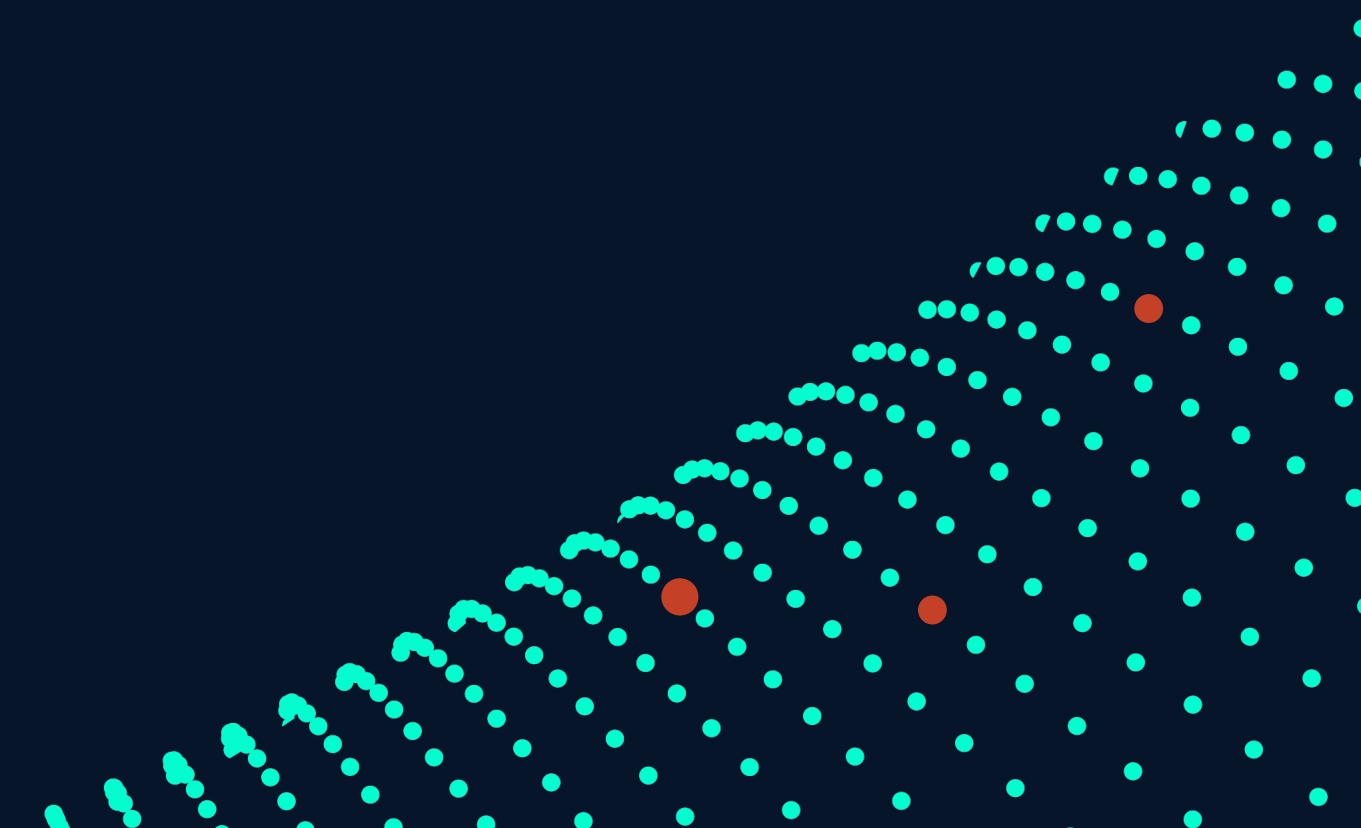
National Counterintelligence and Security Center

