National Protective Security Authority

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 showed 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.

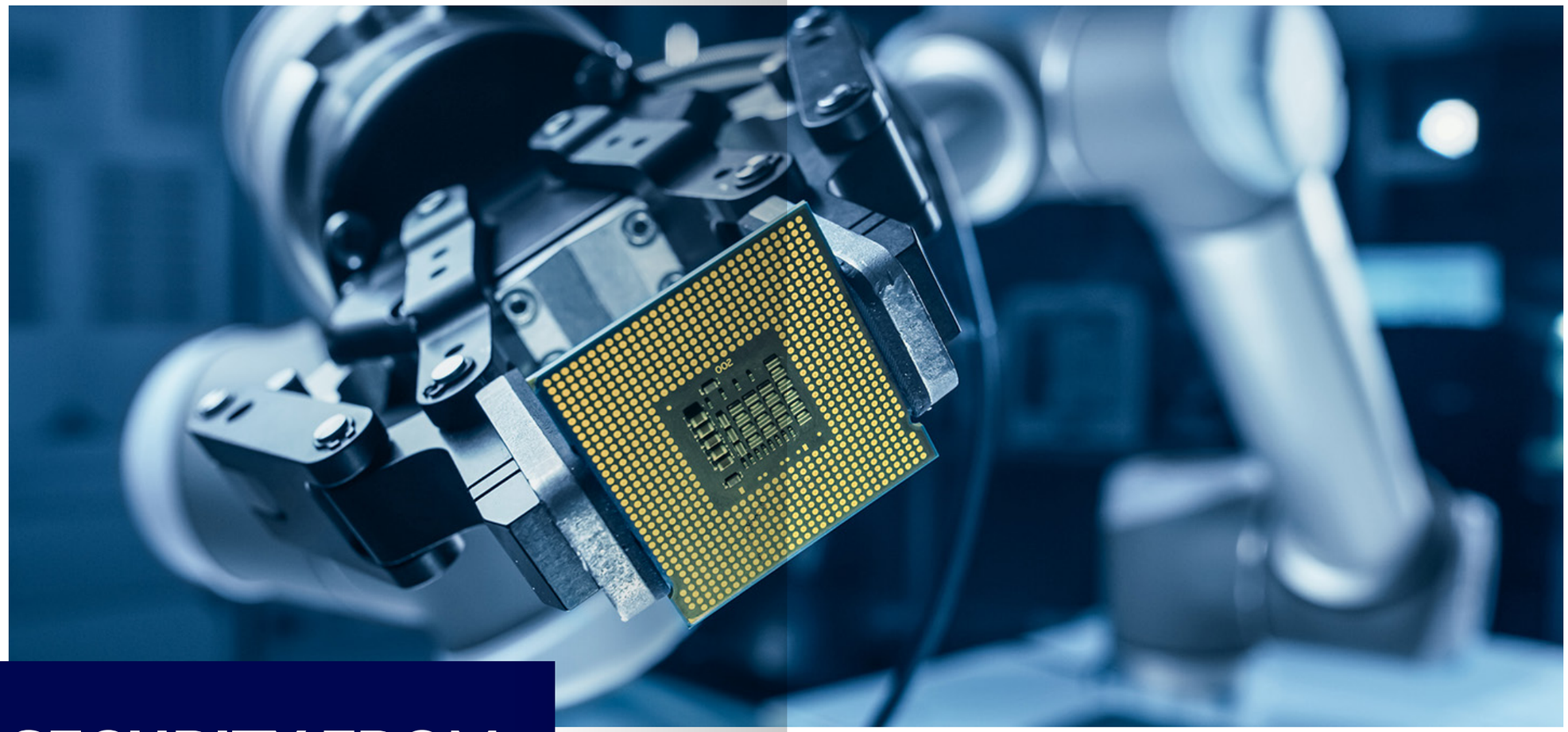
Due to the strength of this vibrant technology ecosystem, UK businesses have been a target for a range of actors who would seek to gain commercial, technological or military advantage from the innovations these firms have made. Protecting physical and information assets are essential parts of managing 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 National Protective Security Authority (NPSA) 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, 2018-2023

CONTENTS



SECURITY FROM THE START

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

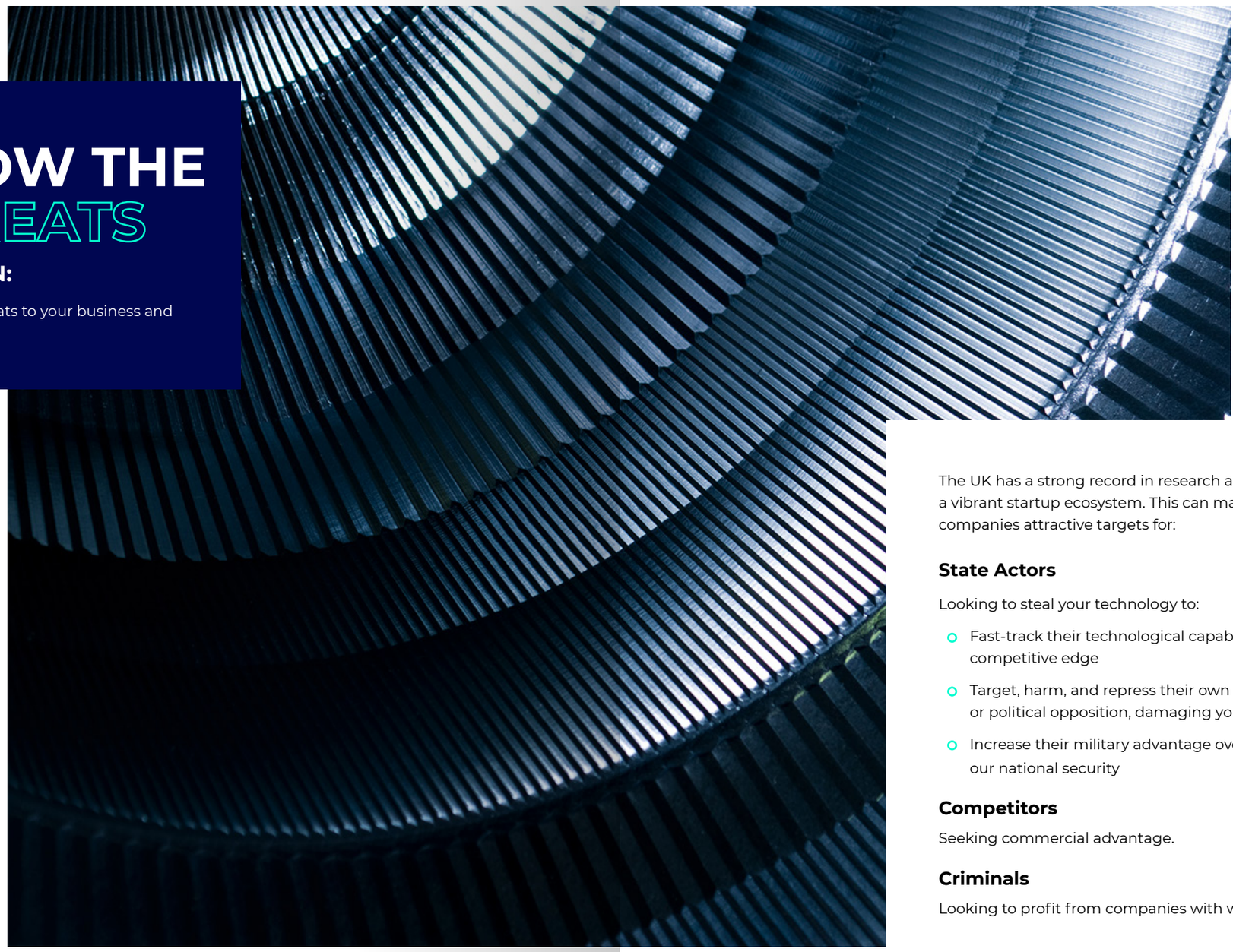
Good security practices can protect your competitive advantage, making your company more attractive to investors and customers. Laying strong foundations from the start will help your security to be more effective and less costly as your business grows.

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

1 KNOW THE THREATS

IN THIS SECTION:

- Understand the threats to your business and innovation



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 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

Competitors

Seeking commercial advantage.

Criminals

Looking to profit from companies with weak security.

2 SECURE YOUR ENVIRONMENT

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.”

01
CASE STUDY

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

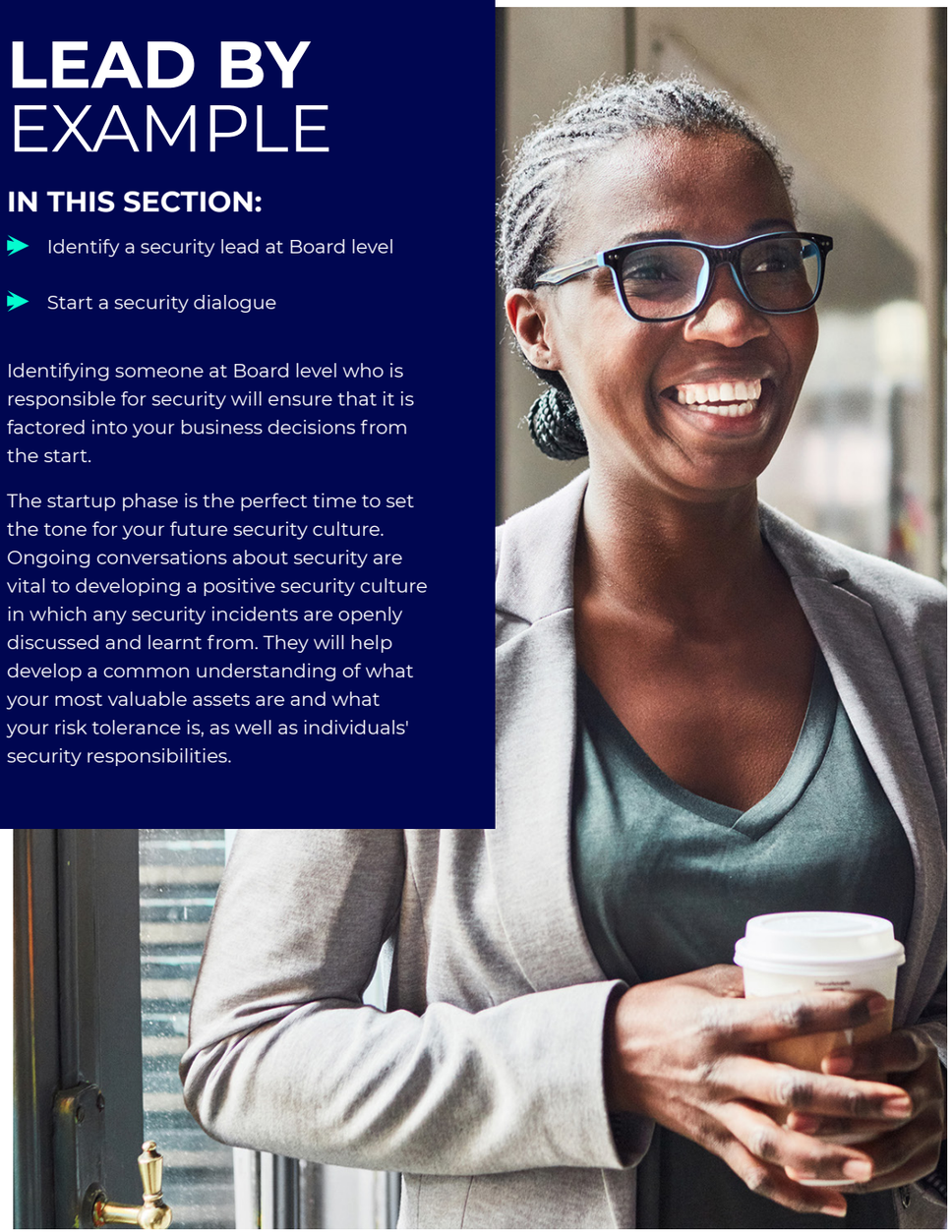
LEAD BY EXAMPLE

IN THIS SECTION:

- Identify a security lead at Board level
- Start a security dialogue

Identifying someone at Board level who is responsible for security will ensure that it is factored into your business decisions from the start.

The startup phase is the perfect time to set the tone for your future security culture. Ongoing conversations about security are vital to developing a positive security culture in which any security incidents are openly discussed and learnt from. 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.



UNDERSTAND THE RISKS

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

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

It is not possible to protect everything against every threat, especially for small companies with limited resources. However, security protections can cost less than expected, and will pay long term dividends. Security decisions should be prioritised, and based on a thorough understanding of what is most important to your survival and success.

Security will be more robust where it is based on a combination of information, physical, people and cyber security measures.

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

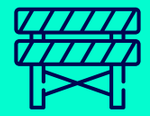
BUILD SECURITY INTO YOUR ENVIRONMENT

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 steps are the minimum cyber security any organisation should consider to reduce the likelihood and impact of your systems being breached.

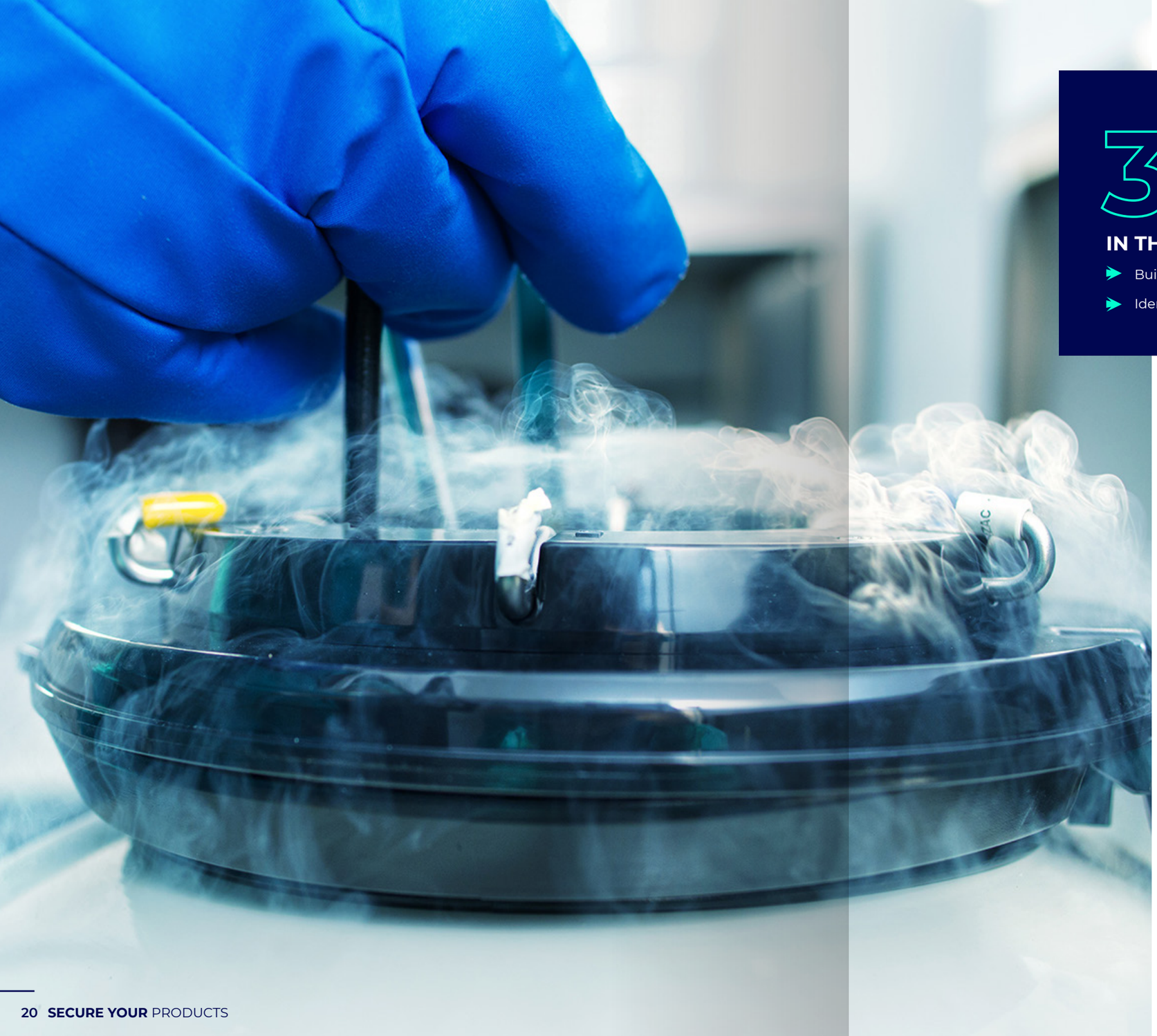
Enable both your firewall and antivirus.

Use strong password protection and, where available, encryption on your devices and accounts. This means changing all default passwords, using unpredictable passwords and multi-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.



3 SECURE YOUR PRODUCTS

IN THIS SECTION:

- Build security into your products from the beginning
- Identify and actively manage your IP

Technology startups should use Secure by Design and Secure by Default principles when designing products to ensure security problems are addressed at root cause. Ensuring that your products are free from security vulnerabilities is a key concern.

Intellectual Asset (IA) and Intellectual Property (IP) management strategies are essential for any business, and are integral with your business plans. Understanding the assets you have and what you want to do with them will help determine the actions required. You need to understand:

1. **What you need to protect**
2. **How you need to protect it**
3. **The in-country laws for the countries in which you are operating**
4. **How you are going to manage your IP**

4 SECURE YOUR PARTNERSHIPS

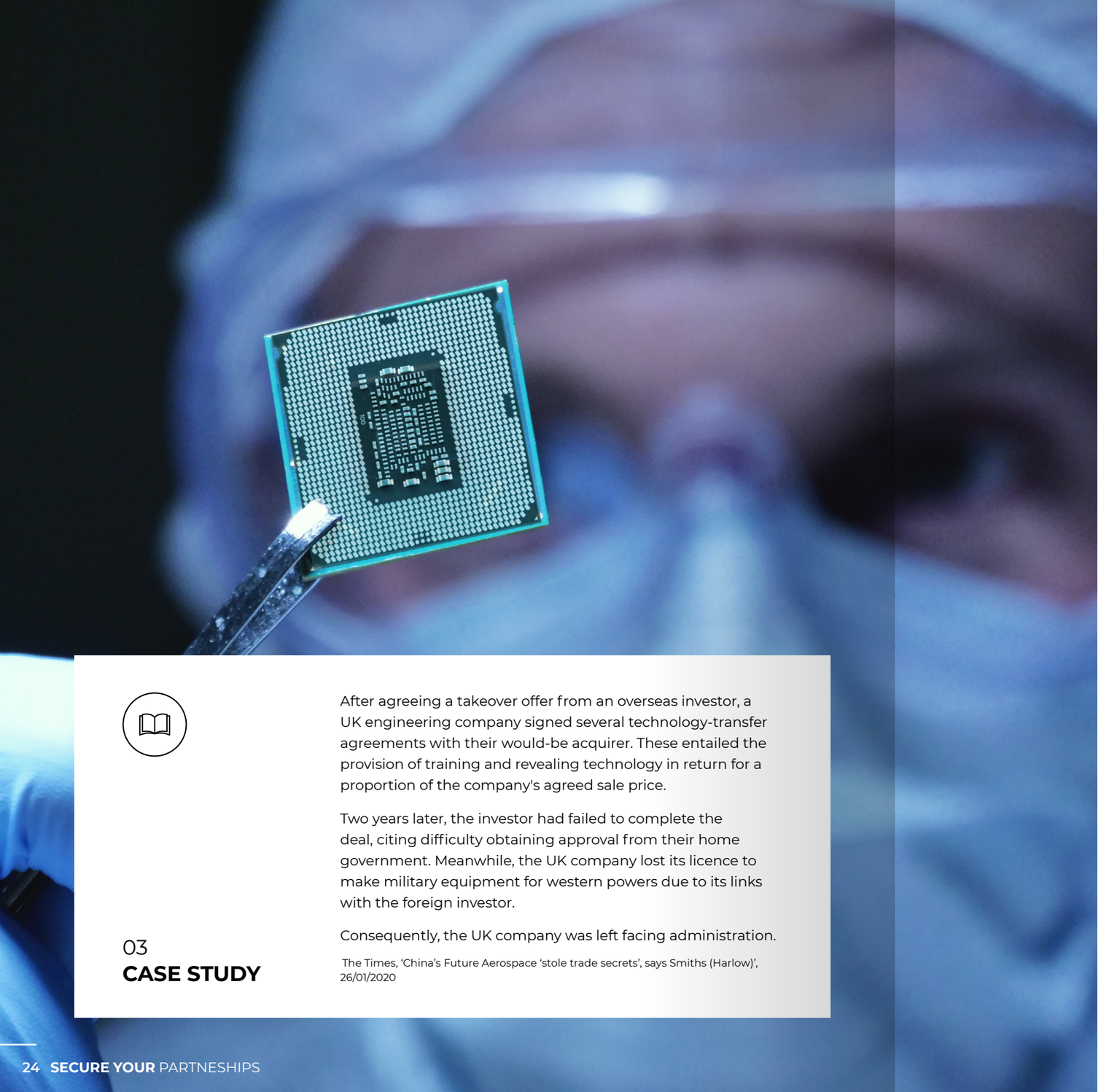
IN THIS SECTION:

- Manage collaboration risks with investors, suppliers, and other partners
- Consider security in your investment strategy

Partnerships increase the number of external routes into your organisation, or to any information or data you may share. To help your company grow safely, manage the additional risks that collaboration brings. Think about:

1. **WHY YOU ARE COLLABORATING**
   Think about the outcomes you need; the benefits a partner can bring; the risks and red lines.
2. **WHO YOU ARE WORKING WITH**
   Conduct due diligence on prospective investors, suppliers, and collaborators.
3. **WHAT YOU ARE SHARING**
   Be strategic about what and when you share with partners.
4. **HOW YOU ARE PROTECTING YOUR INNOVATION**
   Include protections for your assets and data in contracts.

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.



03
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 National Security and Investment (NSI) Act gives businesses and investors the certainty and transparency they need to do business in the UK while protecting national security. The Act provides 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.

5 SECURE YOUR GROWTH

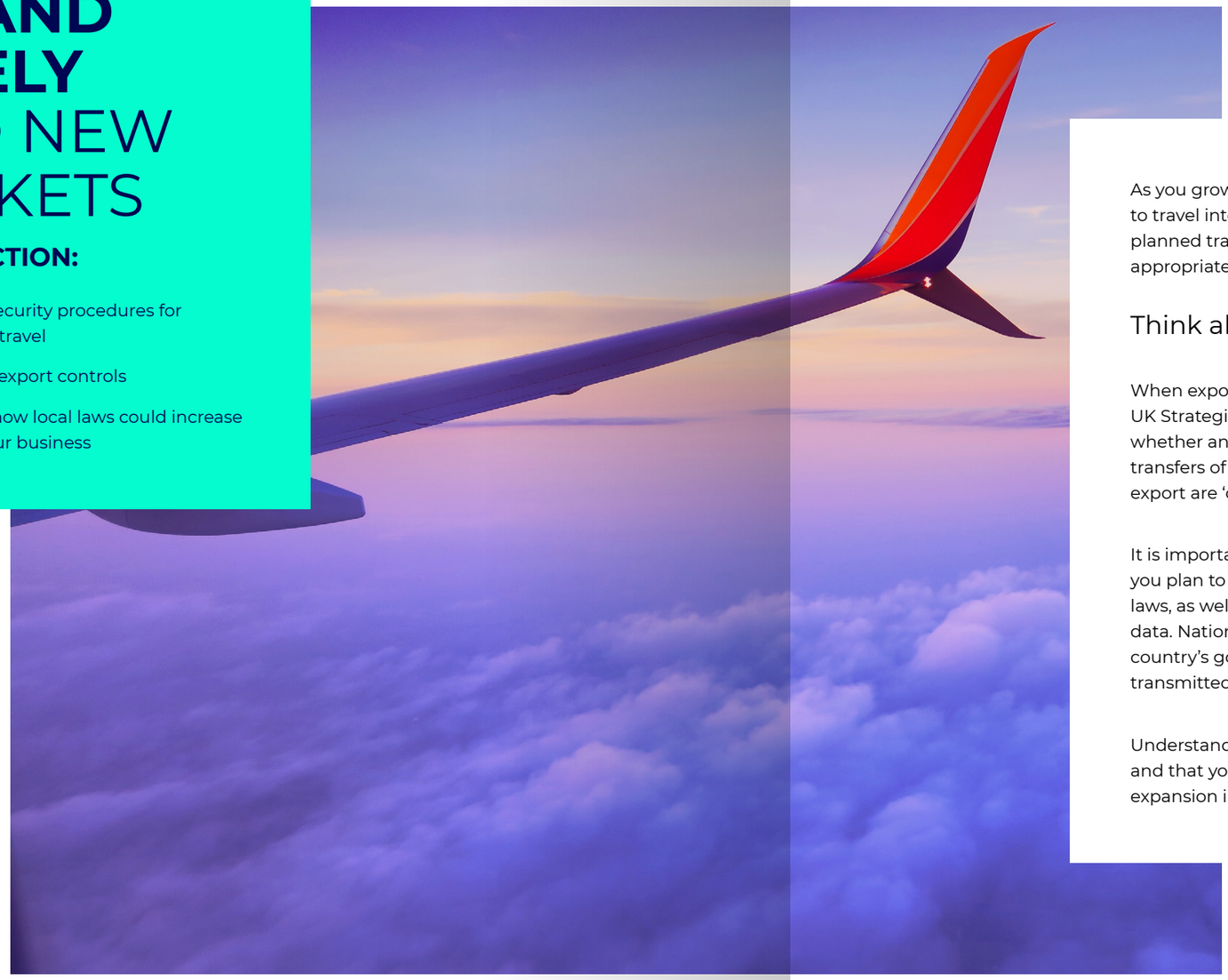
As your company continues to evolve, so too should your security measures. The risks you face may well have changed, for example because your team has grown, you have moved to more or larger premises, you are collaborating with more partners, or because you are looking for investment.

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

EXPAND SAFELY INTO NEW MARKETS

IN THIS SECTION:

- Implement security procedures for international travel
- Comply with export controls
- Understand how local laws could increase the risk to your business



As you grow, there may be more need for you and your employees to travel internationally. We recommend considering whether planned travel is likely to introduce additional risks and, if so, taking appropriate steps to mitigate them.

Think about what to share, trade, and protect.

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 licence.

It is important to understand the local laws in the countries where you plan to operate. Different countries have different export control laws, as well as laws regarding the handling and storage of 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.

Understanding local laws will ensure that you are legally compliant, and that you understand the additional security risks involved in expansion into new markets.

SECURITY FOR A GROWING TEAM

IN THIS SECTION:

- Maintain a positive security culture
- Deliver effective security education for your employees
- Provide additional support to staff in higher risk roles
- Implement a pre-employment screening process

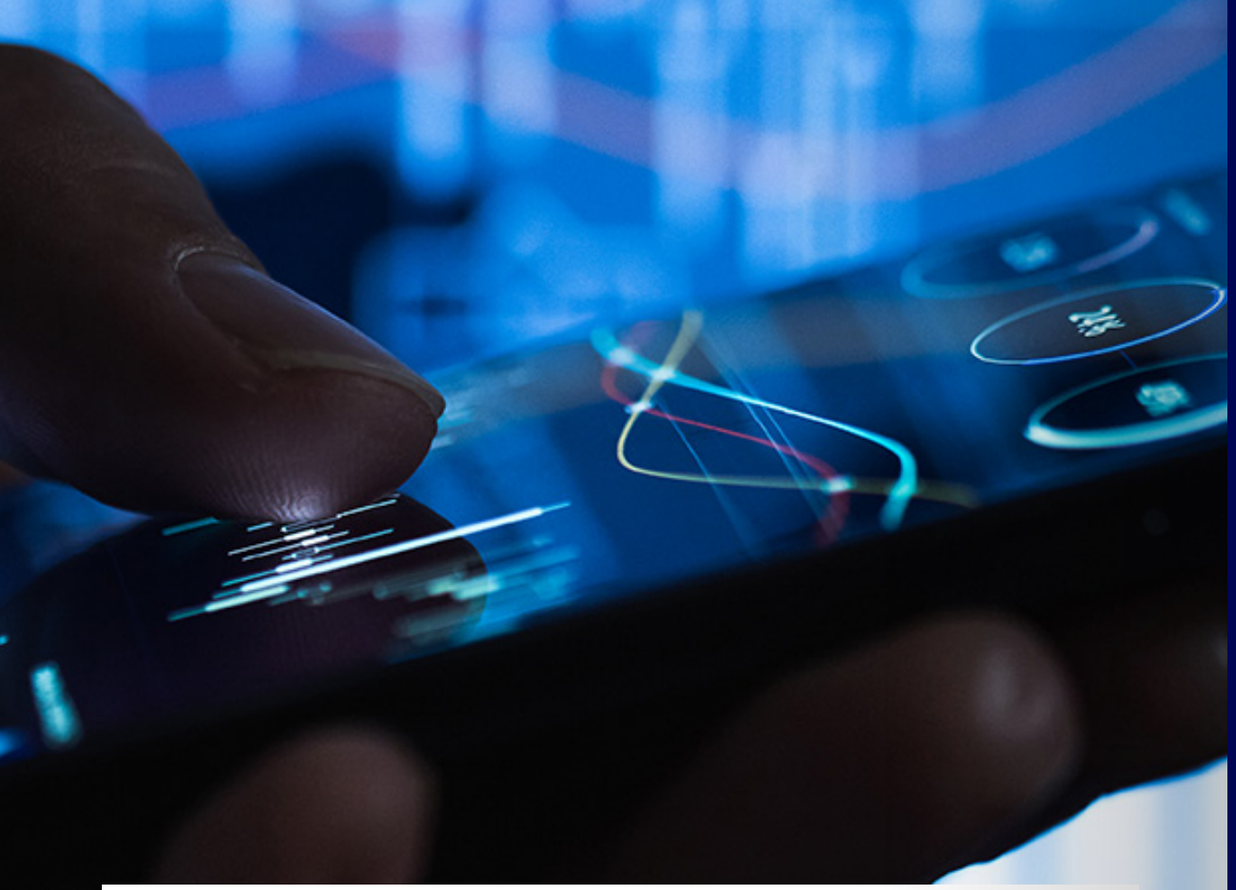
As your workforce grows, you may no longer be able to rely primarily on personal relationships to ensure trust. Fostering a positive security culture is even more important.

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.



04
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 employees' relationship with the company, building trust and the right attitude towards security in the workforce.

05
CASE STUDY

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

Further Information

Please see the following websites for more information.

www.NPSA.gov.uk

www.NCSC.gov.uk

SECURE YOUR ENVIRONMENT.

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

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

NPSA's risk assessment approach: **www.npsa.gov.uk/rmm/protective-security-risk-management**

Training on basic cyber security: **https://www.ncsc.gov.uk/cyberaware/home**

NCSC's Early Warning system: **https://www.earlywarning.service.ncsc.gov.uk**

NCSC's Check your cyber security service: **https://checkcybersecurity.service.ncsc.gov.uk**

NCSC's free personalised Cyber Action Plan: **https://www.ncsc.gov.uk/cyberaware/actionplan**

SECURE YOUR PRODUCTS.

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

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

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

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**

SECURE YOUR PARTNERSHIPS.

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

NPSA's Protected Procurement: **https://www.npsa.gov.uk/protected-procurement-practitioners**

NCSC's supply chain cyber security guidance: **https://www.ncsc.gov.uk/collection/assess-supply-chain-cyber-security**

SECURE YOUR GROWTH.

UK Strategic Export Control List: **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**

Department for Business and Trade: **www.gov.uk/government/organisations/department-for-business-and-trade/about-our-services**

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

NPSA's employment screening guidance: **https://www.npsa.gov.uk/employment-screening**

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

Holistic Management of Employee Risk: **www.npsa.gov.uk/resources/holistic-management-employee-risk-homer-guidance**

Insider Risk Assessment guidance: **www.npsa.gov.uk/resources/role-based-protective-security-risk-assessment**

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

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

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, NPSA 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.npsa.gov.uk. All references to NPSA 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 NPSA. This information is exempt from disclosure under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation.