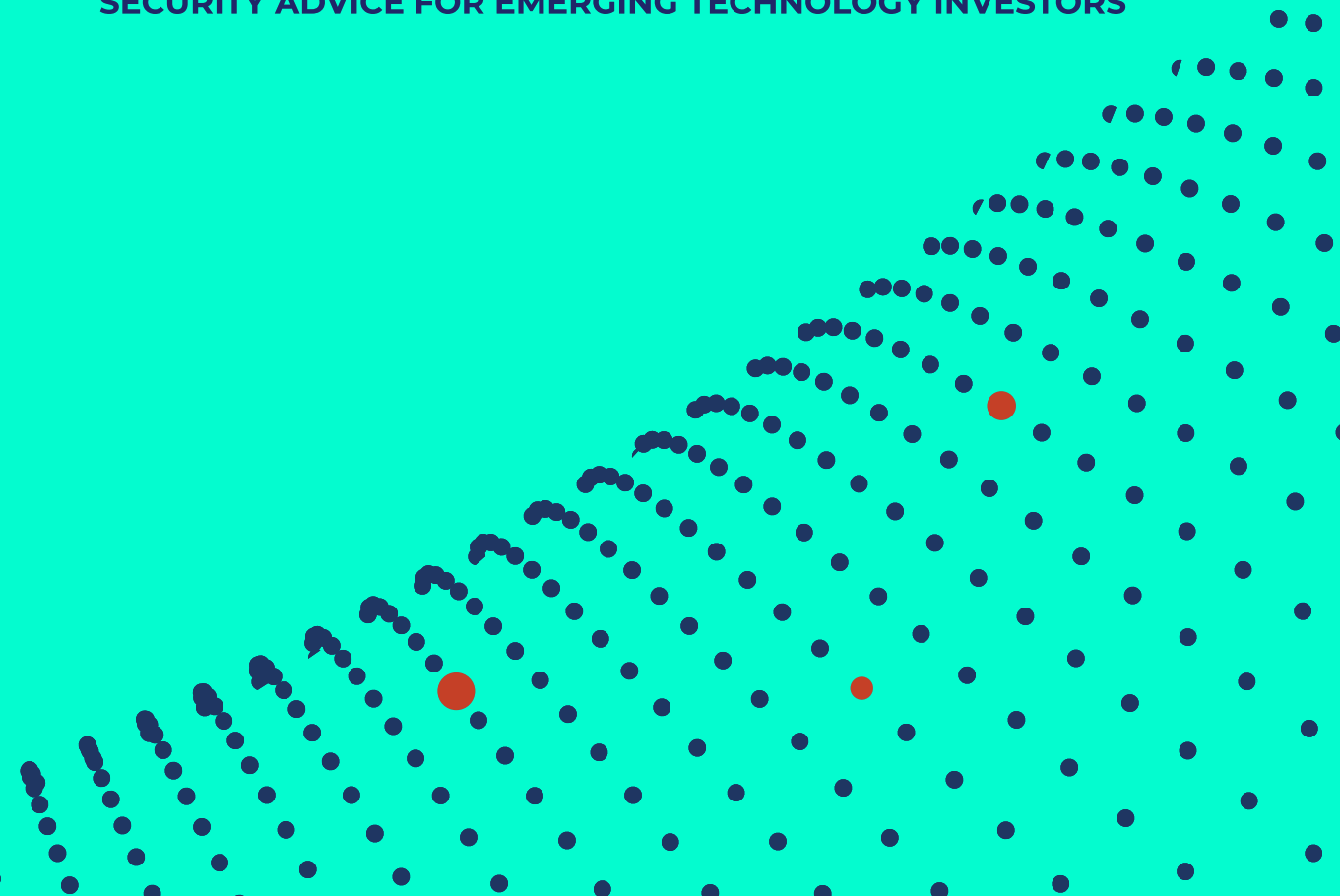
National Counterintelligence
and Security Center