SECURE INNOVATION

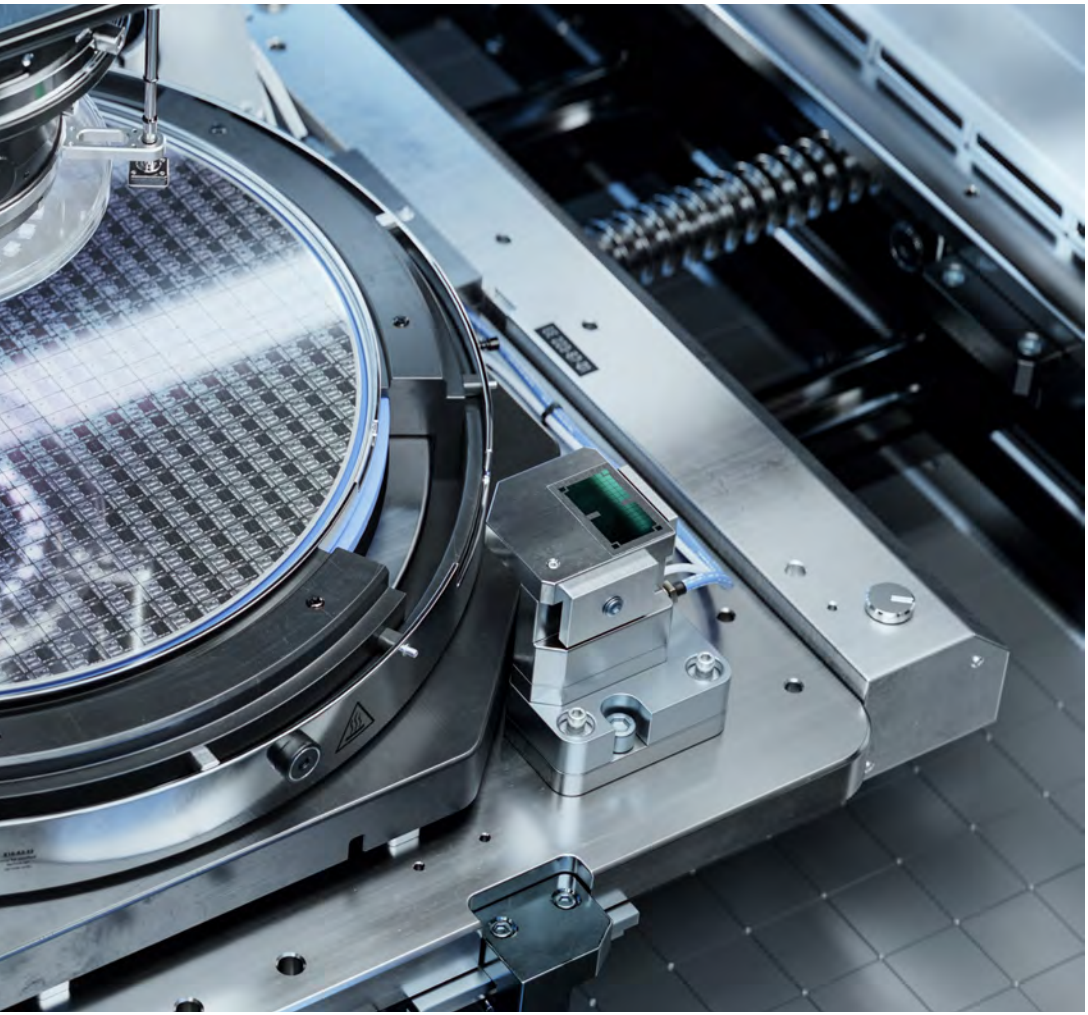
SECURITY ADVICE FOR EMERGING TECHNOLOGY COMPANIES



CONTENTS

SECURITY FROM THE START

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



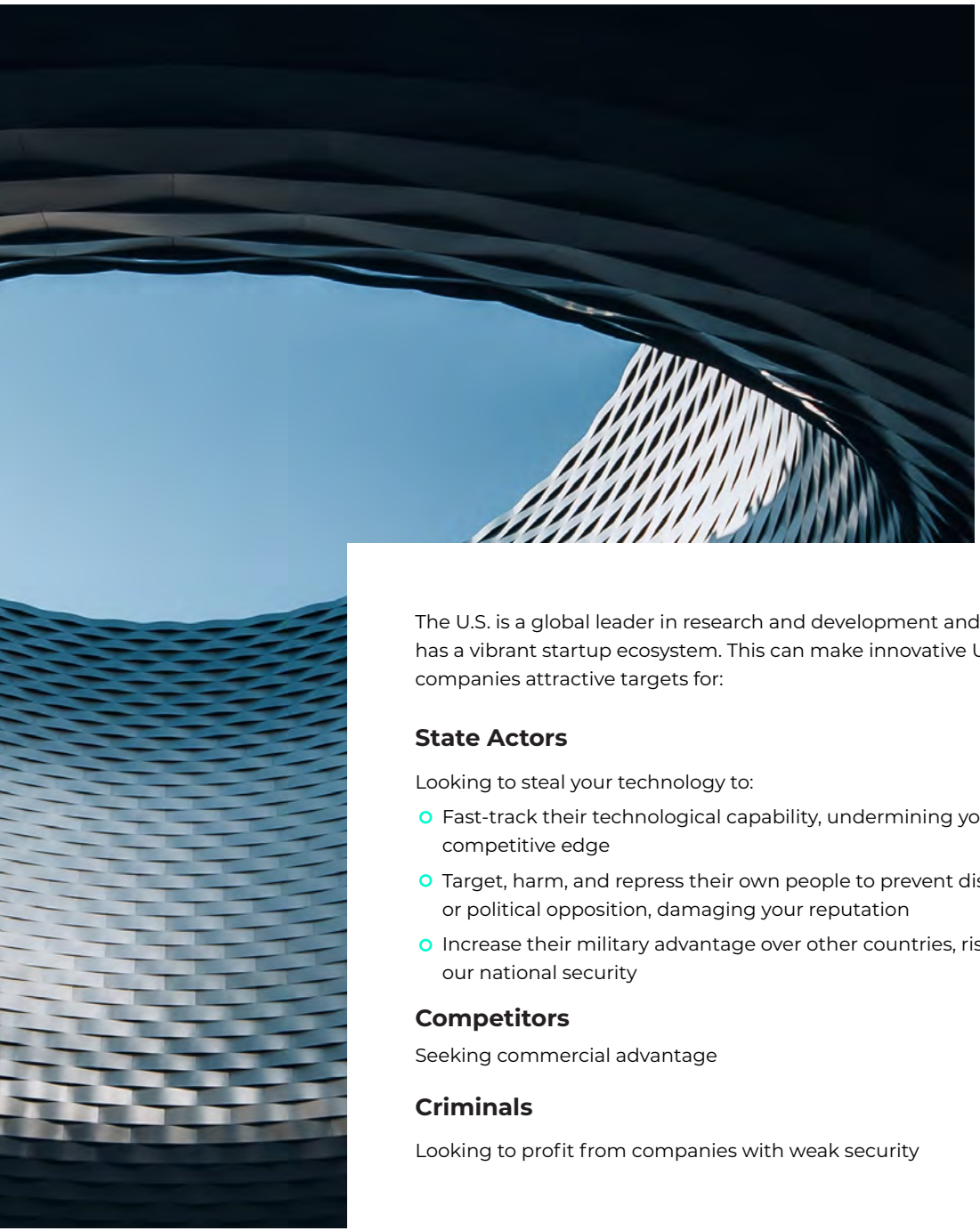
Good security practices can protect your competitive advantage, making your company more attractive to investors and customers. Laying strong foundations from the start will help your security be more effective and less costly as your business grows.

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 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:

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

01 CASE STUDY

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 information 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. He 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 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 work laptop to infiltrate the company's network in France.

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

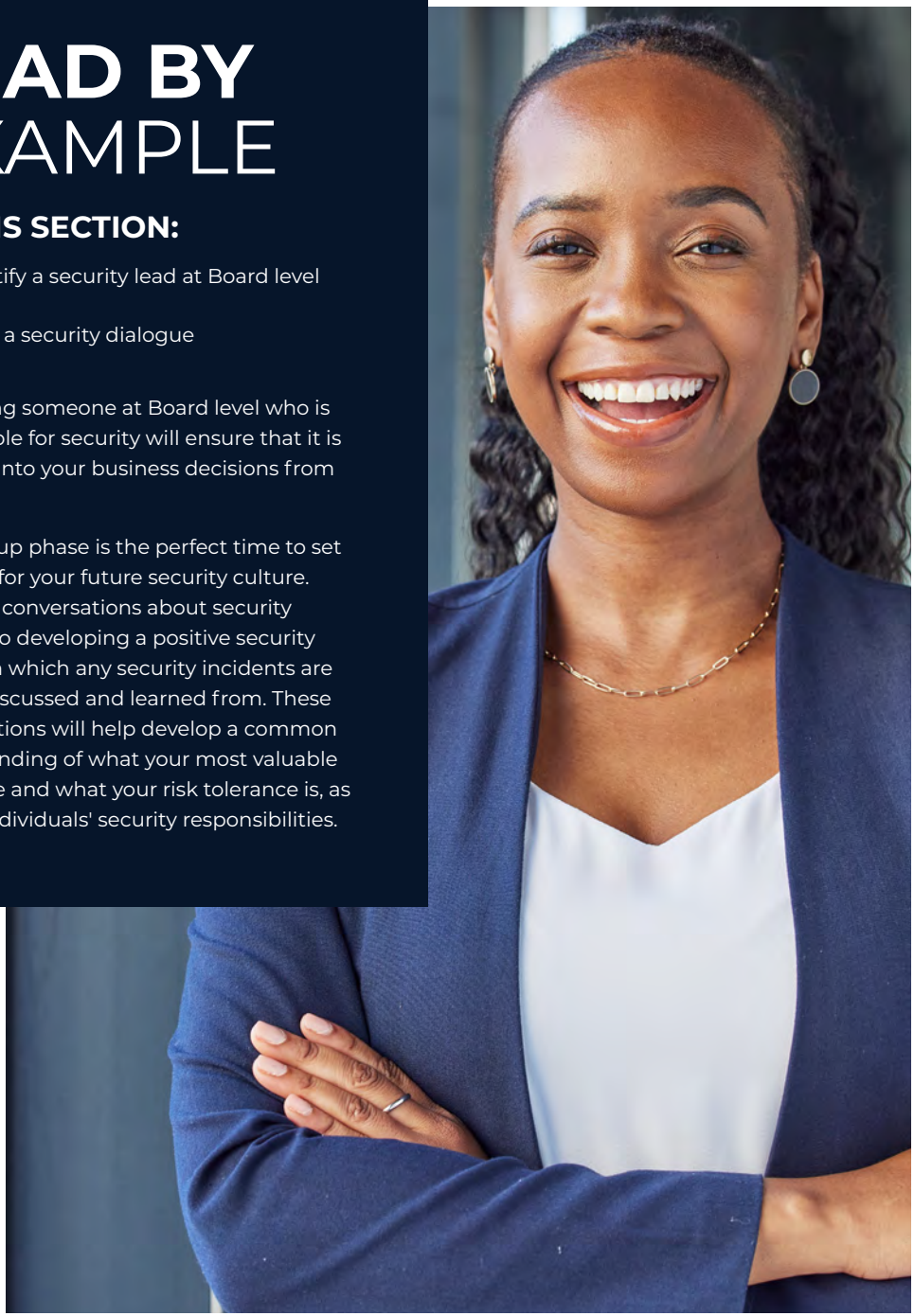
LEAD BY EXAMPLE

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.

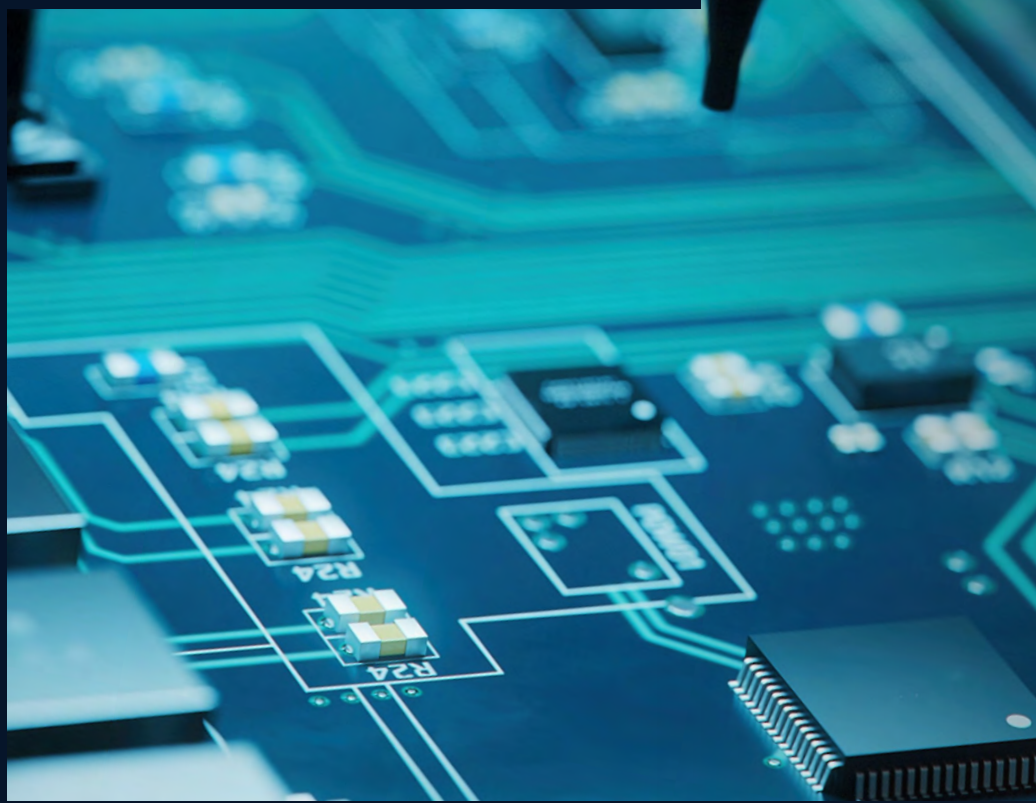
The startup phase is the perfect time to set the tone for your future security culture. Ongoing conversations about security are vital to developing a positive security culture in which any security incidents are openly discussed and learned from. These conversations will help develop a common understanding 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, those 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, office space, 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 prioritize:

- **YOUR ORGANIZATION'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 CONTINUOUSLY 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 prioritized, 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, personnel, and cyber security measures.

02
CASE STUDY

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 to effective mitigation measures.

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

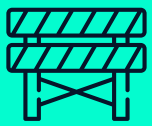
BUILD SECURITY INTO YOUR ENVIRONMENT

IN THIS SECTION:

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

Any security decisions you make will be strengthened by considering personnel, 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.

CENTER SECURITY AROUND YOUR MOST CRITICAL ASSETS



Place barriers (physical or virtual) **around each critical asset you have identified as needing protection,** such as trade secrets and proprietary information. Remember, if your competitors want it, so do foreign actors.

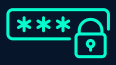
Restrict access to the asset to only those people who need it and are trusted to use it securely by using things like swipe card access and restricting administration rights. Ensure employees do not transport proprietary data about your company on their devices when traveling abroad.

Take regular, ideally automated, **backups of critical data** and keep them physically and virtually 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

Weak IT protocols can provide an easy way for your business to be exploited. The following steps are the minimum cyber security any organization should consider to reduce the likelihood and impact of your systems being breached.

Enable both your firewall and antivirus protection.

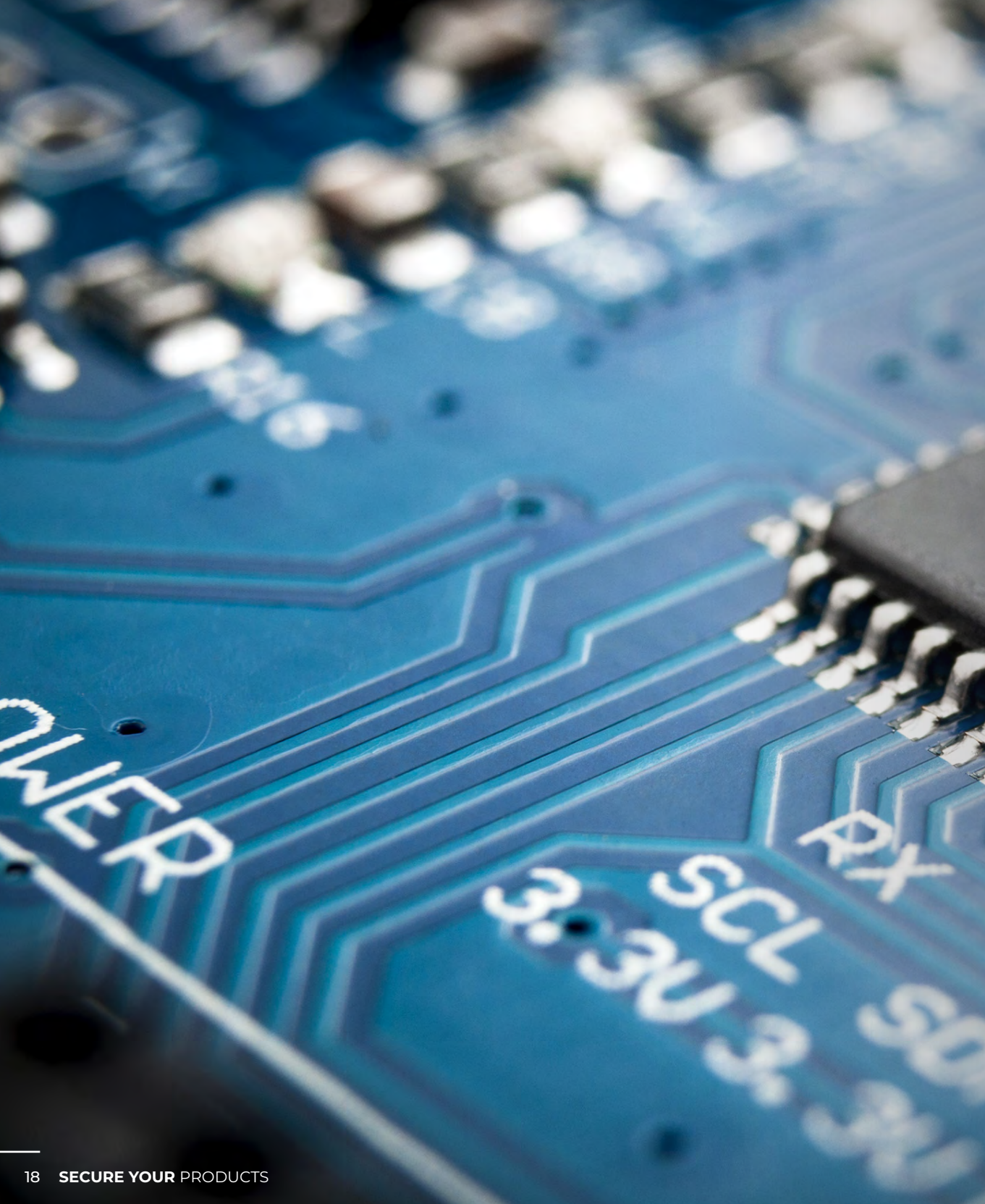


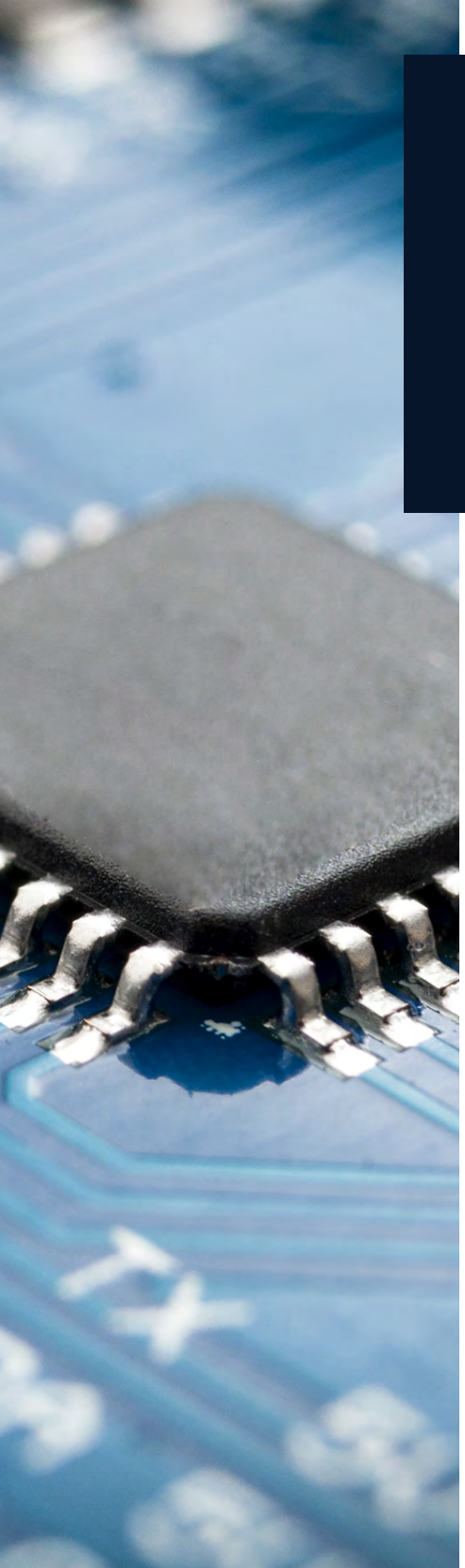
Use strong password protection and, where available, encryption on your devices and accounts. This means changing all default passwords, using unpredictable passwords and multi-factor authentication for important accounts.

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.


RX
SCL
3.3V



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 laws of the countries in which you are operating**
4. **How you are going to manage your IP**

4 SECURE YOUR PARTNERSHIPS

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

Partnerships increase the number of external routes into your organization and 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 mindful 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 to an acquisition offer from an investor in China, Smith's Harlow, a UK engineering company, signed several technology transfer agreements with their would-be acquirer. These agreements entailed the provision of training and revealing technology to the China-based investor, in return for a proportion of the company's agreed sales price.

Two years later, the investor in China had failed to complete the purchase or pay the remainder of funds owed Smith's Harlow, citing difficulty obtaining approval from the government of China. Meanwhile Smith's Harlow lost its license to make military equipment for Western powers due to its links with the China-based investor. Ultimately, Smith's Harlow was left facing bankruptcy and alleged its trade secrets had been stolen by the investor in China.

As the chairman of Smith's Harlow put it: "They've taken what they wanted and now they've got it, they didn't need the shell of Smith's."

- *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*

5 SECURE YOUR GROWTH

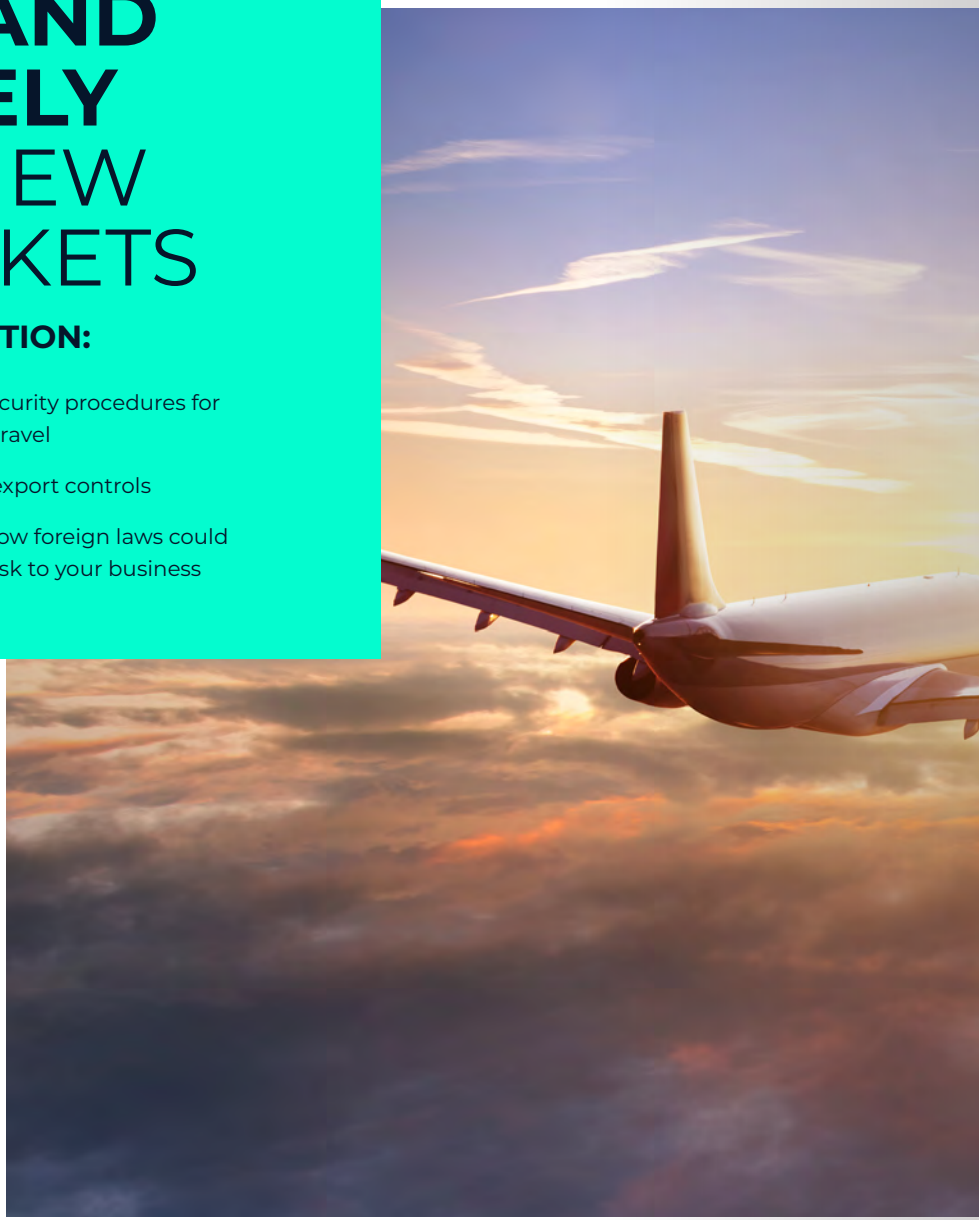
As your company continues to evolve, so too should your security measures. The risks you face may well have changed because your team has grown; you have moved to a new physical location or have added additional workspaces; you are collaborating with more partners; or because you are looking for investment.

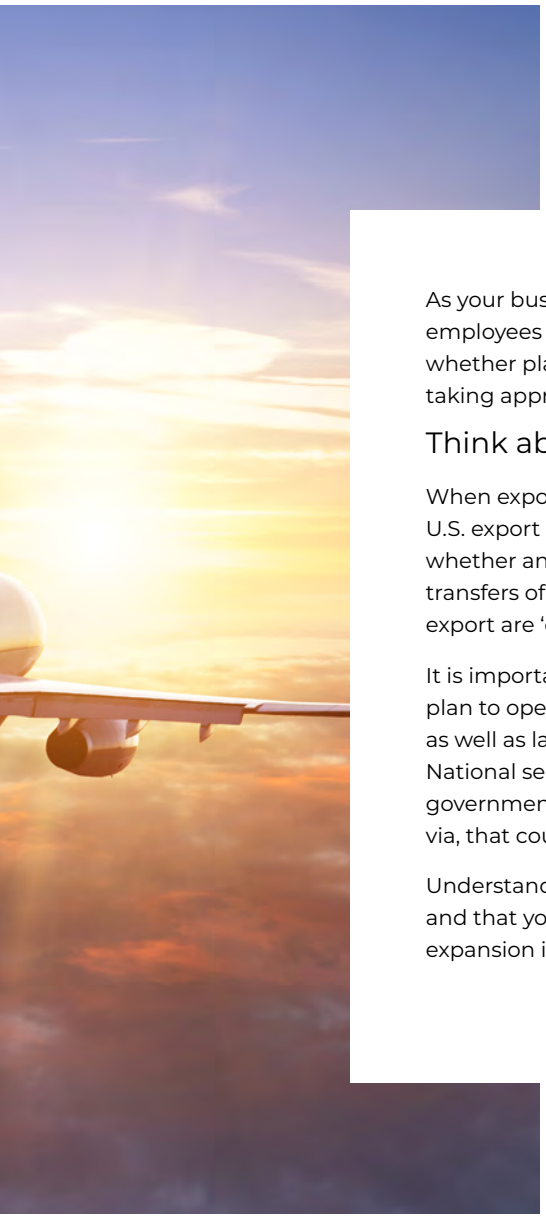
It is worth regularly reviewing your security measures to consider whether you need additional precautions.

EXPAND SAFELY TO NEW MARKETS

IN THIS SECTION:

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





As your business grows, 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 U.S. export control laws. These laws 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.

It is important to understand the 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
- Secure laptops and other portable devices during foreign travel (e.g., do not leave them unattended in hotel rooms, even in hotel safes)

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 assigning 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 onboarding/orientation, for your whole team can 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 can help you 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, requiring 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, is recommended for all individuals who are provided access, including permanent, temporary, and contract workers. Any pre-employment screening should be consistent with applicable laws.

04
CASE STUDY

Sinovel Wind Group, a wind turbine maker in China, was convicted and fined in the U.S. after stealing trade secrets from a U.S.-based company, causing the victim company to lose almost 700 jobs and more than $1 billion in shareholder equity. Sinovel recruited an employee of the U.S.-based company to secretly download source code relating to the U.S. company's 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, but your personnel security practices need to be maintained with ongoing conversations, security training, and observations.

U.S. Department of Justice, Office of Public Affairs | Court Imposes Maximum Fine on Sinovel Wind Group for Theft of Trade Secrets | 07/06/2018

CONSIDERATIONS FOR PRE-EMPLOYMENT SCREENING:*

- CONFIRMATION OF IDENTITY
- NATIONALITY AND IMMIGRATION STATUS
- EMPLOYMENT AND EDUCATION HISTORY
- FINANCIAL RECORDS CHECK
- CRIMINAL RECORDS CHECK
- PERSONAL REFERENCES
- OPEN-SOURCE ENVIRONMENT
- PRIOR FELLOWSHIPS OR FUNDING FROM FOREIGN GOVERNMENTS
- NATIONAL SECURITY VETTING (FOR ACCESS TO GOVERNMENT CLASSIFIED MATERIAL)

**Any pre-employment screening should be consistent with applicable laws.*

PREPARE FOR SECURITY INCIDENTS

IN THIS SECTION:

- Establish and test an incident management plan
- Check your staff and IT to detect unexpected behavior

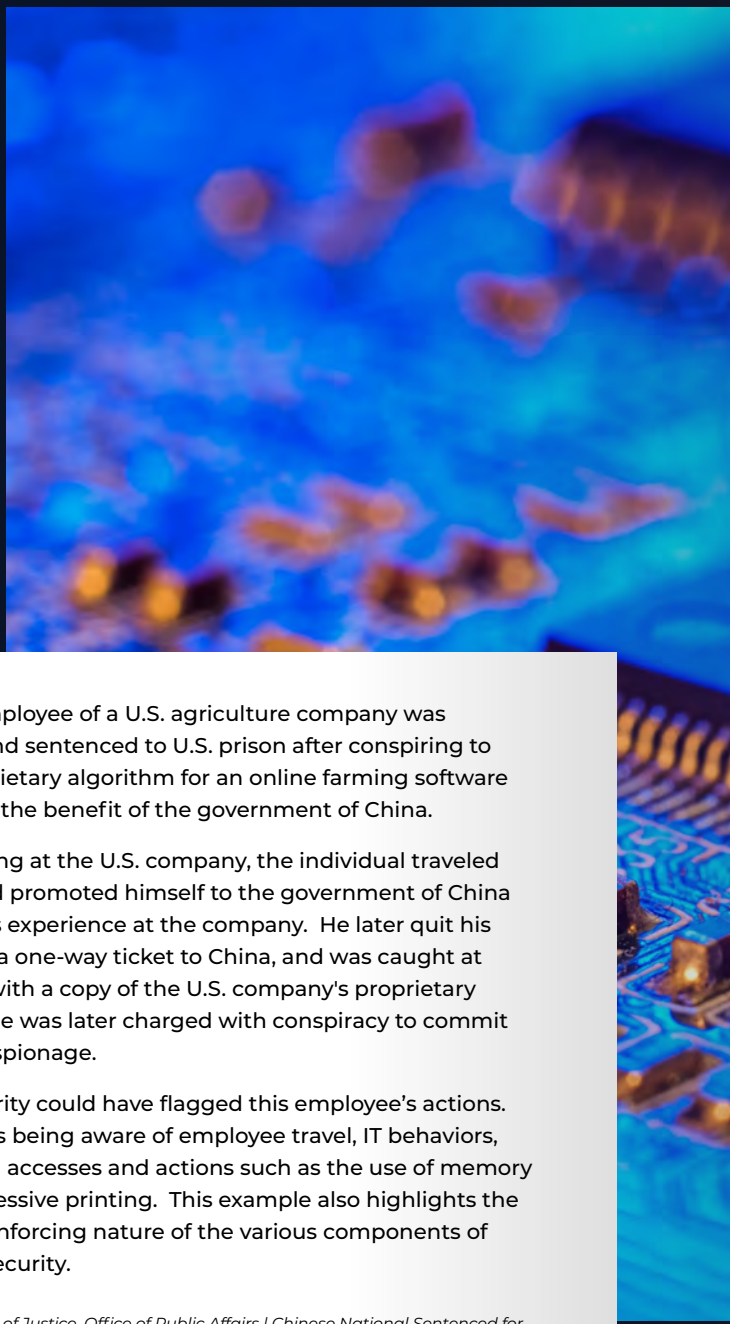
The damage caused by a breach can be reduced through a well-planned and executed response. It is worth assuming that your business will be breached and planning accordingly.

INCIDENT MANAGEMENT

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. Understand what your obligations are to report certain incidents to law enforcement or regulatory bodies.

Maintaining an understanding of your IT's functionality 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 behavior, 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 response designed to help the employee overcome such challenges can help to improve your employees' relationship with the company, building trust and the right attitude towards security in the workforce.



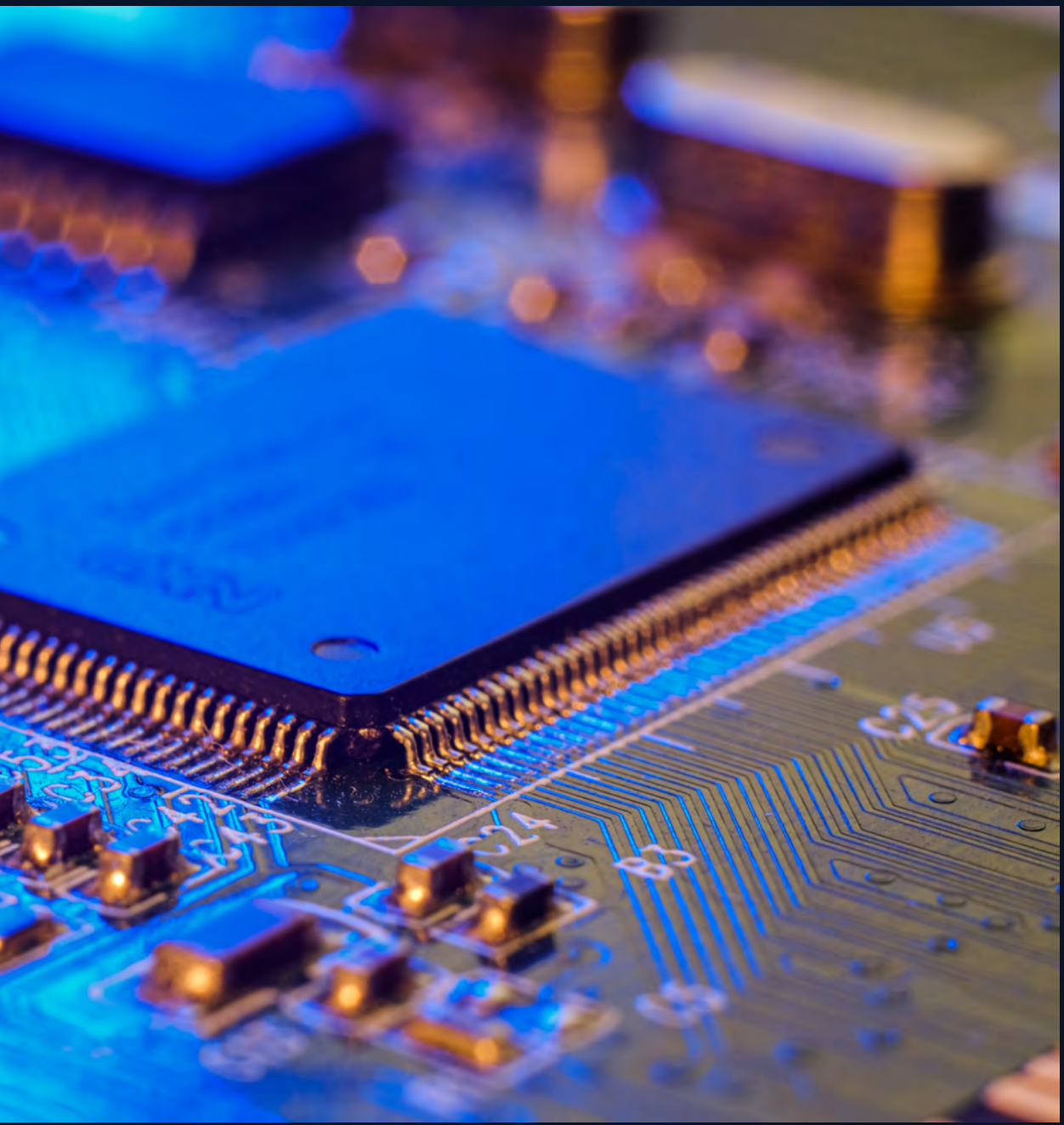
05
CASE STUDY

A former employee of a U.S. agriculture company was convicted and sentenced to U.S. prison after conspiring to steal a proprietary algorithm for an online farming software platform for the benefit of the government of China.

While working at the U.S. company, the individual traveled to China and promoted himself to the government of China based on his experience at the company. He later quit his job, bought a one-way ticket to China, and was caught at the airport with a copy of the U.S. company's proprietary algorithm. He was later charged with conspiracy to commit economic espionage.

Strong security could have flagged this employee's actions. This includes being aware of employee travel, IT behaviors, 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.

U.S. Department of Justice, Office of Public Affairs | Chinese National Sentenced for Economic Espionage Conspiracy | 04/07/2022



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

The information contained in this document is accurate on the date it was created and is intended as general guidance only. Consider the enclosed information within the context of existing laws, regulations, authorities, agreements, policies, or procedures and consult with independent experts. To the fullest extent permitted by law, NCSC accepts no liability whatsoever for any loss or damage incurred or arising because of any error or omission in the guidance or arising from any person acting, relying upon, or otherwise using this guidance. References in this product to any specific commercial product, process, or service or the use of any corporate name herein is for informational purposes only and does not constitute an endorsement, recommendation, or disparagement of that product, process, service, or corporation on behalf of the Intelligence Community.