CPNI
Centre for the Protection of National Infrastructure

National Cyber Security Centre

SECURE INNOVATION

SECURITY ADVICE FOR EMERGING TECHNOLOGY COMPANIES

FOREWORD

The UK is a world leader in research and innovation, and much of this is dependent on our strong international partnerships and international work force. 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.

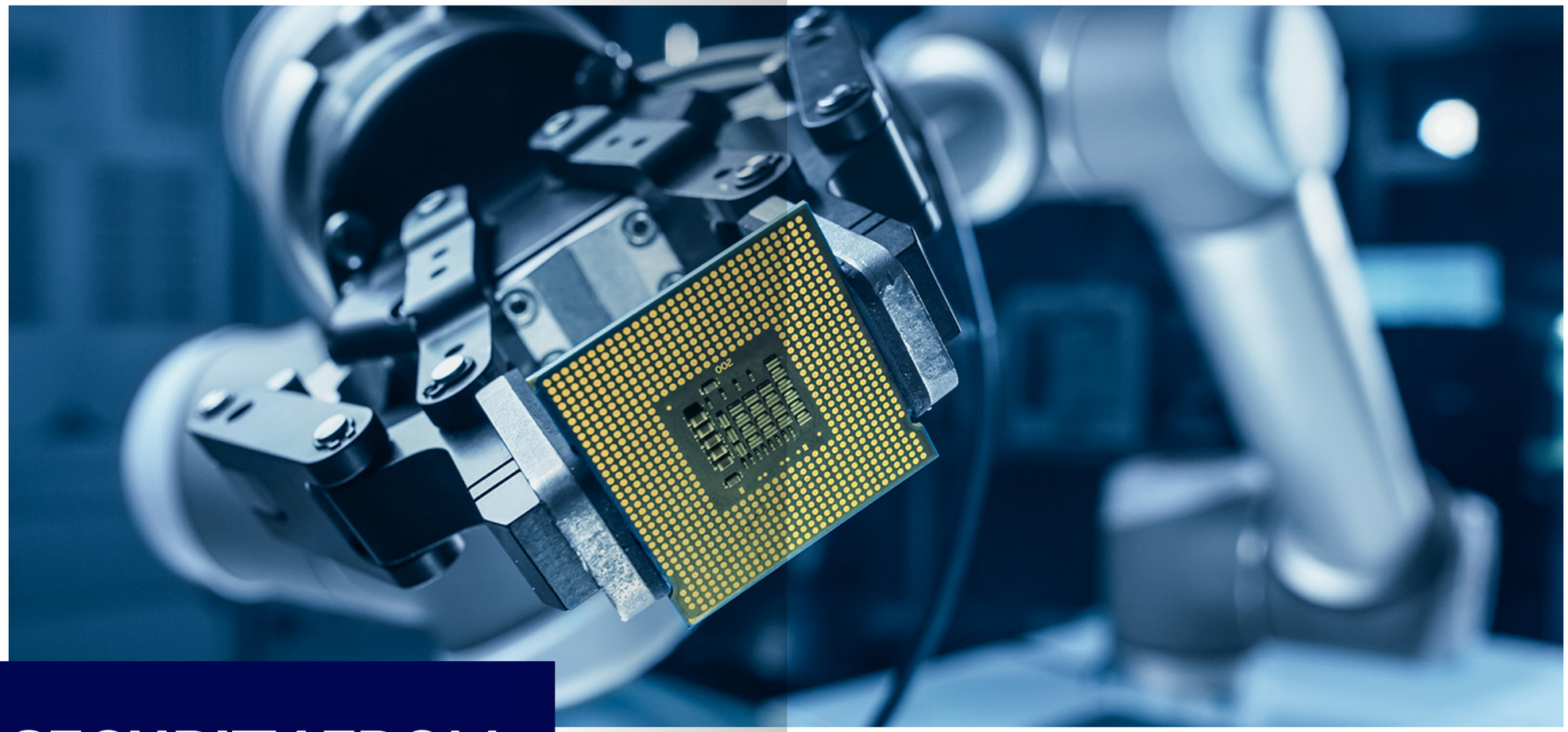
This booklet from the Centre for the Protection of Natural Infrastructure (CPNI) and National Cyber Security Centre (NCSC) sets out simple guidance for innovative start-ups and growing businesses, helping them to embed strong security practices and ensure that they collaborate with other organisations 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 YOU GROW



SECURITY FROM THE START

This guidance is intended for founders and leaders of startups in the emerging technology sector

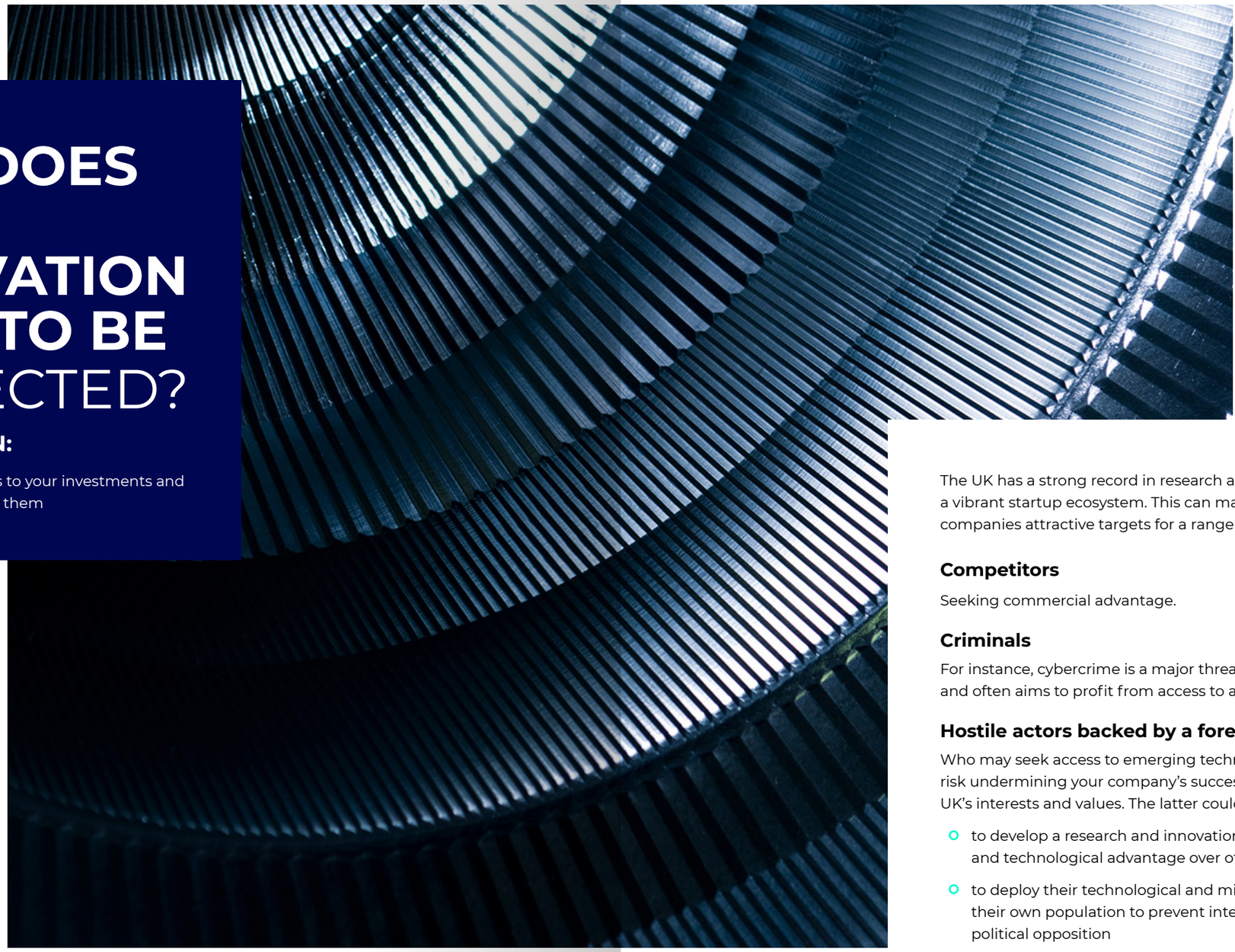
Good security practices can protect your competitive advantage, making your company more attractive to investors and customers. Laying strong foundations from the start will help your security to be more effective and less costly as your business grows.

This booklet outlines cost-effective measures that you can take from day one to better protect your ideas, reputation, and future success.

WHY DOES YOUR INNOVATION NEED TO BE PROTECTED?

IN THIS SECTION:

- Recognising the 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.

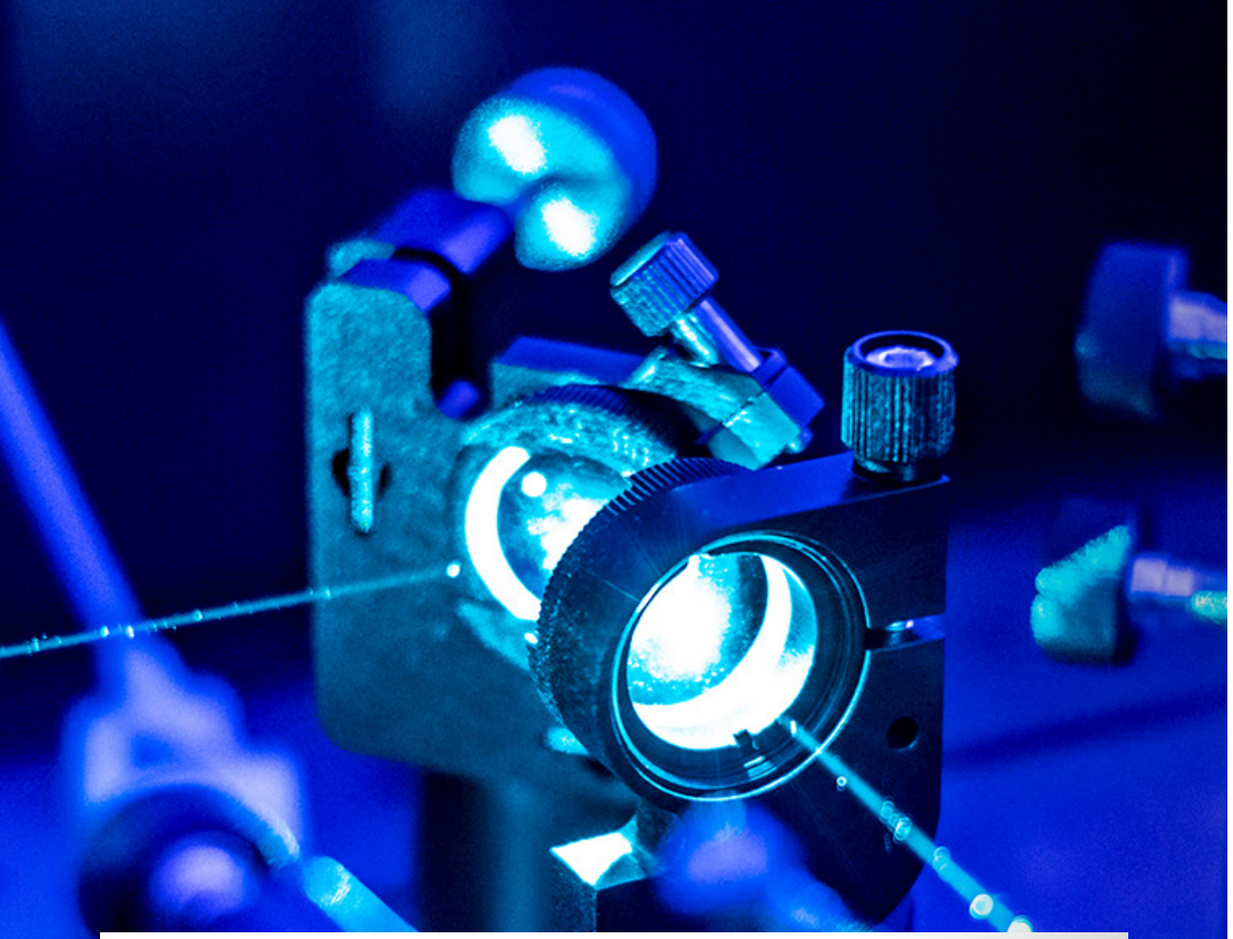
Criminals

For instance, cybercrime is a major threat to businesses of any size and often aims to profit from access to any vulnerable network.

Hostile actors backed by a foreign state

Who may seek access to emerging technology for reasons that risk undermining your 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



01
CASE STUDY

In December 2020, the Netherlands expelled two alleged Russian intelligence officers for espionage against the Dutch high-tech sector. The officers had reportedly built a network of individuals with experience in the Dutch science and technology sector. The technologies in which these officers were reportedly most interested have military as well as civilian applications.

The Dutch Interior Minister said that the actions taken by the alleged Russian intelligence officers had “likely caused damage to the organisations where the sources are or were active and thus possibly also to the Dutch economy and national security.”

BBC, ‘Netherlands expels two Russians after uncovering ‘espionage network’’, 10/12/2020

LEAD BY EXAMPLE

IN THIS SECTION:

- Lead from the top by identifying a security lead at Board level
- Develop a positive security culture through ongoing dialogue

The startup phase is the perfect time to set the tone for your future security culture. Identifying someone at Board level who is responsible for security will ensure that it is factored into your business decisions from the start.

Ongoing conversations about security are vital to developing a positive security culture in which any security incidents are openly discussed. They will help develop a common understanding of what your most valuable assets are and what your risk tolerance is, as well as individuals' security responsibilities.

PROTECT YOUR VALUE

IN THIS SECTION:

- Identify your most valuable assets which are critical to the existence and success of your business
- Assess security risks and mitigations in conjunction with other risks to your business
- Apply for the appropriate intellectual property (IP) protections for the jurisdictions in which you wish to operate

YOUR ASSETS ARE WIDE RANGING

They can include your people, premises, products and services, as well as the information, IP, and knowledge you hold. Identifying which of these assets is critical to your existence is an ideal starting point for your security planning.

Strong security is central to allowing your business to thrive, so security risks should be assessed and managed alongside any other risks to your business. Understanding the following will help you to determine which risks to prioritise:

- **YOUR ORGANISATION'S** GOALS AND PRIORITIES
- **YOUR MOST** CRITICAL ASSETS
- **THE THREATS TO THOSE** CRITICAL ASSETS
- **THE LIKELIHOOD AND CONSEQUENCES OF A** THREAT AFFECTING YOU

PUT IN PLACE MITIGATIONS TO REDUCE RISK TO ACCEPTABLE LEVELS AND KEEP UNDER REVIEW

If used well, IP can offer a solid platform for any business to grow. The way that you plan, manage and protect your ideas should be a crucial aspect of your business planning. You should apply for the appropriate IP protections for the jurisdictions in which you wish to operate. You could invest time and money in your business, only to later find the IP already belongs to someone else.

Having the right legal protections for your IP in place does not mean it is no longer at risk. It is still important to continuously review who has access to your most sensitive information and how you ensure it remains secret.

02
CASE STUDY

It was reported in August 2020 that criminals had attempted to pay a Tesla employee to install malware at one of the company's factories. The malware would reportedly 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 and can be used to facilitate cyber-attacks. This incident demonstrates the interconnected and reinforcing nature of personnel, physical, and cyber security. Integrating all three is essential to effective mitigation measures.

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

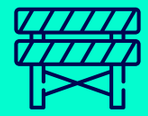
BUILD SECURITY INTO YOUR ENVIRONMENT

IN THIS SECTION:

- Control access to your information and most valuable assets, with measures to detect unauthorised access
- Build in basic security when setting up your IT

Any security decisions you make will be strengthened by considering people, information, physical and cyber risks together. Securely configured IT may still be at risk if left in an unlocked room. Equally, physical barriers such as safes and locks are pointless if you are not checking the credibility and trustworthiness of the people you give access to.

CENTRE SECURITY AROUND YOUR MOST CRITICAL ASSETS



Place barriers (physical or virtual) **around each critical asset you have identified as needing protection.**

Restrict access to the asset to only those people who need it and are trusted to use it securely by using things like swipe card access and restricting administration rights.

Take regular, ideally automated, **backups of critical data** and keep them physically and logically separate from the main system. This will allow your business to function following the impact of physical damage, theft or ransomware attacks.

BUILD IN BASIC SECURITY WHEN SETTING UP YOUR IT

Insecure IT can provide an easy way for your business to be exploited. The following minimal steps can reduce the likelihood and impact of your systems being breached.

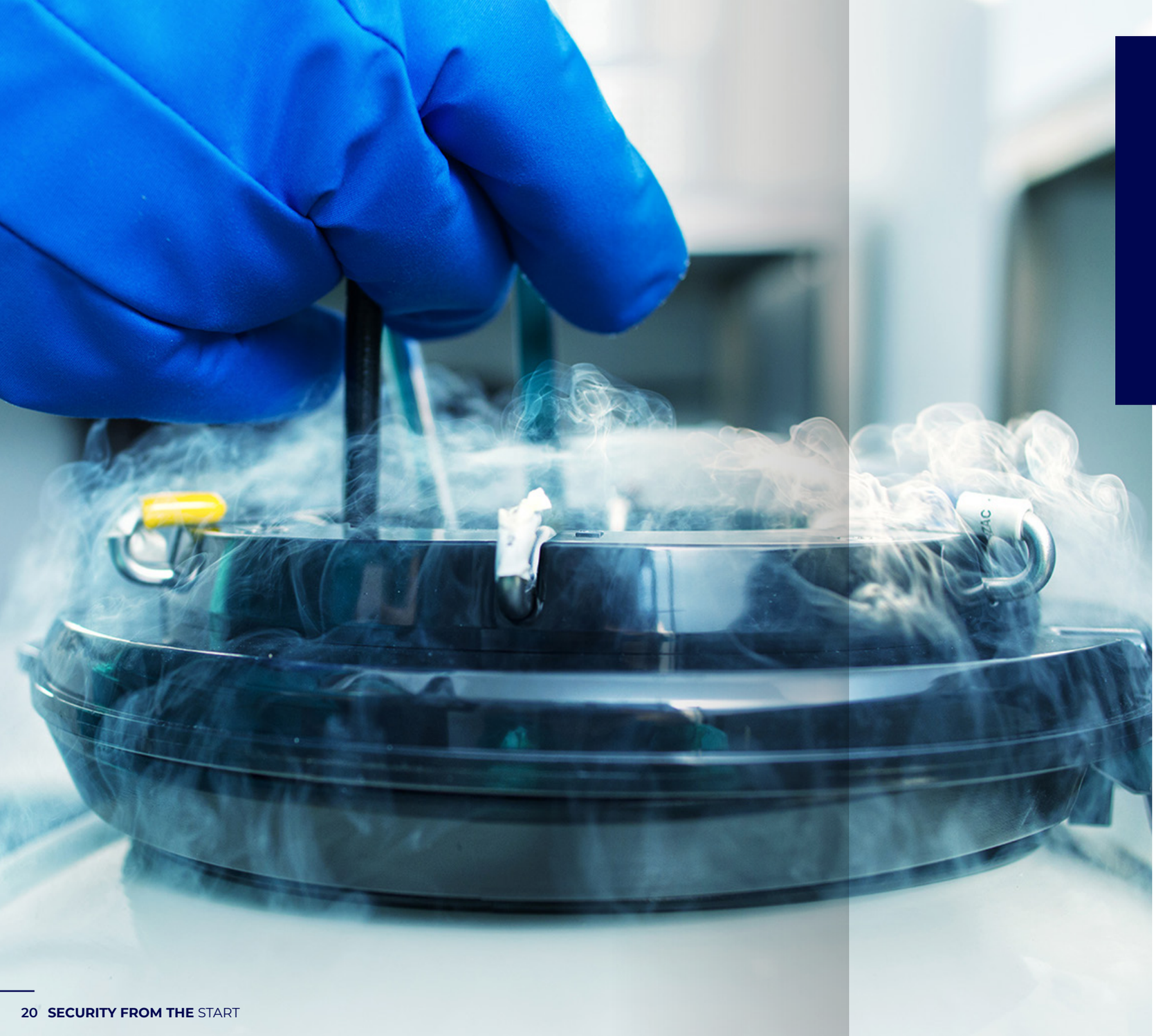
Enable both your firewall and antivirus.

Use strong password protection and, where available, encryption on your devices and accounts. This means changing all default passwords, using unpredictable passwords and two-factor authentication for 'important' accounts.

Keep devices and software up to date with the latest versions from providers. These updates will add new features and patch any security vulnerabilities that have been discovered.

Consider the trustworthiness of your internet connection. If you are using an internet connection as part of shared office space, identify the boundary of networks you control and can trust and implement appropriate and proportionate measures, such as firewalls. Consider using a Virtual Private Network (VPN) if you routinely access the internet over untrusted infrastructure (including public Wi-Fi connections).

Enable tools to track, lock or wipe lost or stolen mobile devices.



SECURE YOUR SUPPLY CHAIN

IN THIS SECTION:

- Assess the risks associated with any product or service you buy
- Seek suppliers whose security posture and assurance best meets your requirements
- Meet your own security requirements as a supplier

Implementing effective supply chain security from the start can save you time when your supply chains are longer and more complex.

Cloud service providers can supply scalable services, removing the need for small organisations to invest in hardware and specialist expertise that they might struggle to justify in terms of cost.

When using cloud services, it is essential to select a provider who prioritises security attributes most relevant to your needs (e.g., confidentiality or availability). You should also consider any legal or regulatory implications (e.g., General Data Protection Regulation).

1. **Understand the risks**, including what needs protection and why; what your suppliers' security looks like; and any risks you may be exposed to as part of your supply chain.
2. **Seek suppliers** whose security offer and level of assurance best matches your requirements.
3. Consider building **diversity** and **resilience** into your supply chain if you identified overreliance on any one supplier.

SECURITY AS YOU GROW

This guidance is intended for founders and leaders of startups and scaleups in the emerging technology sector. It suggests ways to build upon the guidance in part one of Secure Innovation as your company and innovation matures.

As your company continues to evolve, so too should your security measures. The risks you face may well have changed, for example because your team has grown, you have moved to more or larger premises, you are collaborating with more partners, or because you are looking for investment.

It is worth regularly reviewing your security measures to consider whether you need additional precautions.