# SECURE INNOVATION

## SECURITY ADVICE FOR EMERGING TECHNOLOGY INVESTORS

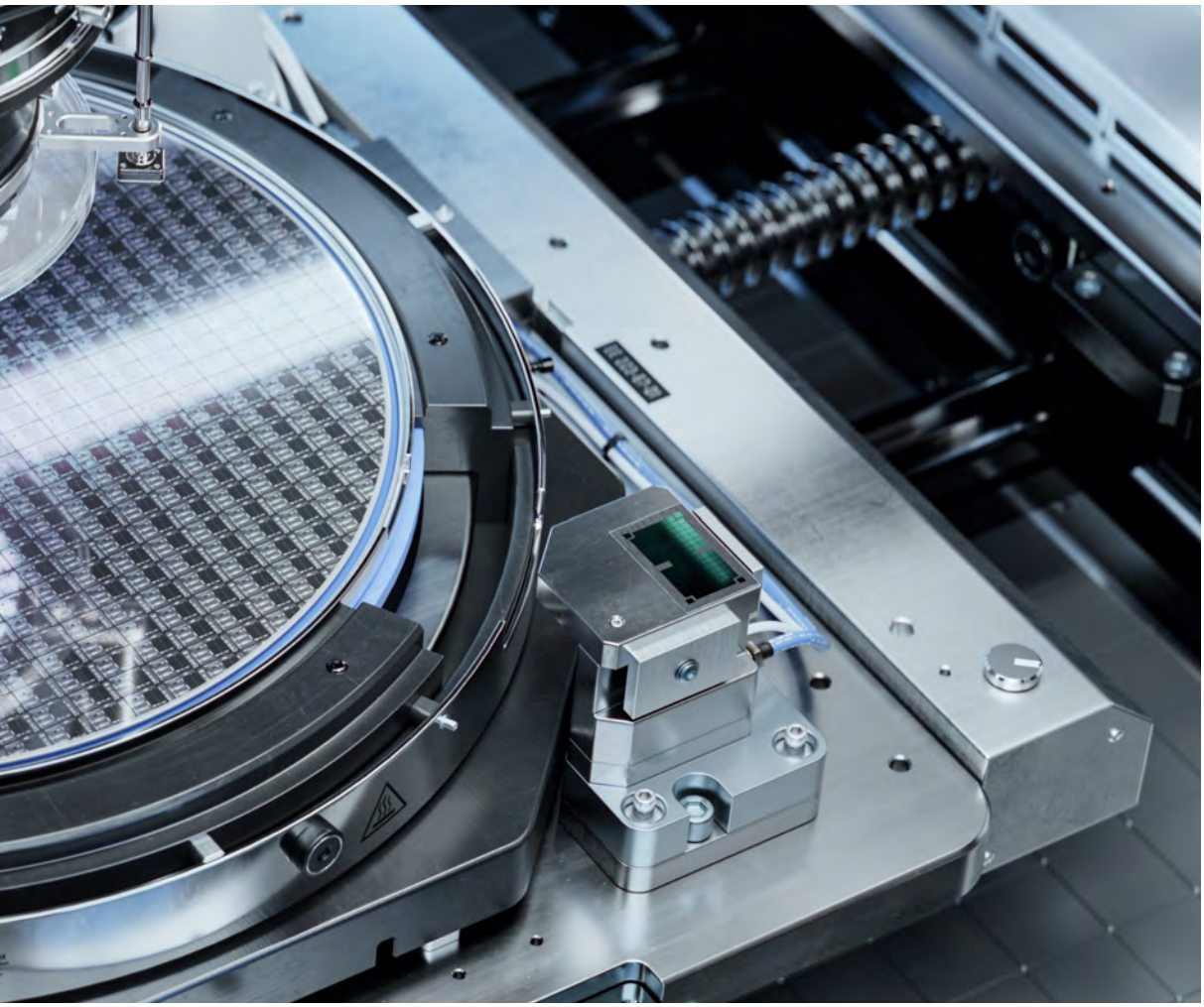


# SECURITY FROM THE START

# 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 make informed decisions that will increase the likelihood of seeing a return on your investment.



America's vibrant startup ecosystem and leading role in research and development bring many 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 prioritize security. Questions in this guidance are intended to help you inform your portfolio companies' attitudes around 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 these threats by continuing to discuss security for the duration of your involvement with the company.

# **WHAT IS** THE RISK?

**IN THIS SECTION:**

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

The U.S. is a global leader in research and development and has a vibrant startup ecosystem. This can make innovative U.S. companies attractive targets for a range of actors, such as:

### Competitors

Seeking commercial advantage.

### Criminals

Cyber crime is a major threat to businesses of all sizes, as criminals will try to 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 U.S. interests and values. The latter could include:

- Efforts to develop a research and innovation base that provides military and technological advantage over other countries
- Efforts 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 that may be viewed as hostile to the U.S. or one which has different non-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, export controls, or Committee on Foreign Investment in the United States (CFIUS) regulations?

The above questions should form part of your due diligence investigations into the startup and any other investors involved. They are intended to help you 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 along with other business risks. Clear accountability within the startup's leadership can indicate 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 that are most valued. A good security culture at the startup level is an essential component of a robust security organization.

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 architecture?

Small companies with limited resources will not be able to protect everything. Security decisions should be prioritized, 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, office space, 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.

01
## CASE STUDY

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

A Russian national pleaded guilty and was later sentenced after conspiring to pay an employee of a Nevada company to install malware on the company's computer networks in a bid to exfiltrate data and extort the company for ransom. The plot was thwarted after the employee reported the incident to the company, which notified law enforcement.

The hacking scheme was designed as a distributed denial-of-service attack, using junk data to flood the company's computer systems, while a second intrusion would allow co-conspirators to extract data from the company network and demand ransom with the threat of making the information public.

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 for a company to protect itself, as well as its investors.

*U.S. Department of Justice, Office of Public Affairs | Russian National Pleads Guilty to Conspiracy to Introduce Malware into a U.S. Company's Computer Network | 03/18/2021*

# THE FOLLOWING QUESTIONS WILL HELP YOU DETERMINE WHETHER THE COMPANY HAS BUILT ESSENTIAL SECURITY MEASURES INTO ITS OPERATIONS:

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?

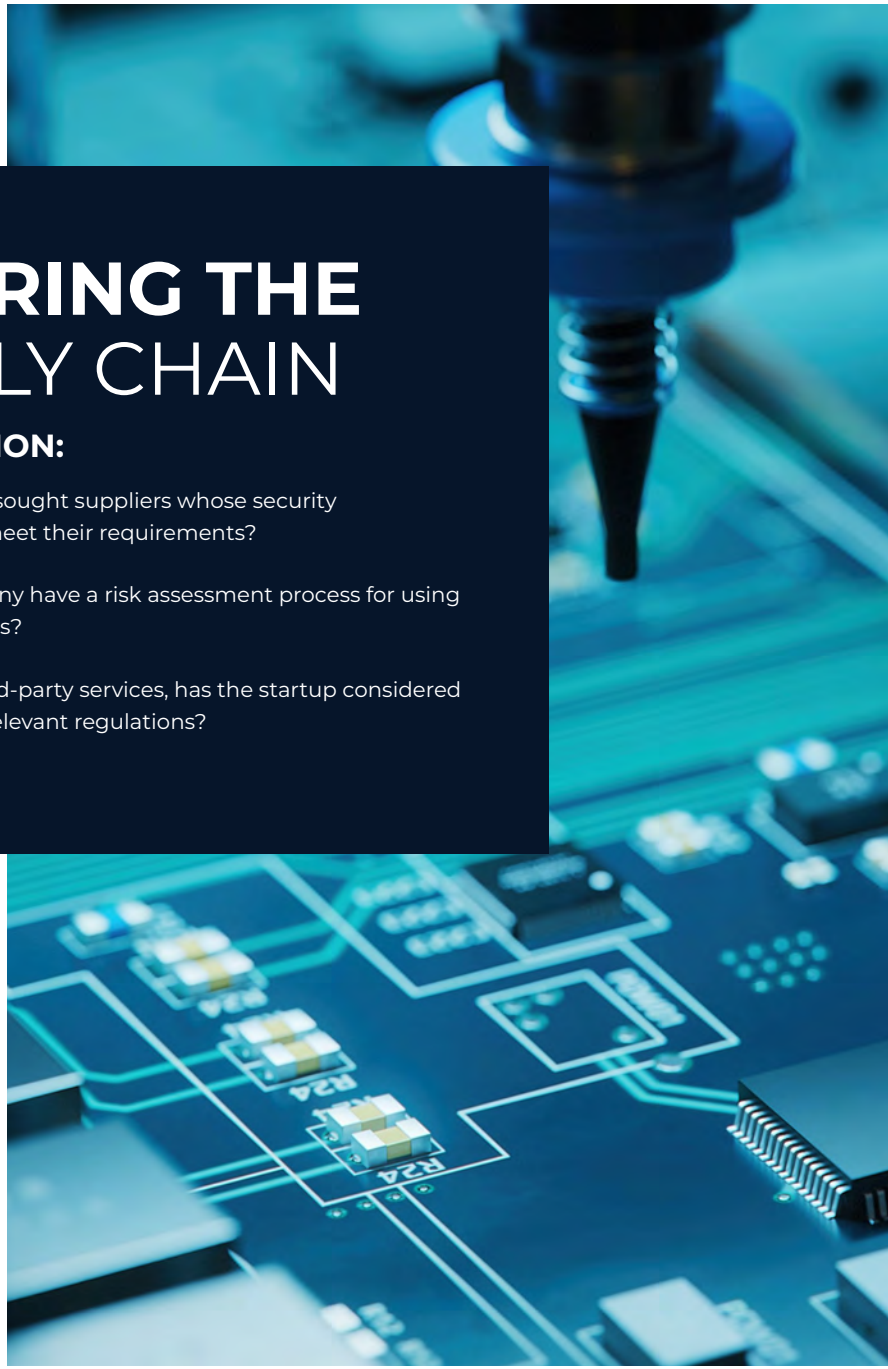
Is consideration given to the trustworthiness of internet connections used?

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 impacts of relevant regulations?



Outsourcing to an external provider, which may have specialist expertise that a small organization would struggle to resource, often brings enormous benefits for a startup. However, supply chains present a complex security risk. Therefore, they should be included in 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 offers a level of assurance that best meets their requirements
3. Considering the impact of relevant regulation, such as data privacy or protection regulations

# 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 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. Due diligence should include ethical, legal, and national security considerations as well as financial. This approach will help ensure they have 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 to ensure the startup has the technology and policies in place to guard against common cyber threats and meets minimum requirements for certain government contracts.

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

Smith's Harlow, a UK engineering company, agreed to a roughly $10 million acquisition by China's Future Aerospace in October 2017. Upon receipt of the first $3.9 million, Smith's Harlow shared sensitive details and committed to train Future Aerospace's engineers.

Press reports indicated that years later Future Aerospace cited difficulty obtaining approval from the government of China and withdrew from the deal without paying the rest of funds owed Smith's Harlow. Smith's Harlow's competitive advantage and intellectual property may have already been compromised.

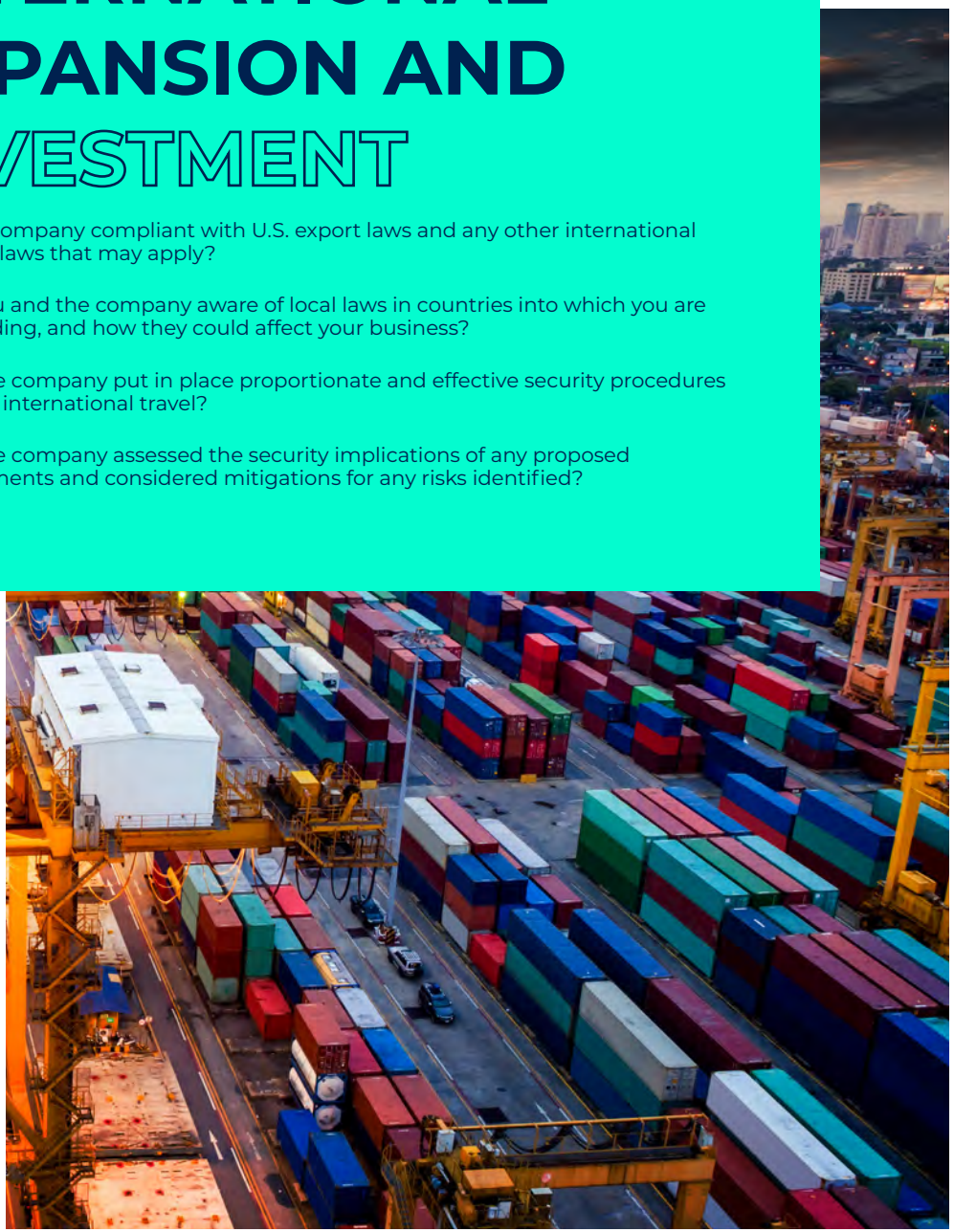
The company lost its license to make military equipment for Western powers due to its links with the China-based Future Aerospace. Ultimately, Smith's Harlow was left facing bankruptcy in 2020, citing Future Aerospace's theft of their trade secrets and reneging on the deal as the cause.

02
## CASE STUDY

- *Remarks by MI5 Director General Ken McCallum, "Joint address by MI5 and FBI Heads," 07/06/2022*
- *UK National Protective Security Authority (NPSA), "Secure Innovation" website, 10/17/2023*
- *Remarks by National Counterintelligence and Security Center (NCSC) Director Mike Casey to Marketplace Morning Report, "U.S. Startups Should be Wary of Knowledge Theft Disguised as Investment," 08/22/2024*

# INTERNATIONAL EXPANSION AND INVESTMENT

- Is the company compliant with U.S. export laws and any other international export laws that may apply?
- 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 U.S. and international sanctions or export control regulations, including the U.S. International Traffic in Arms Regulations (ITAR), particularly when items may have military as well as civilian applications.

## 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)

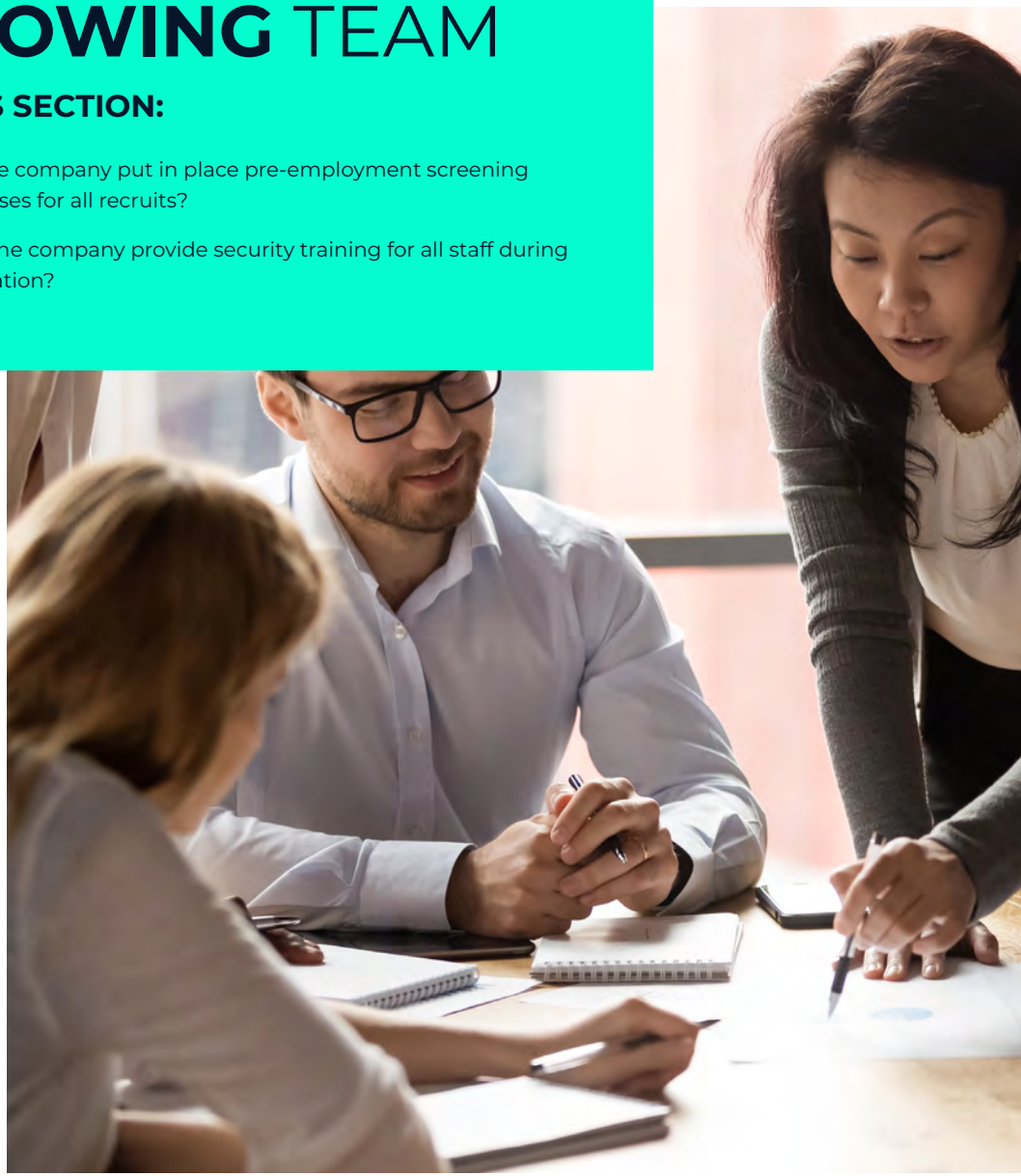
Whether they are on the entity lists of other countries, particularly those the start-up is, or may consider, doing business with

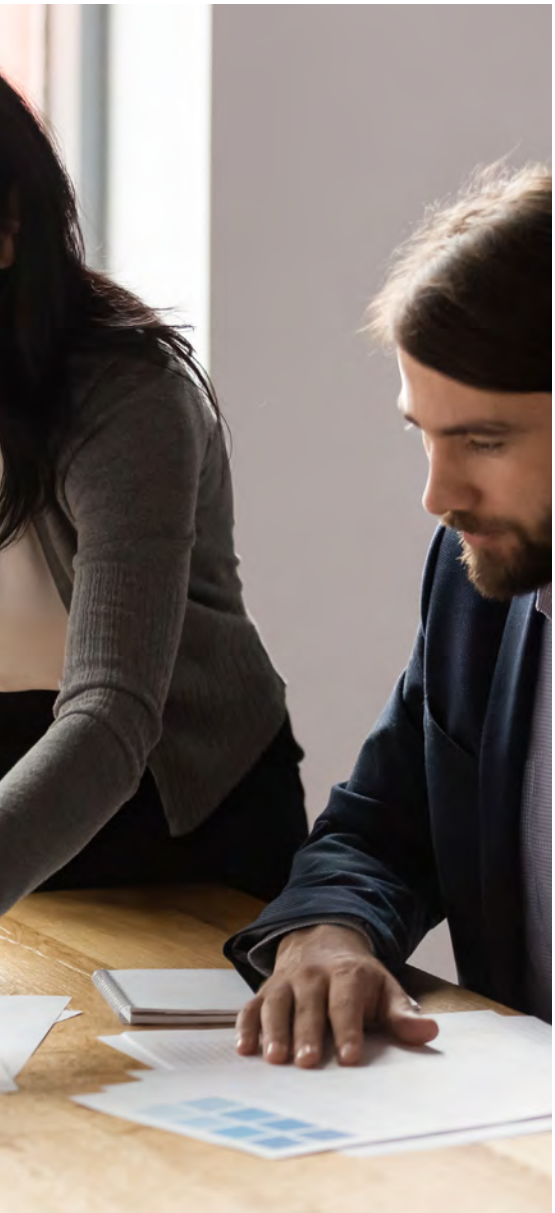
Whether they have unreported/unexpected commercial, political or military ties

# 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 during orientation?





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. Recommendations on ways to manage this include:

01

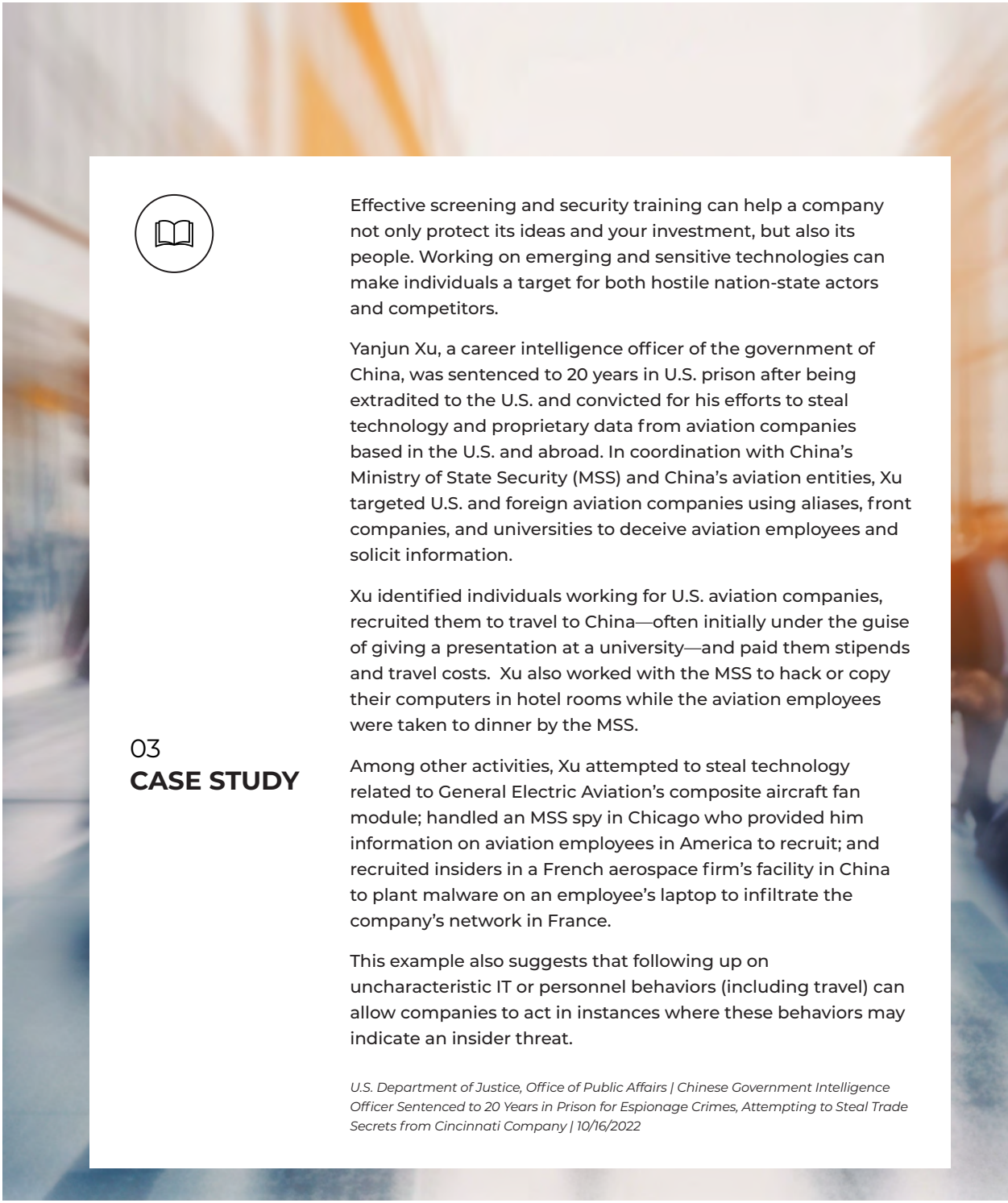
Making staff access controls role-specific, so access to sensitive assets is restricted to only those individuals who need it and are trusted to use it securely.

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.



03
## CASE STUDY

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

Yanjun Xu, a career intelligence officer of the government of China, was sentenced to 20 years in U.S. prison after being extradited to the U.S. and convicted for his efforts to steal technology and proprietary data from aviation companies based in the U.S. and abroad. In coordination with China's Ministry of State Security (MSS) and China's aviation entities, Xu targeted U.S. and foreign aviation companies using aliases, front companies, and universities to deceive aviation employees and solicit information.

Xu identified individuals working for U.S. aviation companies, recruited them to travel to China—often initially under the guise of giving a presentation at a university—and paid them stipends and travel costs. Xu also worked with the MSS to hack or copy their computers in hotel rooms while the aviation employees were taken to dinner by the MSS.

Among other activities, Xu attempted to steal technology related to General Electric Aviation's composite aircraft fan module; handled an MSS spy in Chicago who provided him information on aviation employees in America to recruit; and recruited insiders in a French aerospace firm's facility in China to plant malware on an employee's laptop to infiltrate the company's network in France.

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

*U.S. Department of Justice, Office of Public Affairs | Chinese Government Intelligence Officer Sentenced to 20 Years in Prison for Espionage Crimes, Attempting to Steal Trade Secrets from Cincinnati Company | 10/16/2022*

# PREPARING FOR SECURITY INCIDENTS

## IN THIS SECTION:

- Has the company established and tested an incident management plan?
- Can the company detect and investigate unexpected behavior 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 behavior.

When handled sensitively, an understanding of any uncharacteristic behavior 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:

- National Counterintelligence and Security Center (NCSC): www.NCSC.gov
- Federal Bureau of Investigation (FBI): www.FBI.gov
- If you believe that you, your personnel, or your company's data have been targeted, or are at risk of compromise, contact the FBI by calling 1-800-CALL-FBI (1-800-225-5324), submitting a message online to https://tips.fbi.gov, or reaching out to your local FBI field office at www.fbi.gov/contact-us/field-offices.

## Cyber Resources

- Cybersecurity and Infrastructure Security Agency (CISA): www.CISA.gov / CISA Cyber Guidance for Small Businesses: https://www.cisa.gov/cyber-guidance-small-businesses
- National Institute of Standards and Technology (NIST) — Small Business Cyber Security Corner: https://www.nist.gov/itl/smallbusinesscyber
- U.S. Small Business Administration -- Strengthen Your Cybersecurity Guide: https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity

## Intellectual Property Protection Resources

- U.S. Patent and Trademark Office — IP Basic Toolkits: https://www.uspto.gov/learning-and-resources/inventors-and-entrepreneurs/ip-basic-toolkits
- U.S. Patent and Trademark Office — Protecting Intellectual Property Rights Overseas: https://www.uspto.gov/ip-policy/ipr-toolkits

## Supply Chain Security Resources

- NCSC — Supply Chain Risk Management: https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats
- NIST — Cyber Supply Chain Risk Management: https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/publications

## Insider Risk Resources

- National Insider Threat Task Force: https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf
- Center for Development of Security Excellence — Insider Threat Toolkit: https://www.cdse.edu/Training/Toolkits/Insider-Threat-Toolkit/
- CISA — Resources for Onboarding and Employment Screening: https://www.cisa.gov/sites/default/files/2024-07/resources-for-onboarding-and-employment-screening-fact-sheet_07-25-2024_508.pdf

## Investment Resources

- The Committee on Foreign Investment in the United States (CFIUS): https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius
- Defense Counterintelligence and Security Agency — Foreign Ownership, Control, or Influence: https://www.dcsa.mil/Industrial-Security/Entity-Vetting-Facility-Clearances-FOCI/Foreign-Ownership-Control-or-Influence/
- NCSC — Safeguarding Our Innovation: Protecting U.S. Emerging Technology Companies from Investment by Foreign Threat Actors: https://www.dni.gov/files/NCSC/documents/products/FINALSafeguardingOurInnovationBulletin.pdf

## Export Resources

- International Trade Administration — Comply with U.S. Export Regulations: https://www.trade.gov/us-export-regulations
- U.S. Department of Commerce, Bureau of Industry and Security — Export Administration Regulations: www.bis.gov/regulations
- U.S. Department of State, Directorate of Defense Trade Controls: https://www.pmddtc.state.gov/ddtc_public/ddtc_public
- U.S. Department of Treasury, Office of Foreign Assets Control: https://ofac.treasury.gov/

## International Resources

- U.S. Department of Commerce, International Trade Administration -- Country Commercial Guides: https://www.trade.gov/country-commercial-guides
- U.S. Department of State — Investment Climate Statements: https://www.state.gov/reports/2024-investment-climate-statements/
- U.S. Department of State — International Travel: https://travel.state.gov/content/travel/en/international-travel.html
- U.K. National Cyber Security Centre (NCSC): www.NCSC.gov.uk

## Disclaimer