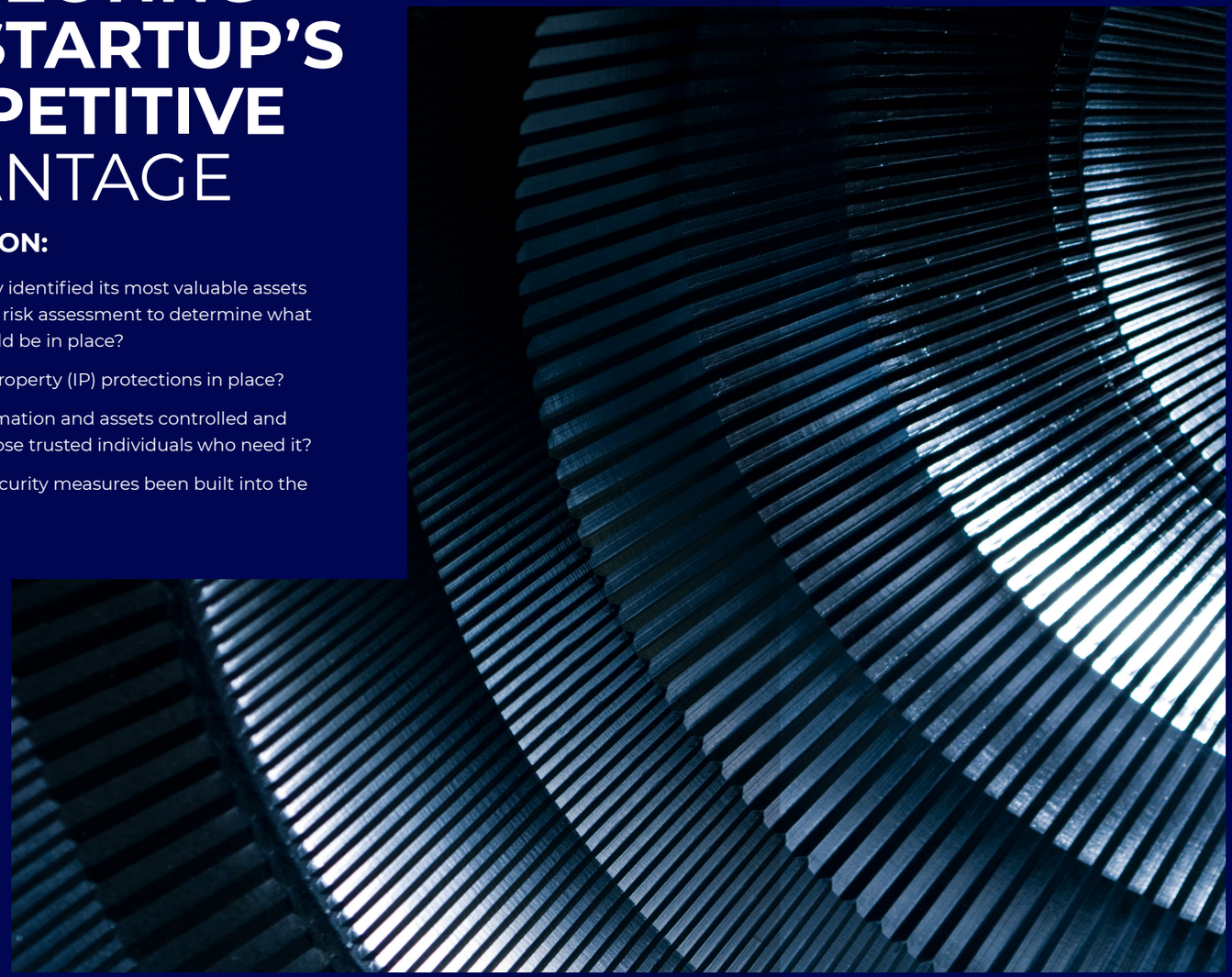
This means identifying a senior leader with the authority and responsibility to ensure that security is considered alongside other business risks. Clear accountability within the startup's leadership will show you that they are taking security seriously and provide you with a point of contact for security.

