RED DART ALLIANCE

Chinese Businessman Pleads Guilty of Spying on F-35 and F-22

SOURCE: Wendell Minnick, /Defense News / March 24, 2016

TAIPEI — Two years after his arrest in Canada, Su Bin, a Chinese citizen who ran Lode-Technology, has pled guilty in a California federal court to carrying out a series of cyber espionage thefts of U.S. military secrets that included the C-17 Globemaster, and Lockheed F-35 and F-22 stealth fighters.

In a March 23 press release issued by the U.S. Department of Justice, Central District of California, in a plea agreement, Su "admitted to conspiring with two persons in China from October 2008 to March 2014 to gain unauthorized access to protected computer networks in the United States, including computers belonging to the Boeing Company in Orange County, California, to obtain sensitive military information and to export that information illegally from the United States to China."

Boeing was hit hard by the cyber intrusion into one of the U.S. company's most protected files on the C-17 Globemaster program, according to a 50-page criminal complaint filed by the FBI in a June 27, 2014, affidavit that revealed the extent of a three-man group's alleged hacking activities. Data on "dozens of U.S. military projects," including the F-35 and F-22 stealth fighters, also was stolen in intrusions into other companies' networks.

Besides Su Bin (Stephen Su) there were two unidentified mainland Chinese cohorts. Lode-Technology is mainly engaged in the aircraft cable harness business, but U.S. and European company websites also indicate the company served as an agent and distributor of aviation tooling and UV-laser products in China.

Continued on Page 2

Chinese Businessman Pleads Guilty of Spying on F-35 and F-22

Continued from Previous Page

Su was arrested June 28, 2014, in Canada and waved extradition to the U.S. in February 2016. Su pleaded guilty this week before U.S. District Judge Christina A. Snyder.

Su is alleged to have obtained F-35 test plans and "blueprints" that would "allow us [China] to catch up rapidly with U.S. levels ... [and] stand easily on the giant's shoulders," according to Su's emails.

Details of other aircraft and U.S. companies are sketchy. Su is alleged to have obtained F-35 test plans and "blueprints" that would "allow us [China] to catch up rapidly with U.S. levels ... [and] stand easily on the giant's shoulders," according to Su's emails.

F-35 Joint Strike Fighter, Lightning II

A former U.S. government counterintelligence analyst on China said the case is a "close parallel" to other cases involving Chinese businessmen "taking government information to ensure long-term success of [their] business." He also said that Canada and Hong Kong were still popular technical transfer shipment points for Chinese industrial and military espionage.

According to the complaint, one of Su's emails states that his team "secured the authority to control the website of the ... missile developed jointly by India and Russia and that they would 'await the opportunity to conduct internal penetration.'"

Su also allegedly focused on military technology in Taiwan and files held by various Chinese "democracy" groups and the "Tibetan Independence Movement." On Taiwan, the intelligence collected was focused on military maneuvers, military construction, warfare operation plans, strategic targets and espionage activities.

Continued on Page 3

Chinese Businessman Pleads Guilty of Spying on F-35 and F-22

Continued from Previous Page

According to one of the several emails, “we still have control on American companies like [identifying U.S. companies] and etc. and the focus is mainly on those American enterprises which belong to the top 50 arms companies in the world.”

One attachment listed 32 U.S. military projects and another listed 80 engineers and program personnel working on a “military development project.” Another listed the names and email addresses for four people at a “European company that develops military navigation, guidance and control systems.”

Cyber intrusions into Boeing and other companies were sophisticated. According to one of Su’s emails, they had control of an unidentified defense company’s file transfer protocol server. Jump servers, also known as “hop points,” were set up in France, Japan, Hong Kong, Singapore, South Korea and the United States According to emails, these were set up to avoid “diplomatic and legal” difficulties for China.

According to one email, “the collected intelligence will be sent first by an intelligence officer placed outside China or via a jump server which is placed in a third country before it finally gets to the surrounding regions/areas or a work station located in Hong Kong or Macao. The intelligence is always picked up and transferred to China in person.”

