SAFEGUARDING THE DATA OF U.S. FINANCIAL INSTITUTIONS

Navigating Threats from China

OVERVIEW

The government of China and its proxies are intensifying their collection of data from public and private U.S. financial institutions and their employees, as China seeks to compete with and ultimately displace the United States as the world's leading economic power.

Targets of these collection activities may include corporate financial data, business strategies, proprietary data, economic information, policymaker plans, and a range of other non-public data. While some targeted data may seem insignificant in isolation, when combined with other information (including bulk data) collected by China, it can be used to advance China's interests and threaten U.S. financial institutions, markets, and economic security.

THREAT

China continues to use an array of tactics to obtain data from U.S. financial institutions, including collection on U.S. financial sector travelers to China and Hong Kong, recruitment of insiders, use of malicious cyber activity, supply chain compromise, and other techniques. China also employs its legal and regulatory framework and leverages Chinese commercial entities to acquire data from U.S. financial institutions doing business in China or Hong Kong.

- U.S. financial sector travelers to China have recently reported perceived government collection activity targeting them in China.
- Authorities in China have placed exit bans on some U.S. persons, including a U.S. financial sector executive in 2025, temporarily blocking their departure from China.
- A 2025 U.S. indictment alleges that Chinese intelligence and security officials posing as students recruited a U.S. Federal Reserve official to provide them proprietary economic data sets, tariff deliberations on China, and other data that could allow China to manipulate U.S. markets.
- In 2024, Chinese state cyber actors accessed U.S. Treasury Department data and workstations by compromising a third-party software-as-a-service provider. In 2025, Treasury sanctioned an individual affiliated with China's civilian intelligence service in connection with this intrusion.
- Recent national security, data privacy, and cybersecurity laws in China have provided China with expanded legal grounds for accessing and controlling data held by U.S. firms in China.
- U.S. firms in China have detected malware in tax software mandated by China's government and supplied by authorized Chinese commercial entities that launched backdoors into their systems, likely allowing cyber actors to preposition to conduct data exfiltration activities.

MITIGATION

Below are steps U.S. financial institutions may consider to help protect themselves and their employees.

ENTERPRISE RISKS:

- Treat your "crown jewels" as intellectual property to support potential legal actions if they are misappropriated. Handle and protect that data in a documented way to support legal actions.
- Ensure collaborative security efforts between cyber, security, Information Technology, insider risk, legal, human resources, and procurement offices across your organization.
- Hold exercises to "war game" a range of damaging scenarios and repeat.

RISKS OPERATING IN CHINA:

- Monitor China's evolving legal and regulatory framework and the implications for U.S. financial institutions. Develop protection plans for your institution and employees in China and Hong Kong, including contingency plans if an exit ban is placed on an employee based in or traveling to China or Hong Kong.
- Understand that China's legal framework may bar your employees in China and Hong Kong from sharing certain information with your institution in the U.S. and account for that gap when evaluating risk.
- As a baseline, have no expectation of privacy when doing business in China or Hong Kong. Conduct your operations accordingly.
- Consider moving or keeping your most critical data or crown jewels out of China and Hong Kong. If possible, consider segregating your IT networks in China and Hong Kong from your other global operations.

FOREIGN TRAVEL RISKS:

- Obtain clean devices for employees traveling to any foreign nation, particularly China and Hong Kong, and ensure the devices only contain data essential to that trip. Employees should expect no privacy on devices abroad.
- Implement training and reporting protocols for employees that address elicitation attempts. Train employees to exercise caution and due diligence before responding to virtual or in-person approaches by unknown parties, including those offering jobs or invitations to speak abroad.
- Set policies on employee reporting of foreign contacts, employment, or travel, including policies regarding acceptance of foreign reimbursement or gifts in exchange for work or information.
- Have pre-and post-foreign-travel security discussions with employees and encourage reporting of any suspicious activity during foreign trips to corporate security or your local FBI office.
- Visit the National Counterintelligence and Security Center's (NCSC) Secure Innovation travel security guidance for additional information.

INSIDER RISKS:

- Implement robust insider risk training and awareness programs in your organization.
- Ensure employees know what must be protected. Provide a positive security environment in which employees are confident reporting security concerns and know where to report them.
- Conduct background checks and vetting of employees, including pre-employment screening and continuous monitoring where possible, and additional oversight for those with sensitive access.
- Add recurring training on threats, indicators, security best practices, and reporting protocols. Document employee participation and incentivize adherence to security policies.
- Engage personnel leaving your institution to ensure they know their continuing responsibilities and/or legal obligations to safeguard sensitive or proprietary data.

CYBER RISKS:

- Follow cyber security best practices, including installing regular software updates and patches, as well as use of strong passwords, multi-factor authentication, data encryption, virtual private networks, backup systems, firewalls, and security controls on applications.
- Maintain access controls and monitoring, including Least Privilege Principle, Segregation of Duties, and use robust logging and monitoring systems to detect unusual or unauthorized access. Keep an "anomaly" log of irregular incidents to potentially spot malicious trends.
- Train employees on their role in cybersecurity.
- Develop and implement incident response plans and conduct periodic tests and exercises.
- Stay up to date on public threat alerts from agencies like the Cybersecurity and Infrastructure Security Agency (CISA) (www.cisa.gov/topics/cyber-threats-and-advisories) and the FBI (www.fbi.gov/how-we-can-help-you/office-of-private-sector).

SUPPLY CHAIN RISKS:

- Maintain an inventory of all vendors, partners, and third-party services your organization uses.
- Implement vendor risk management, including conducting due diligence, developing risk assessments, and using vetted vendors with recognized security certifications.
- Incorporate security requirements, such as incident reporting, into third-party contracts and monitor compliance throughout the lifecycle of a product or service.
- Limit vendor access to only the data and systems necessary for their role. Separate vendor access from internal systems to reduce the potential impact of a breach.

REPORTING INCIDENTS

- If you believe your financial institution has been targeted by foreign threat actors or is at risk, contact your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices.
- Report significant cyber incidents through CISA's Incident Reporting System (IRF) at https://myservices.cisa.gov/irf.
- For additional information on NCSC threat awareness materials or publications, visit https://www.ncsc.gov or contact NCSC_Outreach@odni.gov. Follow NCSC on (X) Twitter @NCSCStreet and LinkedIn for more information.