This is also important when developing an effective security culture, where people feel enabled to protect the things which are most valued. A good security culture at the startup level is an essential component of a robust security regime. Your early engagement can help to shape the startup's culture to be one in which security, and any security incidents, are openly discussed and learned from.

PROTECTING THE STARTUP'S COMPETITIVE ADVANTAGE

IN THIS SECTION:

- Has the company identified its most valuable assets and conducted a risk assessment to determine what mitigations should be in place?
- Are intellectual property (IP) protections in place?
- Is access to information and assets controlled and limited to just those trusted individuals who need it?
- Have essential security measures been built into the IT setup?



Small companies with limited resources will not be able to protect everything. Security decisions should be prioritised, proportionate to the threat and based on a thorough understanding of which assets are most critical to the success of your investment and the startup. Critical assets could include the people, premises, products, services, information, technology, and knowledge that the company could not exist without.

The following questions will help you to discuss this further with companies you are investing in:

- **WHAT ARE YOUR COMPANY'S** GOALS AND PRIORITIES?
- **WHAT ARE YOUR MOST** CRITICAL ASSETS?
- **WHAT ARE THE THREATS TO THOSE** CRITICAL ASSETS?
- **WHAT IS THE LIKELIHOOD AND CONSEQUENCE OF A** THREAT AFFECTING YOU?

The security of any technology products that the startup produces will also be central to the success of the product and, consequently, of the startup. Technology is most secure when security has been built in from the start. Have products been designed to be secure by default? Products designed in this way will fare better in the long term, and so be more usable, than products with security added as an afterthought.

Security is most robust when based on a combination of policy, physical, people and cyber security measures.

In 2020, criminals tried to bribe a Tesla employee to install malware in one of the company's factories. The malware was designed to exfiltrate data and extort ransom money. The FBI arrested a Russian national for attempting to "recruit an employee of a company to introduce malicious software into the company's computer network". The plan was thwarted when the employee reported the incident.

The threat of criminals recruiting an insider to exploit their physical access is not new, but is now being used to facilitate cyber attacks. This incident demonstrates how a company needs to integrate people, physical, and cyber security to protect itself, as well as its investors.

01
CASE STUDY

S-RM, 'When the virtual and physical collide: the need for a joint approach to cyber and physical security', 12/01/2021

THE FOLLOWING QUESTIONS WILL HELP YOU TO DETERMINE WHETHER THE COMPANY HAS BUILT ESSENTIAL SECURITY MEASURES INTO ITS IT SETUP:

- Have both firewall and antivirus software been enabled?
- Is strong password protection and strong encryption (where available) enabled for devices and accounts?
- Is all IT equipment and software regularly updated, ideally using automated updates?
- Are regular backups taken of critical data and stored away from the main system?
- Is consideration given to the trustworthiness of internet connections used?
- Are tools enabled to track, lock or wipe lost or stolen mobile devices?

SECURING THE SUPPLY CHAIN

IN THIS SECTION:

- Has the startup sought suppliers whose security arrangements meet their requirements?
- Does the company have a risk assessment process for using external suppliers?
- When using third party services, has the startup considered the impact of relevant regulation, such as the General Data Protection Regulation (GDPR)?

Outsourcing to an external provider, which may have specialist expertise that a small organisation would struggle to resource, often brings enormous benefits for a startup. However, supply chains present a complex security risk, so should form part of your due diligence process.

The startup can manage its supply chain risks by:

1. Assessing how the relationship with that provider affects the startup's risk profile
2. Seeking suppliers whose security offer and level of assurance best meets their requirements
3. Considering the impact of relevant regulation, such as the General Data Protection Regulation (GDPR)

MANAGING RISKS FROM ADDITIONAL COLLABORATION

IN THIS SECTION:

- Does the collaboration partner share your and the company's values and objectives?
- When collaborating, has the company limited the data, information, and knowledge it shares to only what is necessary and within its risk tolerance?

It is also worth making the company aware of how their choice of third parties may impact upon your, and potential customers', willingness to do business with them. For instance, are the values and objectives of the parties that the company wishes to collaborate with aligned with your own?

Companies should conduct due diligence when considering a new collaboration. This should include ethical, legal and national security considerations as well as financial. This will ensure they have all the information needed to make an informed and balanced decision about whether they want to work with them.

Regardless of the collaboration partner, companies should always ensure that any risks they are exposed to are managed in line with their risk appetite (and yours, as the investor). For instance, are their networks segregated and are there appropriate technical and policy protections to ensure that data shared with partners (customers or other potential investors) is limited to what is necessary?

Partners may ask the startup to demonstrate their commitment to cyber security. The Cyber Essentials certification demonstrates that a company has the technology and policies in place to guard against common cyber threats, and is a minimum requirement for certain government contracts.

Early negotiations with potential investors, customers, or collaborators can reveal sensitive details. This will be especially harmful to a company if they have not made a risk-managed decision regarding what information is shareable and what is not.

Smiths (Harlow) Limited, a UK precision engineering company, agreed an £8m deal with China's Future Aerospace in October 2017. On receipt of the first £3m, the company shared sensitive details and committed to train Future Aerospace's engineers.

According to press reports in January 2020, Future Aerospace subsequently cited difficulties in approval processes within China and withdrew from the deal without paying the rest of the agreed amount.

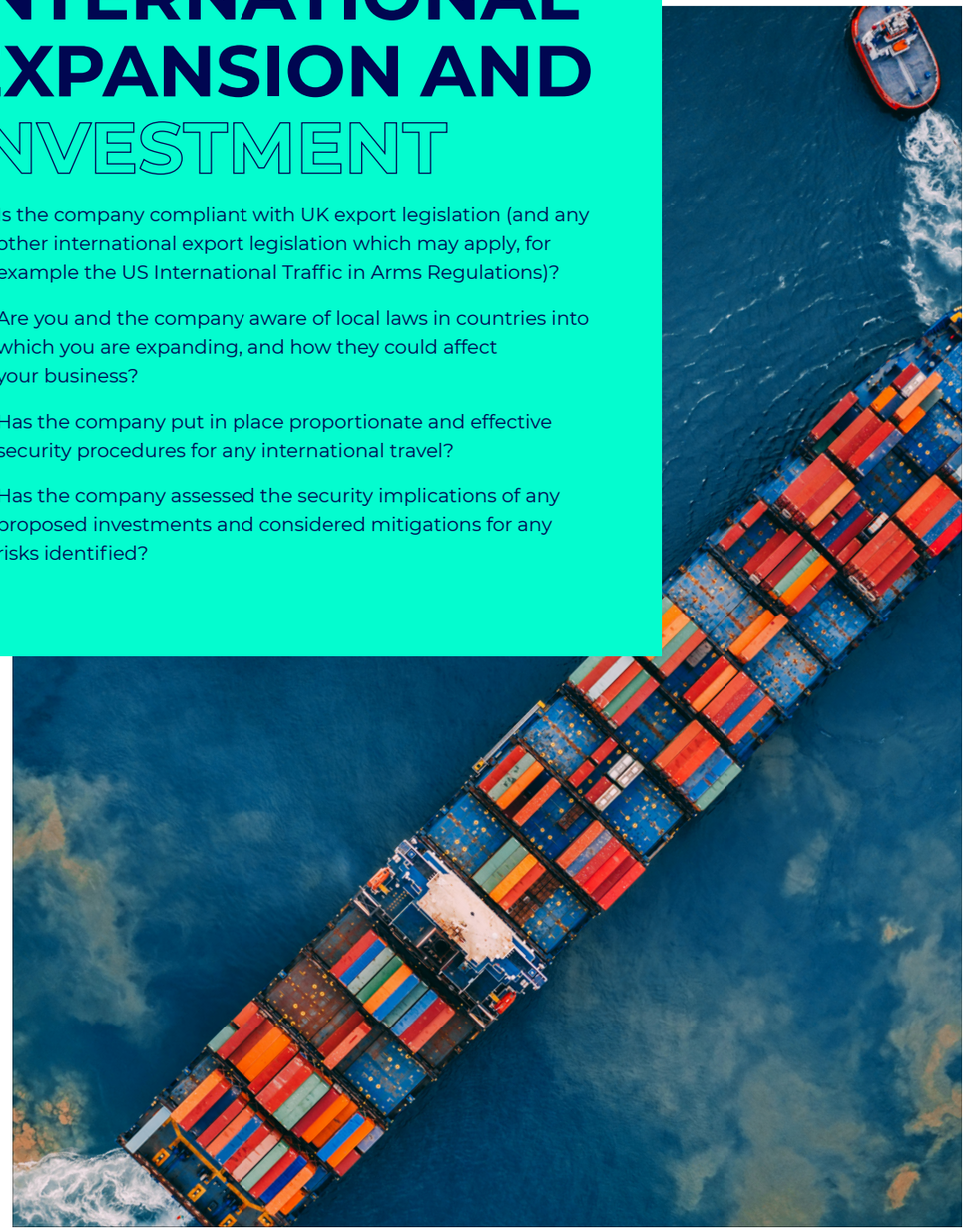
Smith (Harlow) Limited's competitive advantage and intellectual property may have already been compromised. Their links to China also reportedly cost them their licence to make military equipment for western powers. The company was left facing administration in February 2020, citing Future Aerospace's theft of their IP and reneging on the deal as the cause.

02
CASE STUDY

The Times, 'China's Future Aerospace 'stole trade secrets', says Smiths (Harlow)', 26/01/2020

INTERNATIONAL EXPANSION AND INVESTMENT

- Is the company compliant with UK export legislation (and any other international export legislation which may apply, for example the US International Traffic in Arms Regulations)?
- Are you and the company aware of local laws in countries into which you are expanding, and how they could affect your business?
- Has the company put in place proportionate and effective security procedures for any international travel?
- Has the company assessed the security implications of any proposed investments and considered mitigations for any risks identified?



Exports may be subject to UK and international sanctions or export control regulations, including the US International Traffic in Arms Regulations (ITAR), particularly when items may have military as well as civilian applications. The Export Control Joint Unit (ECJU) provides support and advice.

AS ABOVE, THE IDENTITY OF OTHER INVESTORS INTO YOUR PORTFOLIO COMPANIES MAY IMPACT YOU TOO, ESPECIALLY WHEN CONSIDERING:

The investors' reputation and trustworthiness

The source of their funds (hostile actors may seek to obfuscate their involvement)

Any implications of the legal regime they are subject to (especially for an overseas investor)

Whether they have any unexpected commercial, political or military ties

Whether they are on the entity listing of other countries, particularly those the startup is, or may consider, doing business with

THE NATIONAL SECURITY AND INVESTMENT ACT

The National Security and Investment (NSI) Act has been passed to give businesses and investors the certainty and transparency they need to do business in the UK while protecting the UK's national security. The Act will provide the Government with powers to screen investments to assess and address any national security risks.

Investors, including UK investors, must notify and receive clearance from the UK Government before making qualifying acquisitions relating to 17 defined areas of the economy. You can also voluntarily notify the UK Government of acquisitions that fall outside mandatory requirements. The UK Government can request to review any qualifying acquisition that may pose a national security risk.

SECURITY FOR A GROWING TEAM

IN THIS SECTION:

- Has the company put in place pre-employment screening processes for all recruits?
- Does the company provide security training for all staff, including at the point of induction?

As the startup grows, it is likely to hire new employees, contractors, and suppliers, and may no longer be able to rely primarily on personal relationships to establish trust. It is vital that companies can trust their workforce, both to protect valuable assets and information and to report potential security incidents. Ways to manage this include:

01

Making staff access controls role-specific, so access to sensitive assets is restricted to only those individuals who need it and are trusted to use it securely.

02

Security screening for new recruits and staff moving into sensitive roles.

03

Openly discussing security and establishing a security training package to make security a shared responsibility.