The alleged perpetrators accessed Boeing computers “directly,” according to the original 2014 complaint. One Su email announced the first penetration occurred in January 2010. Further, “we discovered that the Boeing Company’s internal network structure is extremely complex.” The email states that its border deployment has firewalls and intrusion prevention systems, the core network deployment has intrusion detection systems, “and the secret network has ... type isolation equipment as anti-invasion security equipment in huge quantities.” Additionally, “we have discovered in its internal network 18 domains and about 10,000 machines.”

Su allegedly wrote, “through painstaking labor and slow groping,” they discovered C-17 data “stored in the secret network.” Getting to the data was obviously not easy, as “the secret network is not open 24 hours and is normally physically isolated, it can be connected only when C-17 project related personnel have verified their secret code.” C-17 data included drawings, revisions, group signatures, performance and flight test documents.

Continued on Page 4

Chinese Businessman Pleads Guilty of Spying on F-35 and F-22

Continued from Previous Page

One Chinese company under suspicion is the Xian Aircraft Industrial Corp., which is building a C-17 look-alike dubbed the Y-20. In one e-mail mentioned in the complaint, Su allegedly expected "big money" for the C -17 data and complained that the unidentified Chinese company was "too stingy" for paying $5,000.

Despite expectations in 2014 that Su would face up to 30 years in prison, the U.S. Department of Justice press release indicated he faces a maximum of only four years and would be sentenced in July. Despite the reduced sentence, there was significant backslapping and self-congratulations in the press release amongst the prosecution, including U.S. Attorney Eileen M. Decker, Assistant Attorney General for National Security John P. Carlin, Assistant Director Jim Trainor of the FBI's Cyber Division, and Assistant Director in Charge David Bowdich of the FBI's Los Angeles Division.

"Protecting our national security is the highest priority of the U.S. Attorney's Office, and cybercrime represents one of the most serious threats to our national security," Decker said. "The innovative and tireless work of the prosecutors and investigators in this case is a testament to our collective commitment to protecting our nation's security from all threats. Today's guilty plea and conviction demonstrate that these criminals can be held accountable no matter where they are located in the world and that we are deeply committed to protecting our sensitive data in order to keep our nation safe."

F-22 Raptor

"Su Bin admitted to playing an important role in a conspiracy, originating in China, to illegally access sensitive military data, including data relating to military aircraft that are indispensable in keeping our military personnel safe," Carlin said. "This plea sends a strong message that stealing from the United States and our companies has a significant cost; we can and will find these criminals and bring them to justice. The National Security Division remains sharply focused on disrupting cyber threats to the national security, and we will continue to be relentless in our pursuit of those who seek to undermine our security."

(Please visit http://www.defensenews.com/story/breaking-news/2016/03/24/chinese-businessman-pleads-guilty-spying-f-35-and-f-22/82199528/ for the entire article.)

U.S. Says It Has Unlocked iPhone Without Apple

The decision to drop the case ends a legal standoff between the government and the world's most valuable public company.

SOURCE: NY Times/By KATIE BENNER and ERIC LICHTBLAUMARCH 28, 2016

SAN FRANCISCO — The Justice Department said on Monday that it had found a way to unlock an iPhone without help from Apple, allowing the agency to withdraw its legal effort to compel the tech company to assist in a mass-shooting investigation.

The decision to drop the case — which involved demanding Apple's help to open an iPhone used by Syed Rizwan Farook, a gunman in the December shooting in San Bernardino, Calif., that killed 14 people — ends a legal standoff between the government and the world's most valuable public company. The case had become increasingly contentious as Apple refused to help the authorities, inciting a debate about whether privacy or security was more important.

Yet law enforcement's ability to now unlock an iPhone through an alternative method raises new uncertainties, including questions about the strength of security in Apple devices. The development also creates potential for new conflicts between the government and Apple about the method used to open the device and whether that technique will be disclosed. Lawyers for Apple have previously said the company would want to know the procedure used to crack open the smartphone, yet the government might classify the method.

"From a legal standpoint, what happened in the San Bernardino case doesn't mean the fight is over," said Esha Bhandari, a staff lawyer at the American Civil Liberties Union. She notes that the government generally goes through a process whereby it decides whether to disclose information about certain vulnerabilities so that manufacturers can patch them.

Continued on Page 6

U.S. Says It Has Unlocked iPhone Without Apple

Continued from Previous Page

“I would hope they would give that information to Apple so that it can patch any weaknesses,” she said, “but if the government classifies the tool, that suggests it may not.”

In a two-paragraph filing on Monday, the Justice Department said it had “now successfully accessed the data stored on Farook’s iPhone and therefore no longer requires the assistance from Apple.”

F.B.I. investigators have begun examining the contents of the phone but would not say what, if anything, they have identified so far. A senior federal law enforcement official who spoke on the condition of anonymity said it was possible that law enforcement might not find anything useful on the phone.

Timothy D. Cook, Apple’s chief, defended the company’s battle with the government at an event last week.

The Justice Department also remained tight-lipped about how it was able to finally get into the smartphone after weeks of furious public debate.

A second law enforcement official who spoke on the condition of anonymity to reporters in a conference call said that a company outside the government provided the F.B.I. with the means to get into the phone used by Mr. Farook, which is an iPhone 5C running Apple’s iOS 9 mobile operating system. The official would not name the company or discuss how it was accomplished, nor would officials say whether the process would ultimately be shared with Apple.

Melanie Newman, a spokeswoman for the Justice Department, signaled in a statement that the broader battle over access to digital data from devices was not over.

“It remains a priority for the government to ensure that law enforcement can obtain crucial digital information to protect national security and public safety, either with cooperation from relevant parties, or through the court system when cooperation fails,” Ms. Newman said. “We will continue to pursue all available options for this mission, including seeking the cooperation of manufacturers and relying upon the creativity of both the public and private sectors.”“This case should never have been brought,” Apple said in a statement, adding that it would continue to help with law enforcement investigations.

Given that the F.B.I. may never tell Apple how it forced open the iPhone, the company also said that it would “continue to increase the security of our products as the threats and attacks on our data become more frequent and more sophisticated.”

Continued on Page 7

U.S. Says It Has Unlocked iPhone Without Apple

Continued from Previous Page

The conflict between Apple and the government erupted openly last month when a federal magistrate judge in California ordered the Silicon Valley company to help unlock the smartphone used by Mr. Farook. Timothy D. Cook, Apple's chief executive, opposed the court order in a public letter, saying that "compromising the security of our personal information can ultimately put our personal safety at risk."

The resistance led to heated rhetoric from both sides in dueling court filings, and the issue spurred debates — finding its way onto late night talk shows, and dividing the public. Apple and the Justice Department had been due in court last week in Riverside, Calif., and the case was seemingly headed toward appeals and even the Supreme Court.

Then last Monday, the Justice Department said it had been approached by a third party with a potential alternative method for opening the iPhone.

The Justice Department's cracking of the iPhone has implications for other cases that involve locked iPhones. Last month, a federal magistrate judge in the Eastern District of New York refused to grant an order, requested by the government, that asked Apple to extract data from an iPhone used by a drug dealer in Brooklyn. The Justice Department is in the process of appealing that decision.

The federal law enforcement official who spoke on the condition of anonymity to reporters on Monday said it was premature to say whether the method it used to open the phone in the San Bernardino case could be used on phones in other cases. The phone in the Brooklyn case was an iPhone 5S running the iOS 7 mobile software.

"Courts should be skeptical going forward when the government claims it has no other option besides compelling a device maker's assistance," said Riana Pfefferkorn, a cryptography fellow at the Stanford Center for Internet and Society.

"Now that the F.B.I. has accessed this iPhone, it should disclose the method for doing so to Apple," she added. "Apple ought to have the chance to fix that security issue, which likely affects many other iPhones."

Feds: TVA Executive Traded Nuclear Information for Cash in Chinese Espionage Case

SOURCE: By Jamie Satterfield of the Knoxville News Sentinel

The indictment consists of one count of conspiracy to illegally engage and participate in the production and development of special nuclear material outside the U.S. and one count of conspiracy to act in the U.S. as an agent of a foreign government.

An East Tennessean who served as a senior manager in the Tennessee Valley Authority's nuclear program swapped information with one of China's top nuclear power companies in exchange for cash, according to federal court records unsealed Thursday.

The U.S. Attorney's Office in Knoxville on Thursday announced an espionage conspiracy indictment against China General Nuclear Power, Chinese nuclear engineer Szuhsiung "Allen" Ho, and Ho's firm, Energy Technology International. Prosecutors said Ho conspired with the companies to lure nuclear experts in the U.S. into providing information to allow China to develop and produce nuclear material based on American technology and under the radar of the U.S. government.

Ho was taken into custody in Atlanta on Thursday afternoon and will be returned to U.S. District Court in Knoxville to face the two-count indictment. The indictment consists of one count of conspiracy to illegally engage and participate in the production and development of special nuclear material outside the U.S. and one count of conspiracy to act in the U.S. as an agent of a foreign government.

"Allen Ho, at the direction of a Chinese state-owned nuclear power company, allegedly approached and enlisted U.S. based nuclear experts to provide integral assistance in developing and producing special nuclear material in China," Assistant Attorney General for National Security John P. Carlin said in a news release. "Ho did so without registering with the Department of Justice as an agent of a foreign nation or authorization from the U.S. Department of Energy. Prosecuting those who seek to evade U.S. law by attaining sensitive nuclear technology for foreign nations is a top priority for the National Security Division."

Continued on Page 9

Feds: TVA Executive Traded Nuclear Information for Cash in Chinese Espionage Case

Continued From Previous Page

Among the six unidentified American co-conspirators listed in the indictment is a person labeled "U.S. Person 1," described as the TVA senior manager for the probabilistic risk assessment in the Nuclear Power Group from April 2010 to September 2014. The TVA executive was born in Taiwan and became a naturalized citizen in 1990, according to the indictment. A payment by Ho to the TVA executive was sent to Chattanooga, according to the indictment.

The TVA executive had the same role with the Florida Power & Light company before joining TVA and met Ho through the Chinese American Nuclear Technology Association in the early 1990s, according to the indictment. The executive's gender is not specified.

The indictment alleges Ho "entered into contracts with" the TVA executive and "other U.S.-based experts to provide assistance to" the Chinese-owned nuclear power company — one of the three largest in China — related to the "development and production of special nuclear material" in the People's Republic of China.

According to the indictment, the TVA executive provided Ho with Florida Power & Light "information regarding nuclear power plant outage times" in 2004 for use at China General's Daya Bay Nuclear Power Plant and provided consulting services to Daya Bay during that time.

The TVA executive in 2013 used TVA ties to access the nonprofit Electric Power Research Institute and provided China General with the nonprofit's reports on nuclear power that were supposed to be restricted to members of the research firm, according to the indictment.

The TVA executive traveled to China in November 2013 "to provide nuclear consulting" to China General and provided reports on fuel reliability for new nuclear plant design, technology innovation and a method to predict damage in power plant piping.

In December 2015, Ho sent the TVA executive a check to a Chattanooga address totaling $15,555 for services in 2013 and 2014, according to the indictment.

Continued on Page 10

Feds: TVA Executive Traded Nuclear Information for Cash in Chinese Espionage Case

Continued from Previous Page

Assistant U.S. Attorney Charles Atchley, who is spearheading the prosecution, is not required to list every act alleged as part of the conspiracy, so the full scope of the TVA executive's involvement is not yet known.

The indictment lists five other Americans as participating in the espionage conspiracy. They, too, are identified only by state of residency and job description. Four worked at the same Pennsylvania-based nuclear firm, which is not identified in the indictment, while the fifth worked for a Colorado-based firm that supplied technical support to the nuclear power industry. That firm also is not identified.

All five were engineers. Two were nuclear engineers living in Pennsylvania. Two lived in South Carolina, with one of those experts born in China before becoming a naturalized U.S. citizen. The fifth lived in Colorado. All were paid for providing Ho and China General with key information on various aspects of the production of special nuclear material — plutonium, uranium-233 and enriched uranium — according to the indictment.
Authorities did not say Thursday whether the engineers face prosecution or have struck deals to cooperate.

The indictment alleges the conspiracy spanned from 1997 to this month. The purpose was to "secure an advantage to China." Ho told the engineers that "China has the budget to spend" and needed help so "China will be able to design their nuclear instrumentation system independently and manufacture them independently after the project is completed," according to an email from Ho cited in the indictment.

The espionage count carries a maximum sentence of life in prison. According to a release, the FBI headed up the probe along with TVA's Office of the Inspector General, the DOE's National Nuclear Security Administration and the U.S. Immigration and Customs Enforcement Homeland Security Investigations.

In a Midwestern Cornfield, a Scene of Chinese Theft and Espionage

SOURCE: The Christian Science Monitor By Josh Kenworthy, Staff writer April 11, 2016

United States law enforcement agencies are urging farmers and businesses more broadly to be increasingly vigilant amid a rise in attempted thefts of genetically engineered seed and other commercial secrets.

The FBI and Justice Department has reported an increase in cases of agricultural espionage in the US.

Mo Hailong, one of six Chinese nationals US authorities accused in 2013 of digging up seeds from Iowa farms with plans to send them back to China, pleaded guilty in January, according to Reuters. Mr. Mo had his case prosecuted by the Justice Department as a matter of national security rather than a normal criminal case.

The FBI and Justice Department has reported a growing number of agricultural espionage cases in the past two years, including government research facilities, companies and research facilities. While the FBI says it knows of connections between the accused individuals and the Chinese government, it does not have evidence to prove the link that would stand up in court. The Chinese government denies it is involved.

The trend particularly highlights how highly coveted and vulnerable advanced food technology secrets are, particularly in China where 1.36 billion of earth's roughly 7 billion person population lives, Reuters said. However, while the Chinese government has indicated it wants to be a leader in the biotechnology world, there is also evidence to suggest this may be stymied by Chinese consumer wariness about the yet unknown problems that could stem from the consumption of genetically modified food.

Continued on Page 12

In a Midwestern Cornfield, a Scene of Chinese Theft and Espionage

Continued From Previous Page

US senators recently called for a review of state-owned ChemChina's $43 billion deal to buy Swiss seed group Syngenta, which generates nearly a quarter of its revenue from North America. From the Chinese government's point of view, such a deal would ease its concerns that foreign companies would control the supply of GM food in China.

However, Carl Pray, a Rutgers University economist who specializes in Chinese agriculture, told the Monitor that "it may not ease the concerns of consumers who are largely focused on food safety."

Agribusiness giant Monsanto says if the Chinese were to acquire GMO seeds and recreate a corn plant it would allow Chinese companies to bypass around eight years of research, which costs the company roughly $1.5 billion per year, Reuters reported.

The NCMS Society of Industrial Security Professionals
Carolina Chapter Sponsors...

Protecting your company in a Global Marketplace

Wednesday, September 21, 2016

SAVE THE DATE

Summit Details

The summit will be held at North Carolina National Guard (NCNG) Joint Forces Headquarters (JFHQ). Located at: 4105 Reedy Creek Rd, Raleigh, NC 27607.

Registration: 7:45 a.m. | Conference: 8:30 a.m. until 4:00 p.m.

Cost: $20, which will include a boxed lunch and refreshments throughout the day.

Key Note Speakers

Michael J. "Mike" Rogers, CNN National Security Commentator

Mike was the U.S. Representative for Michigan's 8th congressional district, serving from 2001–2015. Congressman Rogers served as the Chairman of the Permanent Select Committee on Intelligence from 2011 until he left office in 2015. He graduated from Adrian College, Adrian, Michigan in 1985, from which he earned a bachelor's degree in Criminal Justice and Sociology, and served in the United States Army from 1985 to 1989. He worked as a Special Agent with the Federal Bureau of Investigation in its Chicago office, specializing in organized crime and public corruption, 1989–1994.

Frank W. Abagnale, Forgery, Embezzlement, and Secure Document Subject Matter Specialist

Frank is one of the world's most respected authorities on the subjects of forgery, embezzlement and secure documents. For over forty years he has lectured to and consulted with hundreds of financial institutions, corporations, and government agencies around the world.

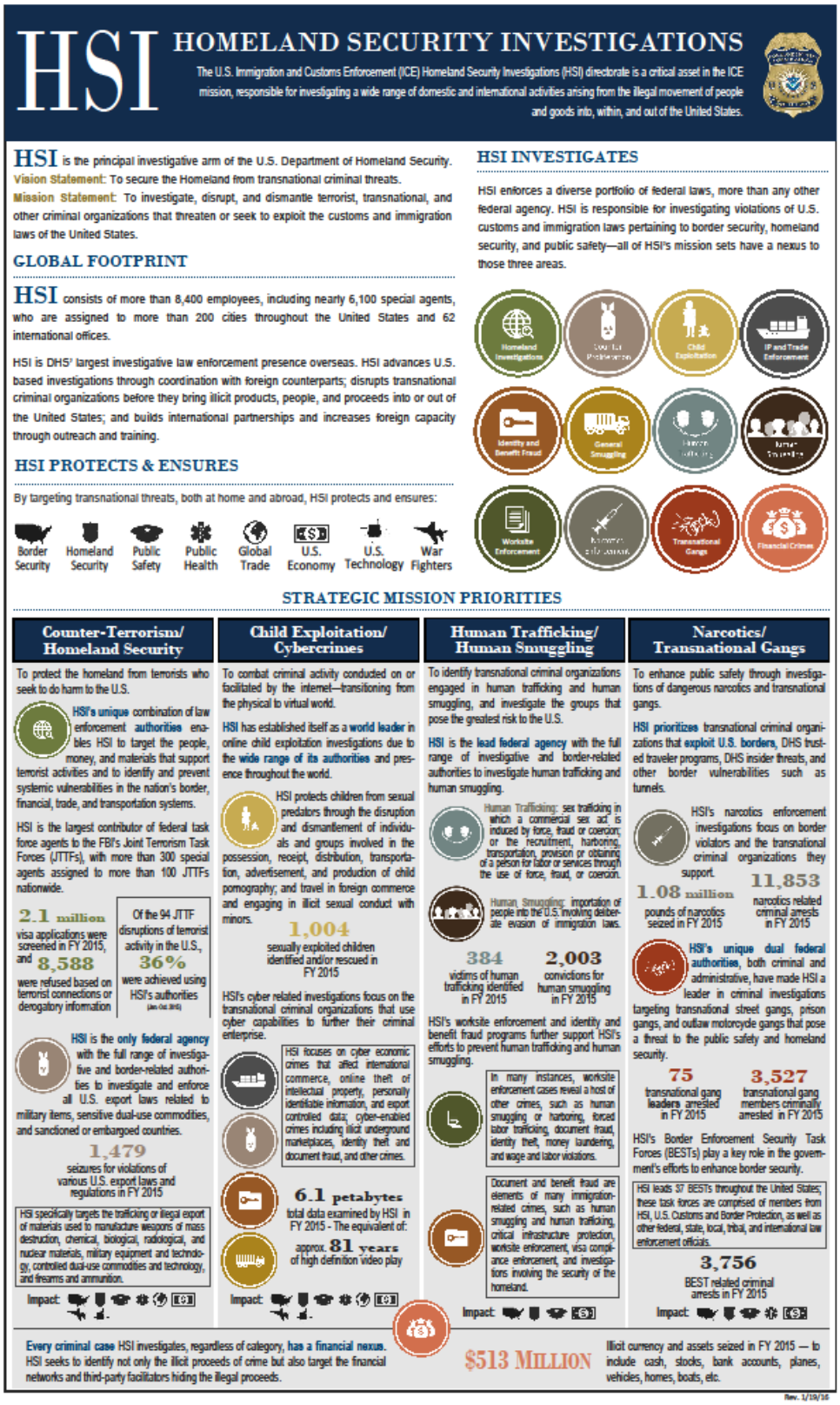
Mr. Abagnale has been associated with the FBI for over four decades. He lectures extensively at the FBI Academy and for the field offices of the Federal Bureau of Investigation. He is a faculty member at the National Advocacy Center (NAC) which is operated by the Department of Justice, Executive Office for U.S. Attorneys. More than 14,000 financial institutions, corporations and law enforcement agencies use his fraud prevention programs. In 1998, he was selected as a distinguished member of "Pinnacle 400" by CNN Financial News. Today Mr. Abagnale is a member of the Board of Editors for Bank Fraud and IT Security, as well as the Financial Fraud Law Report. Mr. Abagnale's early life was portrayed by Leonardo DiCaprio in the 2002 feature film Catch Me If You Can, also starring Tom Hanks.

Seating is limited - registration is currently open -

Visit https://www.eventbrite.com/e/3rd-annual-nc-red-dart-security-summit-tickets-24497532780

RED DART Agency Spotlight

The RED DART Agency Spotlight will continue to feature an overview of each partner agency and their mission. Local RED DART partners may vary depending on location.



REDDART

Tip of the Month

U.S. Department of Justice
Federal Bureau of Investigation

Intellectual Property Protection

Safeguard Your Company's Trade Secrets, Proprietary Information and Research

Information That Could Be Targeted:

- Proprietary formulas and processes
- Prototypes or blueprints
- Research
- Technical components and plans
- Confidential documents
- Computer access protocols
- Passwords
- Employee data
- Manufacturing plans
- Equipment specifications
- Vendor information
- Customer data
- Access control information
- Computer network design
- Software (including source codes)
- Phone directories
- Hiring/Firing strategies and plans
- Negotiation strategies
- Sales forecasts
- Pricing strategies
- Corporate strategies
- Marketing strategies
- Acquisition strategies
- Budget estimates/ expenditures
- Corporate financial data
- Investment data

Domestic and foreign companies may try to illegally acquire your company's information. Foreign nations that seek to improve their economies and militaries target US technology companies.

Protect the programs and systems that support what makes your company successful and unique. If your company has a technological edge, expect your technology, and those with access to it, to be targeted. If your company has developed a process to manufacture an item at less cost than others, that manufacturing process may be targeted. If your company is negotiating with another company or country, the negotiators and negotiation strategy may be targeted. If your company has invested time and resources developing a product or idea—**Protect It!**

Common Tactics:

- Computer hacking! (Electronic-device hacking)
  - A visitor connects an electronic device to your system, such as a thumb drive, that adds malware or downloads your information
  - Someone hacks into your network via a spear phishing attack
  - An unattended laptop is accessed or stolen
- On-site visits to your company:
  - Unauthorized photography or computer access
  - Unauthorized entry into restricted areas
  - Asking questions outside the scope of the visit
- Review of publicly available sources. Are you sharing too much information?
- Obtains your surplus equipment. Thousands of pages of stored information may still reside in the memory of a copier, printer, fax machine, etc.
- Employment solicitation (try to hire your key employees)
- Theft or unauthorized photography of products at trade shows
- Burglary (including copying of restricted documents where the originals stay in-house)
- Dumpster diving – finding information in your company's trash
- Joint ventures
- Front companies
- Unsolicited requests for information
- Elicitation – developing a friendship with an employee with the intention of obtaining restricted data or products. The employee will see someone who appears non-threatening and interested in his/her work.
- Electronic surveillance (listening devices in your hotel room, cell-phone hacking, etc.)

Theft of Intellectual Property Could Result In:

- Lost revenue
- Lost employment
- Damaged reputation
- Health and safety concerns from counterfeit products
- Lost investment for research (R&D)
- Delays or interruption in production

Tip of the Month

Intellectual Property Protection

Who Might Steal Your Intellectual Property?

- Domestic and foreign commercial rivals
- Domestic and foreign start-up companies
- Foreign intelligence officers (spies)
- Disgruntled employees
- Opportunists (lone wolves)
- Organized criminals

Insider Threats

Look for warning signs that an employee may be gathering and passing information outside your company.

Foreign Travel

When traveling to a foreign country, you and your company's information are at greater risk.

- Many foreign countries do not have legal restrictions against technical surveillance.
- Some foreign governments help their domestic corporations collect competitive intelligence.

Protection Strategies

- Assess your company's information security vulnerabilities and fix or mitigate the risks associated with those vulnerabilities.
- Do not store private information vital to your company on any device that connects to the Internet.
- Use up-to-date software security tools. Many firewalls stop incoming threats, but do not restrict outbound data. Competitive intelligence hackers try to retrieve data stored on your network.
- Educate employees on spear phishing email tactics. Establish protocols for quarantining suspicious email.
- Ensure your employees are aware of and are trained to avoid unintended disclosures.
- Remind employees of security policies on a regular basis through active training and seminars. Use signs and computer banners to reinforce security policies.
- Document employee education and all other measures you take to protect your intellectual property.
- Ensure human resource policies are in place that specifically enhance security and company policies. Create clear incentives for adhering to company security policies.
- Ask the FBI or other security professionals to provide additional awareness training. The FBI can provide a vulnerability self-assessment tool.

Contact Law Enforcement

You are ultimately responsible for protecting your own intellectual property. Congress has continually expanded and strengthened criminal laws for violations of intellectual property rights to protect innovation; however, you need to take reasonable steps to protect your intellectual property and products, and document those measures.

Violations that may apply: Economic Espionage, Theft of Trade Secrets, Mail Fraud, Wire Fraud, Interstate Transportation of Stolen Property, Export Control, and Intellectual Property Rights.

If you believe your company is a victim of these crimes, contact the FBI or the National Intellectual Property Rights Coordination Center. Investigators cannot act if they are not aware of the problem. The FBI will minimize the disruption to your business, and safeguard your privacy and your data during its investigation. Where necessary, the FBI will seek protective orders to preserve trade secrets and business confidentiality.

Safeguard Your Company's Trade Secrets, Proprietary Information and Research

www.fbi.gov www.ice.gov/iprcenter

Current RED DART Teams:

- RED DART North Carolina
- RED DART Southern Virginia
- RED DART Huntsville
- RED DART Central Virginia
- RED DART Gulf Coast
- RED DART South Carolina
- RED DART Chicago
- RED DART North Texas
- RED DART North Mississippi
- RED DART Indiana
- RED DART South Florida
- RED DART Tennessee
- RED DART Colorado
- RED DART Sacramento
- RED DART Silicon Valley

The stated purpose of the RED DART program is to create a unified, cross- agency team of counterintelligence professionals dedicated to the protection of classified and sensitive technology research throughout a given area of responsibility (AOR). RED DART operates under a "shared leadership" principle, which allows each partner agency to own the program while being responsible and responsive to the other partner agencies.

Contact your servicing RED DART representative for additional information on the articles and information contained in this newsletter.

New RED DART teams are forming regularly throughout the U.S. Contact your servicing Defense Security Service (DSS) CI agent or Federal Bureau of Investigation (FBI) CI agent to see if a team is being established in your area.