COLLABORATE WITH SECURITY **IN** MIND

IN THIS SECTION:

- Limit the data you share with your partners and ensure they can handle sensitive data securely
- Where possible, keep sensitive systems independent of those accessible by external parties
- Where proportionate, put in place confidentiality and non-disclosure agreements (NDAs) with those who have access to your innovation

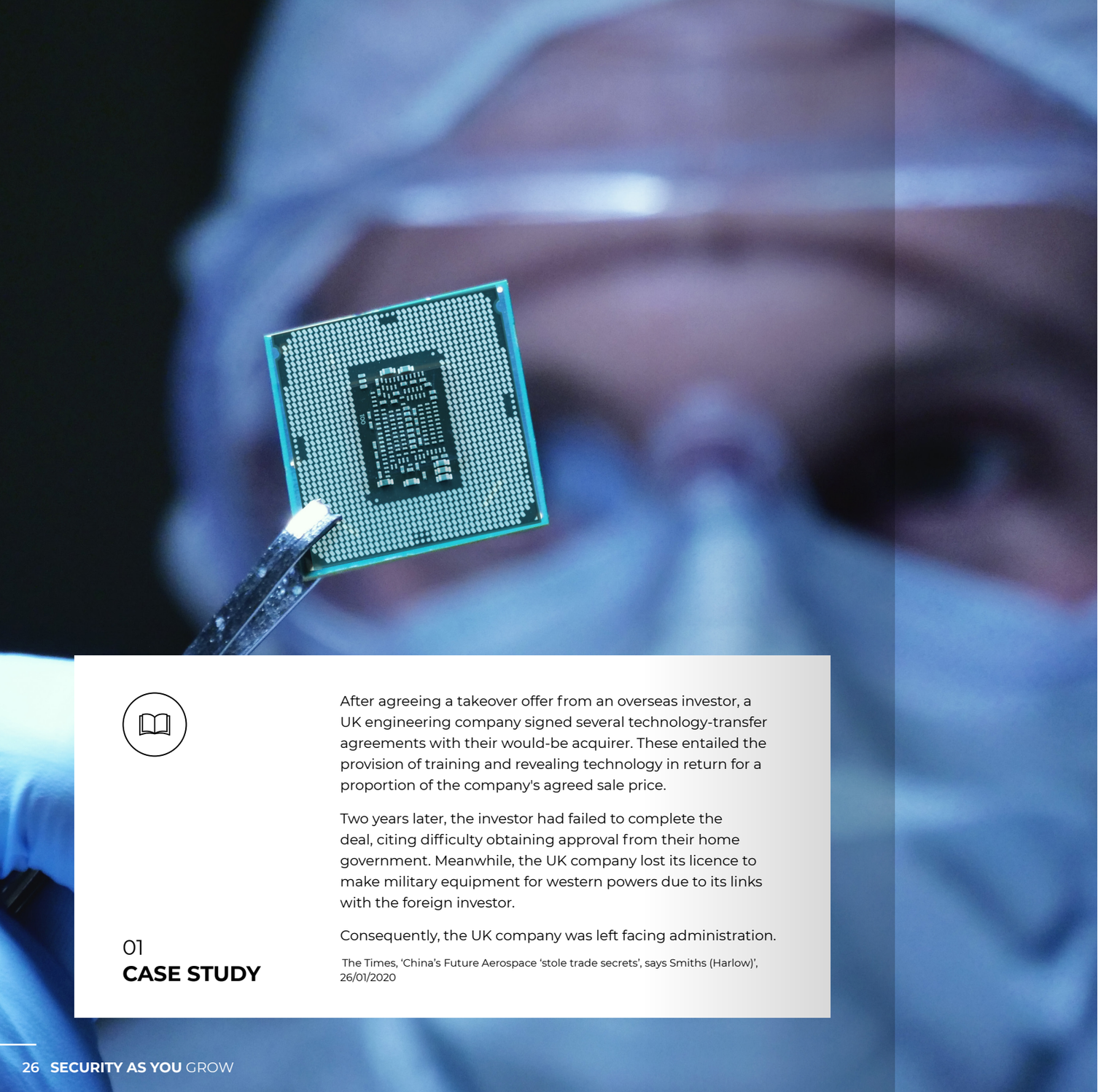
Collaboration increases the number of external routes into your organisation, or to any information or data you may share. You may be targeted to reach the organisation you are supplying, or your suppliers may be targeted to reach you.

You can manage the increased risk by determining what data is appropriate to share and implementing measures to limit access to just that data, keeping sensitive systems independent from those accessible to the wider organisation and any external parties, and taking steps to ensure that your partner is handling any sensitive data appropriately and securely.

A good NDA restricts the use of your ideas and information to a specific permitted purpose. Like legal IP protections, NDAs are another tool you can use, but they do not replace good protective security measures.

As you collaborate more it may be useful to demonstrate your commitment to cyber security. The Cyber Essentials scheme is a good first step: it shows that you have the technologies and policies in place to guard against common cyber-attacks.

It is also worth considering that your early choice of partners - whether they be investors, customers or suppliers - may have an impact upon who is willing to do business with you later.



01
CASE STUDY

After agreeing a takeover offer from an overseas investor, a UK engineering company signed several technology-transfer agreements with their would-be acquirer. These entailed the provision of training and revealing technology in return for a proportion of the company's agreed sale price.

Two years later, the investor had failed to complete the deal, citing difficulty obtaining approval from their home government. Meanwhile, the UK company lost its licence to make military equipment for western powers due to its links with the foreign investor.

Consequently, the UK company was left facing administration.

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

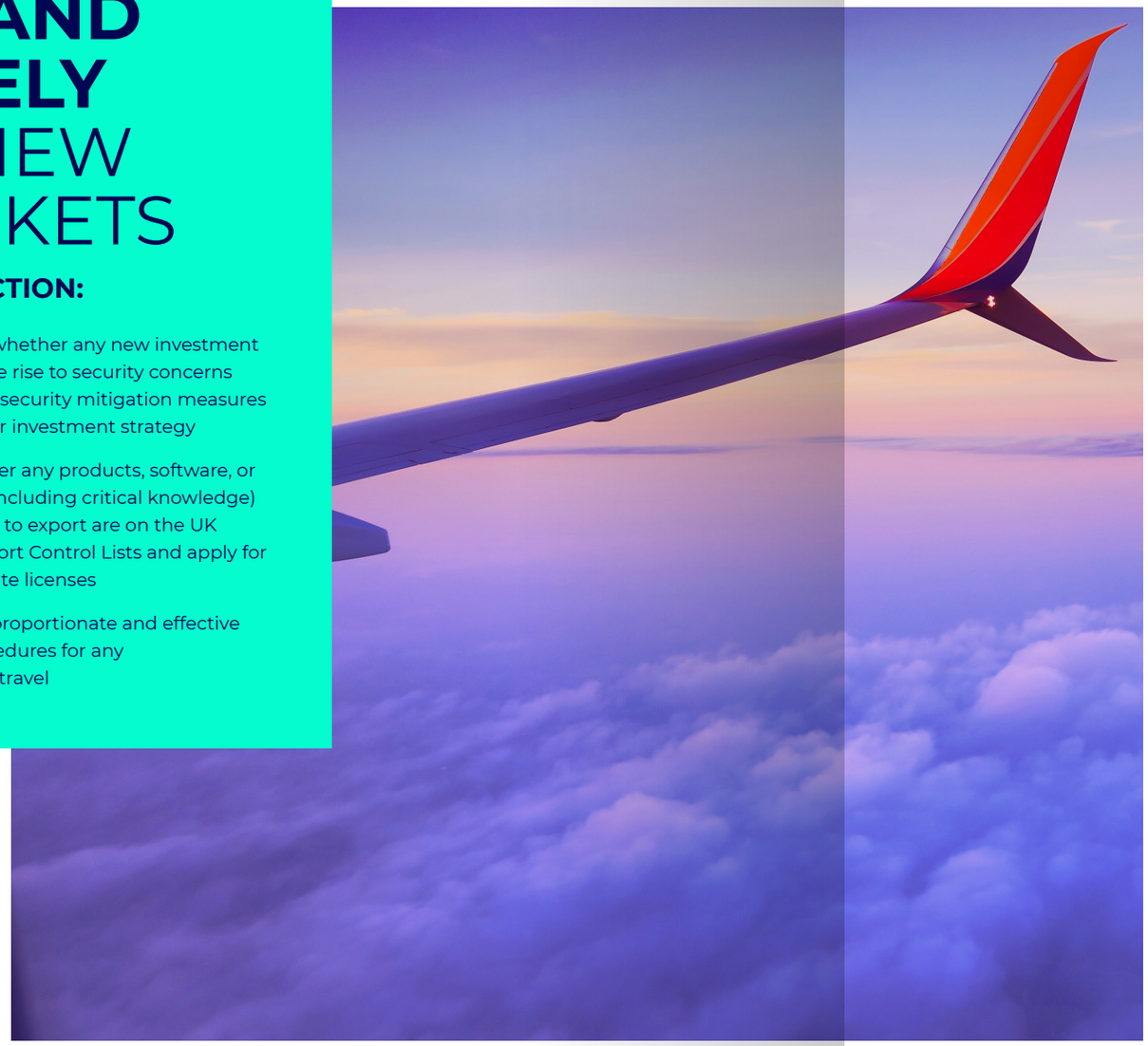
THE NSI ACT

The UK has introduced new legislation - the National Security and Investment (NSI) Act - to give businesses and investors the certainty and transparency they need to do business in the UK while protecting national security. The Act will provide the Government with powers to screen investments and address any national security risks identified. It is needed because, in a minority of cases, investment can result in damage to the interests of your company or the national security of the UK.

EXPAND SAFELY TO NEW MARKETS

IN THIS SECTION:

- Understand whether any new investment is likely to give rise to security concerns and consider security mitigation measures as part of your investment strategy
- Check whether any products, software, or technology (including critical knowledge) that you wish to export are on the UK Strategic Export Control Lists and apply for the appropriate licenses
- Put in place proportionate and effective security procedures for any international travel



In a minority of cases, investment can be used to gain access to, and influence over, your company. An early risk assessment of any investments will allow you to be better prepared for negotiations and any scrutiny under NSI. Understanding the risks may allow you to implement mitigating measures, such as modifying the terms of the deal.

THINGS TO CONSIDER AS A PART OF DUE DILIGENCE ON ANY PROPOSED INVESTORS

- The investor's reputation and trustworthiness
- The source of their funds
- Whether they have unexpected commercial, political or military ties, or links to state repression which may have ethical implications
- Whether they are on the entity listing of other countries, particularly those you are, or may consider, doing business with
- Any implications of the legal regime they are subject to

Some regimes can compel overseas partners to release information or cooperate with their state.

When exporting into new markets you will need to be aware of the UK Strategic Export Control Lists. These form the basis of determining whether any products, software, or technology (including intangible transfers of critical and technical knowledge) that you intend to export are 'controlled' and therefore require an export license.

There may also be a need for you or your employees to travel internationally as you grow.

We recommend considering whether travel is likely to introduce additional risks and, if so, taking appropriate steps to mitigate them. This includes protecting any electronic devices taken overseas, removing any non-essential data, and knowing what to share, trade, and protect.

TRUST YOUR TALENT

IN THIS SECTION:

- Maintain your positive security culture through strong communication
- Establish a security training package for staff, including at point of induction
- Identify any roles that are exposed to higher risks and provide those individuals with additional support
- Put in place a pre-employment screening process for all recruits into your business

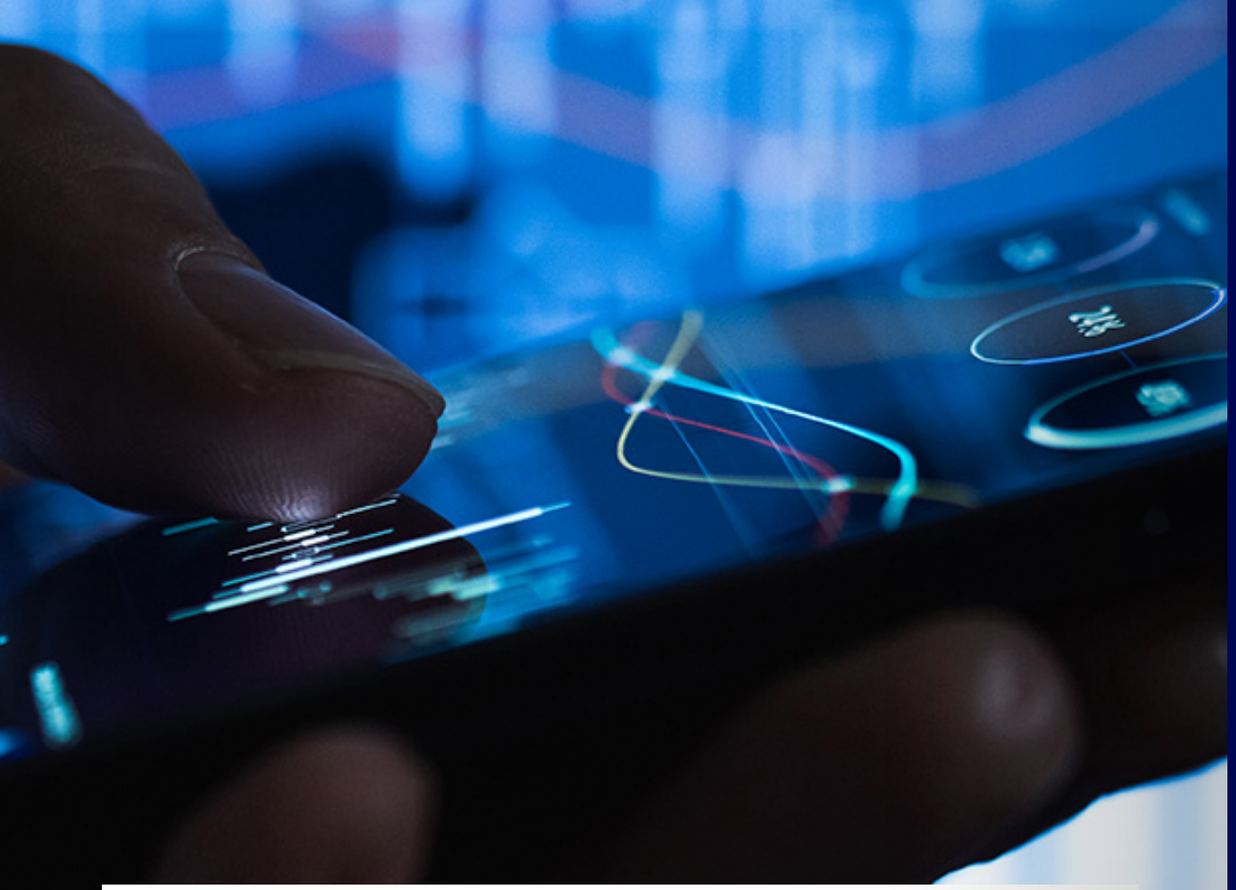
As your workforce grows, you may no longer be able to rely primarily on personal relationships to ensure trust. Fostering a positive security culture is even more important.

Consistency and communication are vital to creating an environment in which people are confident that they can speak openly. This means making it easy and routine to report any concerns, handling those concerns sensitively and without apportioning blame, and keeping those involved informed of both the progress and benefits of any resulting actions to reinforce confidence in reporting.

Providing ongoing security training, including at the point of induction, for your whole team will also help to maintain your security culture. Effective education and training help individuals to understand what policies, standards and procedures are in place to maintain security.

A role-based security risk assessment will help you to keep your security measures proportionate and effective. As a startup, you have already assessed the risks to your business based on the likelihood and consequence of threats to your critical assets. This should provide you with a foundation for assessing which roles have a higher risk exposure, and so require more comprehensive employment checks.

As you recruit more employees it is essential that you conduct screening of potential candidates who wish to be part of your business and have access to your critical assets. A suitable level of screening, informed by a role-based risk assessment, should be applied to all individuals who are provided access. This includes permanent, temporary and contract workers.



02
CASE STUDY

In 2011, a Chinese wind turbine maker was convicted of stealing trade secrets from a US semiconductor company, causing the company to lose more than $1 billion in shareholder equity and almost 700 jobs. The Chinese company recruited an employee of the US company to secretly copy information, including the source code for its wind turbine control system.

The integrity of your people is a major contributor to your success. Employment screening will provide you with a snapshot risk assessment of an individual – your personnel security practices need to be maintained with ongoing conversations, security training and monitoring.

Reuters, 'China's Sinovel convicted in the U.S. of trade-secret theft', 24/01/2018
https://www.reuters.com/article/us-sinovel-wind-gro-usa-court-idUSKBN1FD2XL

YOUR PRE-EMPLOYMENT SCREENING CHECKS COULD INCLUDE:

- CONFIRMATION OF IDENTITY
- NATIONALITY AND IMMIGRATION STATUS
- EMPLOYMENT AND EDUCATION HISTORY
- FINANCIAL RECORDS CHECK
- CRIMINAL RECORDS CHECK
- RIGHT TO WORK
- PERSONAL REFERENCES
- OPEN SOURCES AND MEDIA ENVIRONMENT
- NATIONAL SECURITY VETTING (FOR ACCESS TO GOVERNMENT CLASSIFIED MATERIAL)

PREPARE FOR SECURITY INCIDENTS

IN THIS SECTION:

- Establish and test an Incident Management plan
- Monitor your staff and IT to detect unexpected behaviour

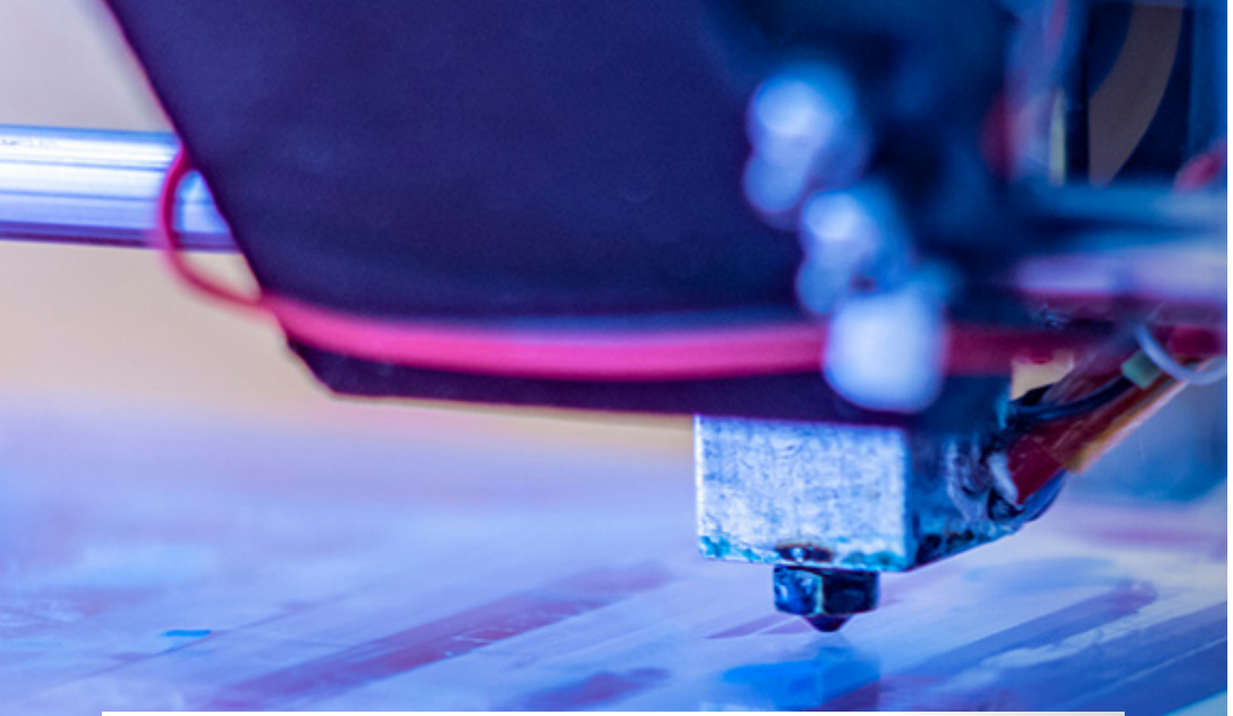
The damage caused by a breach can be reduced through a well-planned and executed response. It is worth assuming that your business will be breached and planning accordingly.

INCIDENT MANAGMENT

A basic incident management plan should include contact details for anyone you would need to help you identify an incident (such as your web hosting provider, IT support services or insurance company), clearly defined responsibilities and an escalation process for critical decisions, a coordination function to track and document findings and actions, and a mechanism to learn from previous incidents. It is also worth understanding your obligations to report certain incidents to the Information Commissioner's Office or any relevant regulatory bodies.

Maintaining an understanding of your IT's behaviour is central to your ability to spot anomalies, which may reveal security incidents. As elsewhere, understanding the risks you are most concerned about will enable you to focus your monitoring to collect information relevant to your needs.

The same is true of your staff. Understanding the causes of any uncharacteristic behaviour, such as conflicts at work, change of work patterns, or decline in performance, can help to prevent as well as detect an increased insider risk. A supportive response can help to improve your team's relationship with the company, and thereby security.



An employee of a US agrochemical and biotechnology company was alleged to have maintained contact with officials within the Chinese government about potential jobs for two years. The employee travelled to China for job interviews and to discuss his knowledge and skills. In doing so, he implied that he could duplicate his employer's IP.

After resigning from his job, the employee allegedly copied and downloaded the company's IP to a memory card and bought a one-way plane ticket to China. Before he could board his flight, the employee was intercepted by law enforcement officials who seized copies of the stolen IP.

Strong security monitoring could have flagged this employee's alleged actions. This includes being aware of employee travel, IT behaviours, and physical accesses and actions such as the use of memory cards or excessive printing. This example also highlights the mutually reinforcing nature of the various components of protective security.

Reuters, 'U.S. charges Chinese national with stealing trade secrets – Justice Dept', 22/11/2019 *https://www.reuters.com/article/usa-china-espionage-idINKBN1XW06J*

03
CASE STUDY

Further Information

Please see the following websites for more information.

www.CPNI.gov.uk

www.NCSC.gov.uk

Guidance

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

Secure development and deployment: ***www.ncsc.gov.uk/collection/developers-collection***

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

Cloud security: ***www.ncsc.gov.uk/collection/cloud-security***

Virtual private networks: ***www.ncsc.gov.uk/collection/mobile-device-guidance/virtual-private-networks***

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

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

Holistic Management of Employee Risk: ***www.cpni.gov.uk/system/files/documents/62/53/Holistic-Management-of-Employee-Risk-HoMER-Guidance.pdf***

Insider Risk Assessment guidance: ***www.cpni.gov.uk/system/files/documents/46/06/Personnel-security-risk-assessment-a-guide-4th-edition.pdf***

Security Messages for New Joiners: ***www.cpni.gov.uk/security-messages-new-joiners***

Training on basic cyber security: ***www.ncsc.gov.uk/training/StaySafeOnline_web/index.html#***

Phishing: ***www.ncsc.gov.uk/files/Phishing-attacks-dealing-suspicious-emails-infographic.pdf***

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

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

Incident response and recovery: ***www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery***

Other resources

Logging made easy: ***https://www.ncsc.gov.uk/information/logging-made-easy***

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

Intellectual Property Office online training tools: ***www.ipo.gov.uk/ip-support***

The British Library Business and IP Centre: ***www.bl.uk/business-and-ip-centre#***

The British Business Bank: ***www.british-business-bank.co.uk/***

Department for International Trade: ***www.gov.uk/government/organisations/department-for-international-trade/about-our-services***

UK overseas intellectual property attaché network: ***www.gov.uk/government/publications/uk-overseas-intellectual-property-attache-network***

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***

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 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.