Effective screening and security training can help a company not only to protect its ideas and your investment, but also its people. Working on emerging and sensitive technologies can make individuals a target for both hostile state actors and competitors.

Xu Yanjun is reportedly a Senior Officer in the Ministry of State Security in China. He was indicted by the US in 2018 for allegedly targeting US and European aviation and aerospace companies. His methodology involved approaching employees in science and technology sectors under the cover of a Science & Technology promotional body. Xu would offer speaking engagements and trips to China, then attempt to elicit further information once a relationship was established.

In one case, Xu allegedly paid an engineer US$3,500 plus expenses to travel to China and speak at a university. Afterwards, he sought answers to questions on composite materials used by the engineer's company and requested a directory map of the company.

This example also suggests that following up on uncharacteristic IT or personnel behaviours (including travel) can allow companies to act, in the rare instances where these behaviours may indicate an insider threat.

03
CASE STUDY

US District Court Southern District of Ohio Western Division, Indictment, 04/04/2018

US Department of Justice, 'Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S. Aviation Companies', 10/10/2018

PREPARING FOR SECURITY INCIDENTS

IN THIS SECTION:

- Has the company established and tested an incident management plan?
- Can the company detect and investigate unexpected behaviour in IT and staff?

You cannot protect against all eventualities, but the damage caused to your investment by a breach can be reduced through a well-planned and executed response.

This means the company needs to establish and test an incident management plan and processes to detect and explore unexpected behaviour. The NCSC's 'Exercise in a Box' is a free online tool to help organisations practice their response to common cyber attack scenarios.

When handled sensitively, an understanding of any uncharacteristic behaviour in staff can help to prevent, as well as detect, an increased insider risk by improving the relationship between staff and company.

Further Information

Please see the following websites for more information.

www.CPNI.gov.uk

www.NCSC.gov.uk

Resources

Risk Assessment: ***www.cpni.gov.uk/rmm/protective-security-risk-management***

NCSC's small business guide: ***www.ncsc.gov.uk/collection/small-business-guide***

Secure Business: ***www.cpni.gov.uk/secure-business***

Guidance for the tech sector on opportunities with China: ***digitalandtechchina.campaign.gov.uk/***

Secure by default: ***https://www.ncsc.gov.uk/information/secure-default***

The NCSC's Board Toolkit: ***www.ncsc.gov.uk/collection/board-toolkit***

CPNI's Passport to Good Security for Senior Executives: ***http://www.cpni.gov.uk/managing-my-asset/leadership-in-security/board-security-passport***

Cyber Essentials: ***https://www.ncsc.gov.uk/cyberessentials/overview***

National security and investment mandatory notification sectors: ***www.gov.uk/government/consultations/national-security-and-investment-mandatory-notification-sectors***

UK Consolidated List of Strategic Military and Dual-Use Items that Require Export Authorisation: ***www.gov.uk/government/publications/uk-strategic-export-control-lists-the-consolidated-list-of-strategic-military-and-dual-use-items-that-require-export-authorisation***

The Export Control Joint Unit: ***www.gov.uk/government/organisations/export-control-organisation***

Exercise in a Box: ***https://www.ncsc.gov.uk/information/exercise-in-a-box***

Disclaimer

The information contained in this document is accurate as at the date it was created. It is intended as general guidance only and you should not rely on it.

This information should be adapted for use in the specific circumstances required and you should seek specialist independent professional advice where appropriate before taking any action based on it. To the fullest extent permitted by law, CPNI and NCSC accept no liability whatsoever for any loss or damage incurred or arising as a result of any error or omission in the guidance or arising from any person acting, relying upon or otherwise using the guidance. Full terms and conditions governing the use of this guidance are available on our website at http://www.cpni.gov.uk . All references to CPNI in the Disclaimer section of those terms and conditions shall in respect of this guidance also include NCSC.

Freedom of Information Act (FOIA)

This information is supplied in confidence to the named reader and may not be disclosed further without prior approval from CPNI. This information is exempt from disclosure under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation.