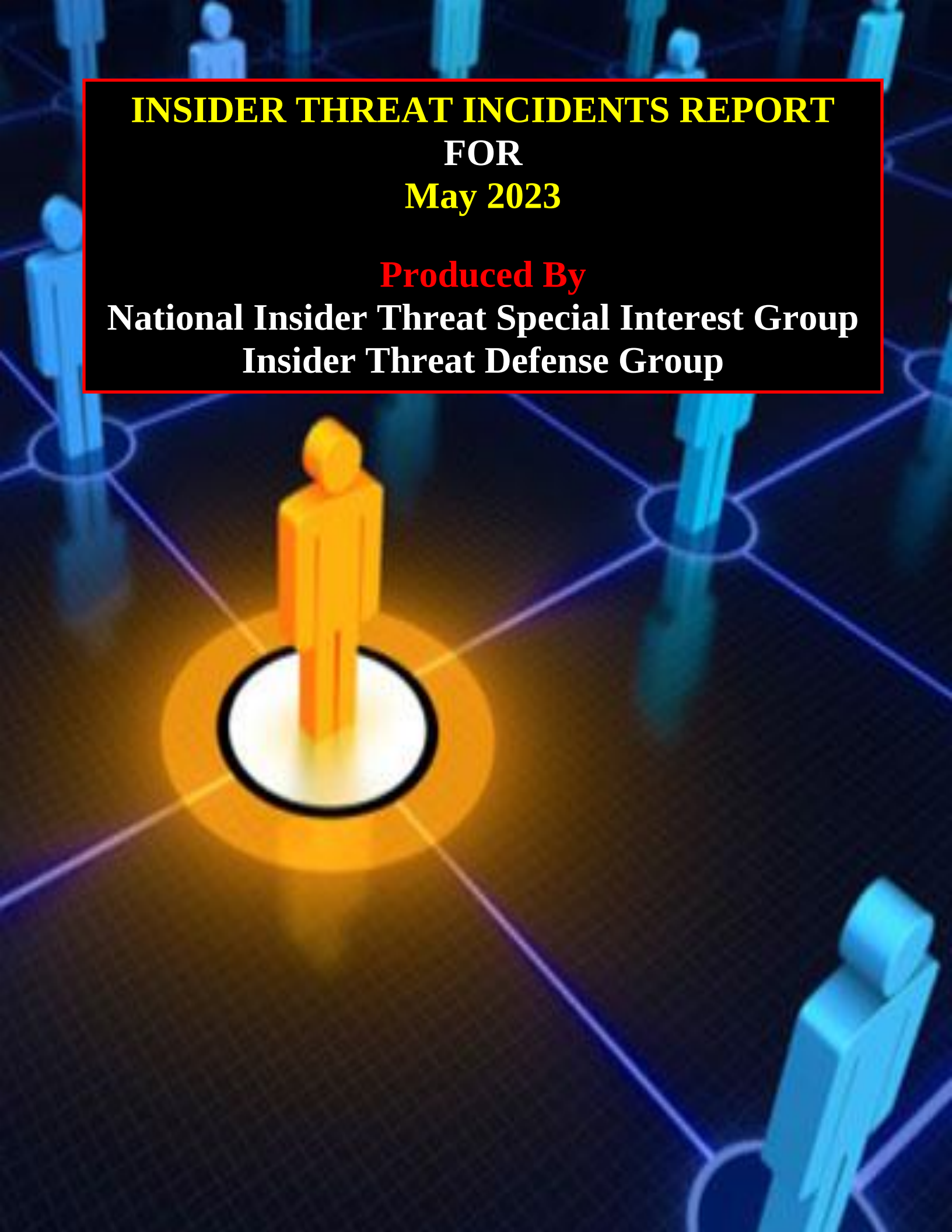


INSIDER THREAT INCIDENTS REPORT
FOR
May 2023

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

INSIDER THREAT INCIDENTS

A Very Costly And Damaging Problem

For many years there has been much debate on who causes more damages (Insiders Vs. Outsiders). While network intrusions and ransomware attacks can be very costly and damaging, so can the actions of employees' who sit behind firewalls or telework through firewalls. Another problem is that Insider Threats lives in the shadows of Cyber Threats, and does not get the attention that is needed to fully comprehend the extent of the Insider Threat problem.

The National Insider Threat Special Interest Group (NITSIG) in conjunction with the Insider Threat Defense Group (ITDG) have conducted extensive research on the Insider Threat problem for 10+ years. This research has evaluated and analyzed over **4,400+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations and businesses of all sizes.

The NITSIG and ITDG maintain the largest public repositories of Insider Threat incidents, and receive a great deal of praise for publishing these incidents on a monthly basis to our various websites. This research provides interested individuals with a "***Real World***" view of the how extensive the Insider Threat problem is.

The traditional norm or mindset that Malicious Insiders just steal classified information, an organizations data, trade secrets or other sensitive information, is no longer the case. Over the years there has been a drastic increase in financial fraud and embezzlement committed by employees'.

According to the Association of Certified Fraud Examiners 2022 Report to the Nations, organizations with less than 100 employees' suffered larger median losses than those of larger companies.

To grasp the magnitude of the Insider Threat problem, one most look beyond Insider Threat surveys, reports and other sources that all define Insider Threats differently. How Insider Threats are defined and reported is not standardized, so this leads to significant underreporting on the Insider Threat problem.

Another problem is how surveys and reports are written on the Insider Threat problem. Some simply cite percentages of how they have increased and the associated remediation costs over the previous year. In many cases these surveys and reports only focus on the technical aspects of an Insider stealing data from an organization, and leave out many other types of Insider Threats. Surveys and reports that are limited in their scope of reporting do not give the reader a comprehensive view of the "***Actual Malicious Actions***" employees' are taking against their employers.

If you are looking to gain support from your CEO and C-Suite for detecting and mitigating Insider Threats, and want to provide them with the justification, return on investment, and funding ($$$) needed for developing, implementing and managing an ITP, the incidents listed on pages 5 to 28 of this report should help. The cost of doing nothing, may be greater then the cost of implementing a comprehensive Insider Threat Mitigation Framework.

DEFINITIONS OF INSIDER THREATS

The definition of Insider Threats can be vast, and must go beyond current definitions (By Sources Such As: National Insider Threat Policy, NISPOM CC2 & Other Sources) and be expanded.

While other organizations have definitions of Insider Threats, they can also be limited in their scope.

TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH

- ☐ Non-Malicious But Damaging Insiders (Un-Trained, Careless, Negligent, Opportunist, Job Jumpers, Etc.)
- ☐ Disgruntled Employees' Transforming To Insider Threats
- ☐ Theft Of Organizations Assets (Physical, Etc.)
- ☐ Theft / Disclosure Of Classified Information (Espionage), Trade Secrets, Intellectual Property, Research / Sensitive - Confidential Information
- ☐ Stealing Personal Identifiable Information For The Purposes Of Bank / Credit Card Fraud
- ☐ Financial / Bank / Wire / Credit Card Fraud, Embezzlement, Theft Of Money, Money Laundering, Overtime Fraud, Contracting Fraud, Creating Fake Shell Companies To Bill Employer With Fake Invoices
- ☐ Employees' Involved In Bribery, Kickbacks, Blackmail, Extortion
- ☐ Data, Computer & Network Sabotage / Misuse
- ☐ Employees' Working Remotely Holding 2 Jobs In Violation Of Company Policy
- ☐ Employees' Involved In Viewing / Distribution Of Child Pornography And Sexual Exploitation
- ☐ Employee Collusion With Other Employees', Employee Collusion With External Accomplices / Foreign Nations, Cyber Criminal - Insider Threat Collusion
- ☐ Trusted Business Partner Corruption / Fraud
- ☐ Workplace Violence(WPV) (Bullying, Sexual Harassment Transforms To WPV, Murder)
- ☐ Divided Loyalty Or Allegiance To U.S. / Terrorism
- ☐ Geopolitical Risks (Employee Loyalty To Company Vs. Country Because Of U.S. - Foreign Nation Conflicts)

ORGANIZATIONS IMPACTED

TYPES OF ORGANIIZATIONS THAT HAVE EXPERIENCED INSIDER THREAT INCIDENTS

- ☐ U.S. Government, State / City Governments
- ☐ Department of Defense, Intelligence Community Agencies, Defense Industrial Base Contractors
- ☐ Critical Infrastructure Providers
  - Public Water / Energy Providers / Dams
  - Transportation, Railways, Maritime, Airports, Aviation / Airline Industry (Pilots, Flight Attendants)
  - Health Care Industry, Medical Providers (Doctors, Nurses, Management), Hospitals, Senior Living Facilities, Pharmaceutical Industry
  - Banking / Financial Institutions
  - Food & Agriculture
  - Emergency Services
  - Manufacturing / Chemical / Communications
- ☐ Law Enforcement / Prisons
- ☐ Large / Small Businesses
- ☐ Defense Contractors
- ☐ Schools, Universities, Research Institutes
- ☐ Non-Profits Organizations, Churches, etc.
- ☐ Labor Unions (Union Presidents / Officials)
- ☐ And Others

INSIDER THREAT DAMAGES / IMPACTS

The Damages From An Insider Threat Incident Can Many:

Financial Loss

- ☐ Intellectual Property Theft (IP) / Trade Secrets Theft = Loss Of Revenue
- ☐ Embezzlement / Fraud (Loss Of $$$)
- ☐ Stock Price Reduction

Operational Impact / Ability Of The Business To Execute Its Mission

- ☐ IT / Network Sabotage, Data Destruction (Downtime)
- ☐ Loss Of Productivity
- ☐ Remediation Costs
- ☐ Increased Overhead

Reputation Impact

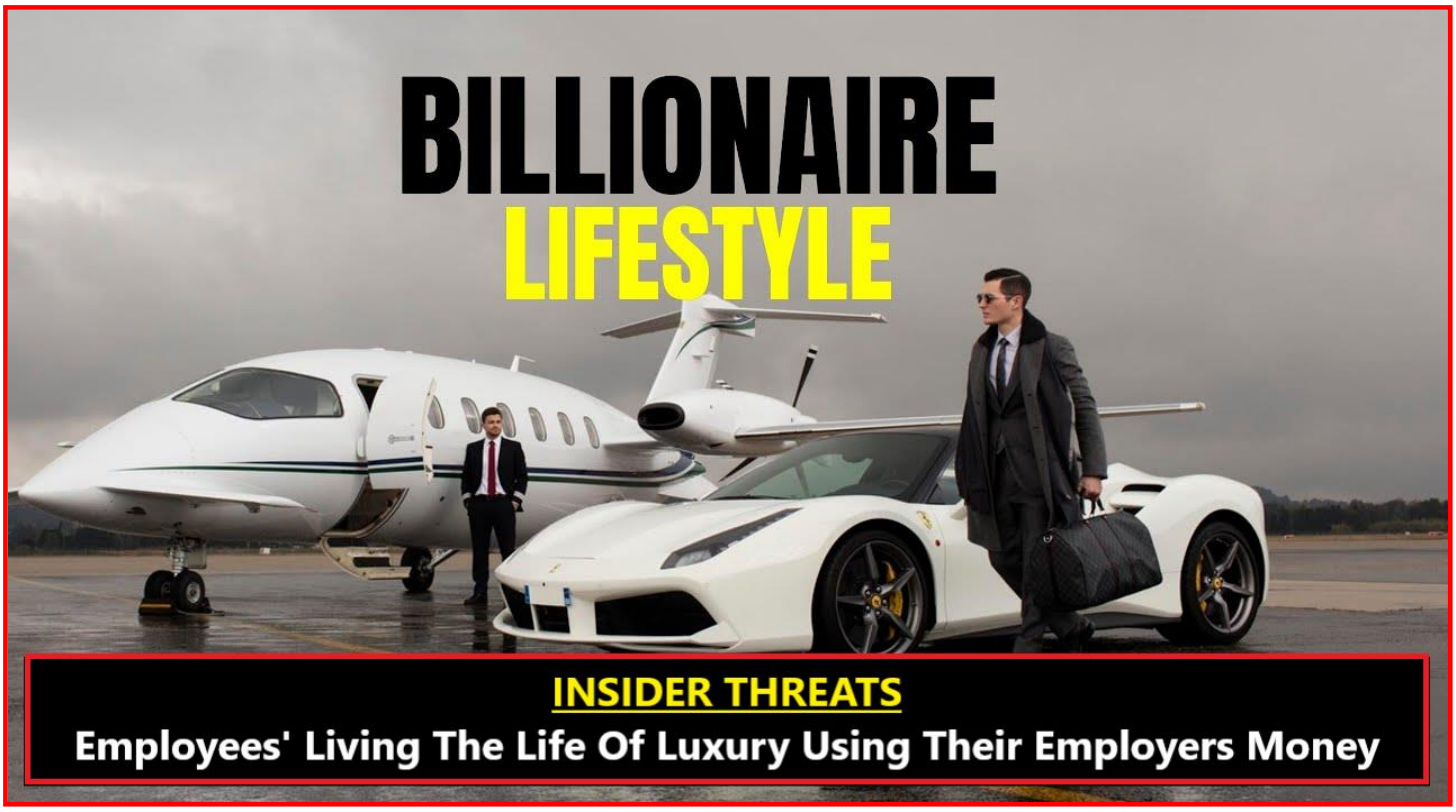
- ☐ Public Relations Expenditures
- ☐ Customer Relationship Loss
- ☐ Devaluation Of Trade Names
- ☐ Loss As A Leader In The Marketplace

Workplace Culture - Impact On Employees'

- ☐ Increased Distrust
- ☐ Erosion Of Morale
- ☐ Additional Turnover
- ☐ Workplace Violence (Deaths) / Negatively Impacts The Morale Of Employees'

Legal & Liability Impacts (External Costs)

- ☐ Compliance Fines
- ☐ Breach Notification Costs
- ☐ Increased Insurance Costs
- ☐ Attorney Fees
- ☐ Employees' Loose Jobs / Company Goes Out Of Business



NITSIG research indicates many employees may not be disgruntled, but have other motives such as financial gain to live a better lifestyle, etc.

You might be shocked as to what employees do with the money they steal or embezzle from organizations and businesses, and how many years they got away with it, until they were caught. (1 To 20 Years)

What Do Employees' Do With The Money They Embezzle / Steal From Federal / State Government Agencies & Businesses Or With The Money They Receive From Bribes / Kickbacks?

They Have Purchased:
Vehicles, Collectible Cars, Motorcycles, Jets, Boats, Yachts, Jewelry, Buy Properties & Businesses

They Have Used Company Funds / Credit Cards To Pay For:
Rent / Leasing Apartments, Furniture, Monthly Vehicle Payments, Credit Card Bills / Lines Of Credit, Child Support, Student Loans, Fine Dining, Wedding, Anniversary Parties, Cosmetic Surgery, Designer Clothing, Tuition, Travel, Renovate Homes, Auto Repairs, Fund Shopping / Gambling Addictions, Fund Their Side Business / Family Business, Buying Stocks, Firearms, Ammunition & Camping Equipment, Pet Grooming, And More.....

They Have Issued Company Checks To:
Themselves, Family Members, Friends, Boyfriends / Girlfriends

INSIDER THREAT INCIDENTS
FOR MAY 2023

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

United Kingdom

IT Employee Impersonates Ransomware Gang To Extort Employer - May 23, 2023

Ashley Liles worked as an IT Security Analyst at an Oxford based company that suffered a ransomware attack.

Due to his role in the company, Liles took part in the internal investigations and incident response effort, which was also supported by other members of the company and the police.

However, during this phase, Liles is said to have attempted to enrich himself from the attack by tricking his employer into paying him a ransom instead of the original external attacker.

Liles accessed a board member's private emails over 300 times as well as altering the original blackmail email and changing the payment address provided by the original attacker.
The plan was to take advantage of the situation and divert the payment to a cryptocurrency wallet under Liles' control. Liles also created an almost identical email address to the original attacker and began emailing his employer to pressurize them to pay the money.

However, the company owner wasn't interested in paying the attackers, and the internal investigations that were still underway at the time revealed Liles' unauthorized access to private emails, pointing to his home's IP address.

Liles realized the investigations closed in on him, and had wiped all data from his personal devices by the time police stormed into Liles' home to seize his computer it was still possible to restore incriminating data. (Source)

U.S. GOVERNMENT

Congressman George Santos Charged With Fraud, Money Laundering, Theft of Public Funds And False Statements - May 10, 2023

George Santos a United States Congressman representing the Third District of New York, was charfed with seven counts of wire fraud, three counts of money laundering, one count of theft of public funds, and two counts of making materially false statements to the House of Representatives.

Beginning in September 2022, during his successful campaign for Congress, Santos operated a limited liability company (Company #1) through which he allegedly defrauded prospective political supporters. Santos enlisted a Queens-based political consultant (Person #1) to communicate with prospective donors on Santos's behalf. Santos allegedly directed Person #1 to falsely tell donors that, among other things, their money would be used to help elect Santos to the House, including by purchasing television advertisements. In reliance on these false statements, two donors (Contributor #1 and Contributor #2) each transferred $25,000 to Company #1's bank account, which Santos controlled.

Shortly after the funds were received into Company #1's bank account, the money was transferred into Santos's personal bank accounts, and in one instance laundered through two of Santos's personal accounts. Santos allegedly then used much of that money for personal expenses. Among other things, Santos allegedly used the funds to make personal purchases
for designer clothing, to withdraw cash, to discharge personal debts, and to transfer money to his associates. (Source)

Former Small Business Administration Employee Sentenced To Prison For Role In $11 Million+ COVID Relief Fraud Scheme - May 25, 2023

Lakeith Faulkner was an employee of the Small Business Administration (SBA). He used his position to assist borrowers in submitting over $11 Million worth of fraudulent loan applications for Economic Injury Disaster Loans, which were intended to help small businesses recover from the economic impacts of the COVID-19 pandemic. In return for his assistance in submitting the fraudulent loan applications, those borrowers paid Faulkner and his co-defendant, Norman Beckwood, $2.3 Million. (Source)

Former IRS Revenue Agent And 5 Five Other Individuals Charged In $3 Million COVID Fraud Scheme - May 10, 2023

The U.S. Attorney's Office charged six defendants with a variety of crimes in connection with an alleged scheme to obtain millions of dollars by submitting fraudulent loan applications through the U.S. government's Payroll Protection Program (PPP).

Central to the allegations in the charging documents is the role of Frank Mosley a former IRS Revenue Agent and current City of Oakland Tax Enforcement Officer. Mosley conspired with others to submit fraudulent PPP-loan applications and then, after securing the proceeds from the loans, used his share of the illegally-obtained proceeds for personal investments and expenses. The defendants, including Mosely, received approximately $3 million as a result of submitting fraudulent loan applications under the PPP program. (Source)

Department Of Energy Procurement Officer Paid $18,000+ In Bribes For $960,000+ Worth Of Contracts - May 3, 2023

Michael Montenes the owner of M.S. Hi-Tech, Incorporated (MSHT), a Hauppauge-based distributor of electronic components, pleaded guilty to a criminal information charging him with bribery of a federal official in connection with a scheme to pay more than $18,000 to a Department of Energy (DOE) Procurement Officer in exchange for approximately $969,000 in DOE contracts.

Between approximately December 2017 and December 2020, Montenes paid a Procurement Officer (Co-conspirator 1), who was employed at a DOE laboratory in Virginia approximately $18,800 in bribes to induce Co-conspirator 1 to enter into contracts for electronic components that MSHT, supplied to the DOE's Virginia laboratory. Montenes mailed these payments, which ranged from $500 to $7,200, from Long Island to Co-conspirator 1 in Virginia. During the bribery scheme, Co-conspirator 1 awarded contracts worth more than $969,000 to MSHT, which represented 95% of all of MSHT's sales to the DOE's Virginia laboratory. In July 2021, some of the electronic components that MSHT sold to DOE based upon Montenes's bribes failed and caused a fire, resulting in approximately $1.8 million in repairs and other costs to DOE. (Source)

Former IRS Employee Sentenced To Prison for Scheme To Defraud IRS Of $190,000+ And Commit Identity Theft - May 8, 2023

Deena Lan was sentenced today to four years and six months in prison and ordered to pay $191,597 in restitution following her convictions for preparing and filing false tax returns for other individuals, underreporting her own taxable income on her personal tax returns, and committing wire fraud and aggravated identity theft.

From 2012 through 2016, Lee, in her role as a tax preparer, put materially false information on customers' tax returns without their knowledge or consent and submitted the returns to the IRS. As part of the scheme, Lee obtained the identification of multiple individuals and falsely listed these individuals as child care providers on multiple customers' tax returns without their knowledge or consent. (Source)

Former U.S. Postal Service Supervisor Charged With Misappropriation Of $65,000 Of Postal Funds For Personal Use - May 17, 2023

Austin Mahan is charged with misappropriating approximately $65,000 in postal funds.

For approximately six months in 2022 and 2023 Mahan worked as a U.S. Postal Service (USPS) Supervisor.

At various times Mahan misused USPS credit cards to make personal purchases at various retail stores in and around New Jersey. These purchases included tens of thousands of dollars' worth of gift cards as well as various home décor items, home renovation materials, power and handheld tools, tool storage equipment, and personal items such as a Dyson cordless vacuum, LED fog light bulbs for Mahan's personal vehicle, batteries, shampoo, shaving cream, food products and other items. (Source)

Former U.S. Postal Service Office Employee Sentenced To Probation For Misappropriation Of $26,000+ Of USPS Funds / Used Funds For Herself And Family - May 10, 2023

Megan Torrez was employed by the U. S. Postal Service in June 2021, as a Postal Support Employee in Nelson, Wisconsin. Her assigned duties included conducting postal business with the public and performing financial accounting functions to report the sales of postage, money orders and other items. When postage and money order stock were sold, she was responsible for collecting money from those sales and remitting that money to the bank.

Between August 2021 and February 2022, Torrez manipulated postal funds accessible to her in her position at the post office by issuing postal money orders to herself and family members and paying with personal checks that she admitted had insufficient funds to clear her bank. Postal money orders may only be purchased with cash, debit card, or traveler's check, and no personal checks are accepted by the Postal Service.

In January 2022, the Office of Inspector General received information about the checks written by Torrez to the Postal Service that were returned as "non-sufficient funds." At the time of their investigation, thirty-two checks were outstanding for over $26,000 in postal money orders. The money orders that Torrez issued to herself and her family were used to pay for her family's personal expenses. Torrez claimed that her decision to use postal funds to pay for her family's bills was out of desperation when her husband lost his job during the pandemic. (Source)

Former U.S. Postal Carrier Sentenced To Prison For Role In Distributing Cocaine Packages - May 24, 2023

Michelle Prieto is a former United States Postal Carrier.

Prieto and her co-defendant, Angel Coss, orchestrated a scheme by which Prieto provided addresses on her delivery route to Coss who used those addresses to secure shipments of cocaine from Puerto Rico. As a result, kilogram quantities of cocaine were shipped in packages to these addresses. Prieto then removed the packages from the mail stream and provide them to Coss who then distributed the cocaine. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Former Air Force Civilian Employee Sentenced To Prison To $2.3 Million+ Bribery And Government Contract Fraud Scheme Over 11 Years - April 25, 2023

Keith Seguin, a former civilian employee at Randolph Air Force Base in San Antonio, admitted to receiving millions of dollars in bribes in connection with a government contract fraud scheme that spanned more than a decade and impacted hundreds of millions of dollars in contract awards.

According to formal charges, the QuantaDyn Corporation, a software engineering company based in Ashburn, Virginia; its owner, David Bolduc; Rubens Lima and Seguin all conspired to secure government contracts. Seguin used his position to steer lucrative contracts and sub-contracts to QuantaDyn for aircraft and close-air-support training simulators. Seguin, who was intimately involved in the government contracting process, leaked confidential competitor proposals to a prime contractor who would then subcontract the work to QuantaDyn. He also leaked confidential government budget information to prime contractors and to QuantaDyn, enabling them to maximize profits at government expense. Seguin admitted to accepting more than $2.3 million in bribes from Bolduc and QuantaDyn from 2007 to 2018. (Source)

Former Army Employee Charged For Theft Of $800,000+ Of Military Heavy Equipment - May 10, 2023

From a time unknown but no earlier than November 1, 2021, and continuing through approximately December 31, 2021, Tamilo Fe'a stole military heavy equipment, including vehicles, semi-trailers, generator trailers, flatbed trailers, refrigerator trailers, armored office trailers, tractors, and box vans from the Hawthorne Army Weapons Depot in Hawthorne, Nevada.

The total value of the stolen property was over $800,000.00. From September 2020 to August 2021, Fe'a made about 69 transactions with a fuel fleet credit card for his personal benefit at various gas stations in Nevada, Arizona, New Mexico, and California. (Source)

3 Individuals (2 Of Them Police Officers) Are Charged In Role With Conspiracy To Steal Government Property From Army Depots - May 25, 2023

Kelvin Battle, Steve Bonner and Shane Farthing are each charged with one count of conspiracy to steal United States property. Battle and Bonner are also each charged with an additional count related to specific instances of stealing or selling property stolen from the Anniston Army Depot (ANAD). Six other individuals have pleaded guilty or agreed to plead guilty to offenses related to the theft of property from ANAD.

Battle and Farthing, who were police officers at ANAD, and other civilian employees of the Directorate of Emergency Services stole military property from warehouses at ANAD. Bonner acted as a middleman, selling stolen property directly to buyers and delivering stolen property to the owner of a military surplus store in Sylacauga. The stolen items included equipment that was designed to be attached to military weapon systems to provide operators with instant nighttime engagement capabilities and/or improved target acquisition. (Source)

CRITICAL INFRASTRUCTURE

Former Sewage & Water Board Official Charged With Theft Of Cash - May 25, 2023

James Arnold is the former Utility Services Administrator for the Sewerage and Water Board of New Orleans.

Arnold is accused of stealing cash that belonged to the Sewerage and Water Board. Arnold would instruct plumbers to provide him with payments for plumbing permits and that Arnold would keep the payments for his own use. (Source)

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

Former Homeland Security Investigations Special Agent Convicted Of Maintaining Corrupt Relationship W/ Confidential Informant (CI) - Was Paid $50,000 By CI - May 5, 2023

Anthony Sabaini was assigned to Homeland Security Investigations (HSI's) field office in Oakbrook Terrace, Ill.

Sabaini maintained a corrupt relationship with an HSI confidential informant (CI). Sabaini tipped off the CI to sensitive law enforcement investigations and protected the CI from other federal law enforcement investigations conducted by the FBI and DEA. In exchange for Sabaini's protection, the CI paid Sabaini at least approximately $50,000. The evidence showed that Sabaini stole money from HSI that was earmarked for investigative activity. He also stole cash from drug dealers.

Evidence at trial revealed that Sabaini deposited more than $250,000 in cash into a bank account for which he was the sole signatory. He made the deposits through more than 162 transactions, with the amount of each deposit being less than $10,000. The deposits were structured in an effort to evade federal reporting rules, which require financial institutions to notify the U.S. Department of the Treasury about transactions of more than $10,000.

The evidence also showed that Sabaini lied in official HSI memoranda in 2017 and 2018 to protect his corrupt relationship with the CI.

In the memoranda, Sabaini knowingly covered up material facts, including that the CI was a target of ongoing criminal investigations conducted by other law enforcement agencies, and that the CI had recently engaged in unauthorized criminal conduct that Sabaini knew would have affected his suitability as a paid HSI informant. (Source)

U.S. Border Patrol Agent Charged With Attempting To Distribute Methamphetamine And Receiving $25,000 In Bribes - May 11, 2023

U.S. Border Patrol Agent Hector Hernandez agreed to accept $25,000 in bribes to distribute methamphetamine and to open a restricted border gate to allow unauthorized migrants to illegally enter the United States.

The complaint alleges that on May 8, 2023, Hernandez opened a restricted border gate while on duty as part of an agreement to allow an unauthorized migrant to enter the United States from Mexico in exchange for a $5,000 cash payment to Hernandez. Hernandez was unaware that he'd made that agreement with an undercover federal agent.

Then, on May 9, 2023, in exchange for another cash payment, Hernandez arranged to pick up a duffle bag loaded with methamphetamine from a storm drain near the border fence while on duty. According to the complaint, Hernandez put the bag into his Border Patrol vehicle and drove it to his house in Chula Vista, where he stored it for the remainder of his shift.

In the morning on May 10, 2023, Hernandez retrieved the bag and met with the undercover agent intending to deliver the drugs in return for an expected $20,000 cash payment, the complaint said. At that meeting, after delivering the drugs, Hernandez was arrested. (Source)

Former Sheriff's Office Employee Charged With Theft Of $150,000+ - May 11, 2023

From July 2018 to September 2022, while employed at the West Baton Rouge Parish Sheriff's Office, Mandy Miller stole cash paid for traffic tickets and hid the thefts by recording fraudulent journal entries in the Sheriff's Office accounting system.

In all, it is alleged that Miller embezzled, stole, and otherwise without authority, knowingly converted to her own use more than $150,000 in official funds. (Source)

STATE / CITY GOVERNMENTS / MAYORS

Former State Contractor Pleads Guilty To $550,000+ Fraudulent Unemployment Insurance Scheme - May 3, 2023

Autumn Mims worked with the State of Michigan Unemployment Insurance Agency (MUIA)

In August 2020, she began using her access to fraudulently process claims in the names of third parties without their knowledge or authorization. As part of the scheme, Mims personally (1) altered third-party contact information for unemployment insurance assistance; (2) accessed third-party unemployment insurance assistance claim information without authorization; (3) authenticated unauthorized access attempts for third-party unemployment insurance assistance information; (4) dismissed fraud prevention triggers and information requests relating to third-party unemployment insurance assistance; (5) conducted cash withdrawals of unemployment insurance assistance issued in the names of third parties; and, (6) conducted financial transactions utilizing unemployment insurance assistance funds issued in the names of third parties.

Mims also admitted that while she was working with the MUIA and executing her fraud, she was also fraudulently obtaining unemployment insurance benefits for herself by falsely claiming that she was unemployed.

As a result of the conspiracy, over $550,000 in fraudulent unemployment assistance payments were made by the State of Michigan. (Source)

Former Garbage Company Executive Pleads Guilty To Paying $55,000+ In Bribes To Department of Public Works Director - May 3, 2023

John Porter pleaded guilty in court in San Francisco to conspiring to commit honest services mail and wire fraud, admitting that he participated in a scheme with another Recology executive to bribe the former head of the San Francisco Department of Public Works, Mohammed Nuru.

Porter is the former Vice President and Group Manager of the Recology Group. Porter paid bribes to influence Nuru. The bribes included $55,000 in payments for holiday parties Nuru hosted for friends, political supporters, and select DPW employees, from October 2017 through January 2020. (Source)

Former Department Of Public Works Employee Pleads Guilty To Role In Fraud Scheme That Involved Boyfriend - May 9, 2023

Shaun Lindsey was used her position within the City of Richmond Department of Public Works (DPW) to steer governmental contract awards towards herself and her co-conspirators.

Lindsey was a Senior Administrative Technician at DPW, a governmental entity responsible for providing engineering, technical, and administrative services to Richmond residents.

Before she was placed on administrative leave in February 2022, Lindsey was responsible for managing and obtaining approval for DPW procurements with outside vendors.

From at least 2018 through 2021, Lindsey and her co-conspirators operated a scheme to defraud the DPW. Lindsey and her co-conspirators owned and operated straw companies to bid on DPW work, circumventing Virginia law and City of Richmond rules against self-dealing by public employees. Additionally, Lindsey and her co-conspirators designated and approved DPW work to be performed by these straw companies using their positions at DPW. In some instances, the work to be performed was completely fabricated and no such work was ever needed.

In other instances, the work was actually performed by DPW employees, not by contracted vendors. Sometimes, Lindsey and her co-conspirators subcontracted the work out for profit upon winning the DPW work.

Where procurement amounts exceeded $5,000, a DPW approval threshold requiring that work be competitively bid, Lindsey manufactured fictitious straw bids on behalf of competitor companies to engineer Lindsey's preferred company winning the work. In one instance, Lindsey steered a $28,700 contract award to her boyfriend. Finally, within days of Lindsey's straw company winning work, she sent checks for a portion of the funds to a senior DPW leader, Lindsey's co-conspirator. (Source)

Former D.C. Government Employee Pleads Guilty To Stealing $350,000+ - May 17, 2023

Rhayda Thomas, 52 is a former employee of the D.C. Department of Employment Services' Project Empowerment Program.

Thomas pleaded guilty today to stealing more than $350,000 from the Project Empowerment Program between May 2015 and April 2018.

In 2011, Barnes Thomas pleaded guilty in Maryland federal court to theft involving a federal government program in connection with a scheme to use federal funds received by her school employer to buy technology for herself, her family, and friends. She was sentenced to 27 months in prison for that offense.

In August 2013, following her release from prison, Thomas participated in the Project Empowerment Program. From May 2015 through April 2018, she stole hundreds of thousands of dollars from the program by reviving 16 former Project Empowerment participants' profiles and modifying entries in a database to falsely show them as working for a non-profit organization, which was not true. She also used the name of a former employee from the non-profit organization to enter and approve time in the database showing individuals as working when they were not. In addition, she ordered or caused to be ordered replacement and new prepaid debit cards on behalf of the former Project Empowerment participants whose profiles she fraudulently revived. As a result of her conduct, she caused the D.C. government to request that Wells Fargo Bank load funds onto those prepaid debit cards, which she controlled. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

No Incidents To Report

CHURCHES / RELIGIOUS INSTITUTIONS

Fomer Church Bookkeeper Sentenced To Prison For Embezzling $175,000+ From Church - May 15, 2023

Anitia Hobdy pled guilty to wire fraud, stemming from fraudulent charges made from First Baptist Church of LaPlace.

Hobdy conducted the wire fraud scheme from 2015 through 2021. Hobdy worked as a Bookkeeper for a church's daycare and embezzled over $175,000 from church accounts during that period. (Source)

LABOR UNIONS

Former Union Secretary - Treasurer Sentenced To Prison For Embezzling $96,000 - May 4, 2023

The former Secretary - Treasurer of the Hawaii Longshore Division, Charles Brown was paid according to vouchers that he submitted to the accounting department of Local 142. The hours Brown was supposed to list on the vouchers were based upon the "lost time" that he could have worked for his employer, McCabe, Hamilton & Renny Co., Ltd., where he worked as a machine operator. This was an "honor system" which depended upon the honesty of the defendant and other union officers to accurately report the number of hours they could have worked for their employers instead of working for the union.

While Brown was charged with submitting two false wage vouchers that resulted in him embezzling $1,425.01, the prosecution argued during the trial, and in sentencing, that he should be held accountable for all of the false vouchers that he submitted while acting as Secretary-Treasurer of the union, including 384 false entries, with a total embezzlement of $96,000 during a span of 4.5 years. Judge Kobayashi agreed and sentenced him to a term of imprisonment of 24 months and a fine of $96,000. (Source)

Former Union Chief Financial Officer Pleads Guilty To Embezzling $19,000+ - May 10, 2023

From December 20, 2018 until June 12, 2019, Gary Fridley was a Union Officer in while employed by American Electric Power (AEP).

As the union's elected Financial Secretary, Fridley was the Union's Chief Financial Officer and was responsible for preparing and co-signing union checks and maintaining financial records.

Fridley was one of three signatories on the union's checking account at a bank. As Financial Secretary, Fridley was entitled to an officer's salary as well as reimbursement for lost time or wages lost from his employment when he took off from work for union business.

On about June 12, 2019, Fridley received a check for $1,321.55 as reimbursement for lost time. Fridley admitted that he had not lost any time with AEP during that pay period. Fridley submitted a false voucher to receive an unauthorized lost time payment and forged the signature of another union official in order to cash the check for the fictitious lost time.

Fridley further admitted that he improperly received $19,732.88 through his wrongful actions as the union's financial secretary. Fridley submitted additional false vouchers to receive unauthorized lost time payments from the union and forged the signatures of other union officials to cash the union checks he wrote payable to himself for the fictitious lost time payments. (Source)

Former President Of State Police Union And Former Lobbyist Sentenced To Prison For Kickbacks, Fraud, Obstruction And Tax Charges - May 10, 2023

From at least 2012 until Dana Pullman resigned as the President in September 2018, Pullman and Anne Lynch turned the State Police Association of Massachusetts (SPAM) into a racketeering enterprise, using Pullman's position and power to defraud SPAM members, the Commonwealth of Massachusetts, and vendors looking to do business with the MSP.

Among other things, Pullman and Lynch defrauded SPAM members and the Commonwealth of their right to honest services from Pullman when Lynch paid Pullman a $20,000 kickback in connection with a settlement agreement between SPAM and the Commonwealth. Pullman and Lynch defrauded two different companies that sought to do business with the MSP by hiding from the vendors the fact that Lynch was paying Pullman to direct vendors to use Lynch's services.

The defendants hid the payments from Lynch and her lobbying firm to Pullman in a manner designed to avoid reporting and paying taxes on that income to the IRS. Pullman and Lynch also attempted to obstruct the grand jury's investigation of this matter by manipulating subpoenaed records, and Lynch attempted to obstruct the grand jury's investigation by lying to investigators. (Source)

BANKING / FINANCIAL INSTITUTIONS

Bank Manager Sentenced To Prison For Stealing $175,00 / Used Money For Living Expense, Pay Debts, Buy Motorcycle - May 8, 2023

From Feb. 20, 2020 to May 25, 2021, while Manager of the Commerce Bank branch on Natural Bridge Avenue in St. Louis, Andrea Hopkins logged into customer accounts and transferred funds out into either cashier's checks or prepaid cards. She changed the address on some account statements, forged signatures and transferred funds among customers to try and hide the thefts. The bank has since repaid customers.

Hopkins took more than $328,000 from the accounts of 15 customers, but returned some of the money to earlier victims to perpetuate the scheme.

Hopkins stole from the accounts of some victims multiple times, he said. Some of her victims were elderly and had a diminished ability to understand their financial affairs. Among them are two 80-year-olds, one 95-year-old and one 82-year-old, her plea agreement says.

She used the money to buy a motorcycle, to pay for living expenses and to pay personal debts. (Source)

Former Bank Financial Advisor Sentenced To Prison For Stealing $158,000+ From Elderly Bank Customers - May 1, 2023

From 2016 to 2021, Tyler Rigsbee worked as a FINRA registered financial advisor at a major bank in Sacramento. During his employment, Rigsbee targeted elderly bank customers and stole $158,960 from these victims' accounts.

Rigsbee stole $113,160 from one elderly victim's account by using the name and identity of the account beneficiary to fraudulently transfer the funds into another account that Rigsbee had set up and controlled in the beneficiary's name.

Rigsbee next stole $45,800 from the account of a second elderly victim by transferring funds in incremental amounts into a separate account that Rigsbee had set up and controlled in the victim's name. Rigsbee then pocketed the money by transferring these funds into his own personal bank account.

Toward the end of his scheme, Rigsbee attempted to conceal his theft by stealing $16,700 from a third elderly customer's account and attempting to funnel that money into the second victim's account to partially replace what he previously stole. However, this transaction was flagged, and the funds were reverted. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Former Apple Engineer Charged With Theft Of Trade Secrets After Accepting Offer With Chinese Company - May 17, 2023

Apple hired Weibao Wang as a software engineer in 2016 on a team that designed and developed hardware and software for autonomous systems.

In 2017, Wang signed a letter accepting employment with the U.S.-based subsidiary of a Chinese company allegedly working to develop self-driving cars.

Prosecutors said Wang waited more than four months after accepting the new employment agreement before informing Apple that he was leaving.

Apple later discovered that Wang accessed large amounts of sensitive information in the days leading up to his departure from at Apple in 2018, prosecutors said.

A search of Wang's Mountain View home found large amounts of Apple data. While he told agents during the search that he had no plans to travel, Wang bought a one-way ticket to Guangzhou, China, and boarded a flight that night, authorities said. (Source)

Tesla Employee Releases 100 GB Of Data On Safety Problems To German Media Outlet - May 25, 2023

How bad is Tesla Autopilot's safety problem? According to thousands of complaints allegedly from Tesla customers in the U.S. and around the world, pretty bad.

A huge data dump based on a whistleblower's leak of internal Tesla documents shows that problems with Tesla's automated driving technology may be far more common than media reports and regulators have let on, according to the German newspaper Handelsblatt, which published an article about it.

The reportedly leaked files add to the troubling anecdotes that have appeared in the media and on social media over the years about Tesla's Autopilot and the experimental technology it has branded as Full Self-Driving.

They spotlight Tesla's attempts to keep safety complaints secret and what appears to be a strategy to limit customer communications that might end up in lawsuits.

Tesla believes that a single former employee is responsible for the leak and downloaded the data before leaving. The company plans to take legal action against that former employee, according to an email by Tesla managing counsel Joseph Alm. (Source)

CHINESE ESPIONAGE TARGETING U.S. GOVERNMENT / COMPANIES / UNIVERSITIES

Former Employee Arrested For Stealing Sensitive Software From His U.S. Employers To Build A Competing Business In China - May 16, 2023

Liming Li worked for Company #1 from 1996 to 2018 and then worked at Company #2 from 2018 until November 2019. Shortly before beginning his employment with the Company #2, Li and his wife established their own business, JSL Innovations, which was based out of their Rancho Cucamonga home.

After Company #2 terminated Li, company security discovered that Li was using his company-issued laptop to attempt to download files from Company #2's root directory onto his personal external hard drive. Company security searched Li's company-issued laptop and found a folder labeled China Government.

That folder allegedly contained numerous documents showing Li's efforts to participate in the PRC's Thousand Talents Program and to use JSL Innovations to provide services and technology to PRC business and government entities related to the export-controlled and trade secret technology that Li took from his former employers in Southern California.

In March 2020, Li entered into an agreement with a PRC-based manufacturing company to serve as its chief technology officer. Li's agreement with this employer required him to spend at least six months per year in the PRC.

Six months later, FBI agents executed a search warrant at LI's home and found numerous digital devices containing millions of files belonging to Company #1 and Company #2 and containing the source code for those companies' proprietary software, the complaint alleges. Although the source code files had been developed by and belonged to these companies, some of the files had been moved into folders labeled "JSL" or "JSL Projects."

Both Company #1 and Company #2 derive significant value from the secrecy of their proprietary software source code and take extensive steps to protect the source code from discovery by competitors. (Source)

Democratic Representative Frequently Met With Alleged Chinese Police Station Director Arrested By The FBI - April 30, 2023

New York Democratic Rep. Grace Meng frequently met and attended events with an alleged Chinese Communist Party (CCP) operative who was recently arrested by the FBI, according to photos and news reports reviewed by the Daily Caller News Foundation.

Since 2016, Meng has attended multiple New York City events held by Chinese-American organizations to which Lu Jianwang, the suspected CCP operative, has belonged, according to photos and reports from multiple Chinese-language news sites.

On April 17, 2023 the FBI arrested Lu Jianwang, the former Chairman of the nonprofit America Changle Association, for allegedly opening and operating an illegal overseas police station within the nonprofit's Manhattan headquarters.

Not only has Meng attended multiple events alongside Lu Jianwang, who also goes by Harry Lu, but the six-term congresswoman was also present at several key moments in America Changle's history, photos and reports from multiple Chinese-language news sources reveal. (Source)

PHARMACEUTICAL COMPANINES / PHARMICIES / HOSPITALS / HEALTHCARE CENTERS / DOCTORS OFFICES / ASSISTED LIVING FACILITIES

No Incidents To Report

EMBEZZLEMENT / FINANCIAL THEFT / FRAUD / BRIBERY / KICKBACKS / EXTORTION / MONEY LAUNDERING / INSIDER TRADING

Former IT Employee Sentenced To Prison For Stealing Confidential Data And Extorting Company For $2 Million In Ransom / Also Publishes Misleading News Articles Costing Company $4 BILLION+ In Market Capitalization - May 10, 2023

Nickolas Sharp was employed by his company (Ubiquiti Networks) from August 2018 through Apri 1, 2021. Sharp was a Senior Developer who had administrative to credentials for companys Amazon Web Services (AWS) and GitHub servers.

Sharp pled guilty to multiple federal crimes in connection with a scheme he perpetrated to secretly steal gigabytes of confidential files from a public New York-based technology company where he was employed.

While purportedly working to remediate the security breach for his company, that he caused, Sharp extorted the company for nearly $2 million for the return of the files and the identification of a remaining purported vulnerability.

Sharp subsequently re-victimized his employer by causing the publication of misleading news articles about the company's handling of the breach that he perpetrated, which were followed by the loss of over $4 billion in market capitalization.

Several days after the FBI executed the search warrant at Sharps's residence, Sharp caused false news stories to be published about the incident and his company's response to the Incident and related disclosures.

In those stories, Sharp identified himself as an anonymous whistleblower within company, who had worked on remediating the Incident. Sharp falsely claimed that his company had been hacked by an unidentified perpetrator who maliciously acquired root administrator access to his company's AWS accounts. Sharp in fact had taken the his company's data using credentials to which he had access in his role as his company AWS Cloud Administrator. Sharp used the data in a failed attempt to his company for $2 Million. (Source)

Former Company Chief Financial Officer Charged For Using $35 Million In Company Cash To Invest In Cryptocurrency Venture - May 17, 2023

Nevin Setty was hired as the CFO of a private company in March 2021.

The company was raising capital for its work in multiple rounds of funding. The company adopted an investment policy statement that called for company cash to be invested only in fixed income instruments payable in U.S. dollars. Only certain types of conservative investments were approved.

Despite the fact that Shetty helped draft the policy and disseminate it, he moved $35 million in company funds to a cryptocurrency platform he controlled as a side business. Shetty created that side business, called HighTower Treasury, in or around February 2022. In March 2022, he was told he could not continue as CFO at his employer due to concerns about his performance. Shortly after he got this news, Shetty secretly transferred the funds out of the company's account.

Between April 1 and 12, 2022, Shetty transferred $35,000,100 of his employer's money to an account for HighTower. No one else at the company knew of these transfers. The money was supposed to be invested by HighTower in a realm of cryptocurrency sometimes referred to as decentralized finance or "DeFi." HighTower would pay Shetty's company 6% interest and keep the remainder of any interest earned, which could have been substantial. As an owner of HighTower, Shetty stood to keep those profits. Shetty kept this investment in cryptocurrency secret from the board and other employees at the company where he worked.

However, the cryptocurrency investments soon began declining and by May 13, 2022, the value of the $35 million investment was nearly zero. (Source)

Former Dental Practice Bookkeeper Sentenced To Prison For Embezzling $1.2 Million+ And Defrauding The U.S. Government Of $52,000+ - May 15, 2023

Between 2015 and 2021, Jack Massarsky worked as a Dentist and Bookkeeper for a general dentistry practice in Massachusetts. In 2015, Massarsky opened a secret bank account in the name of the dentistry practice. Massarsky then intercepted insurance reimbursement checks sent to the dentistry practice in the mail and deposited those checks in the secret bank account. He continued this practice for over five years and embezzled over $1.2 million. Massarsky used the stolen funds for personal and family expenses.

Additionally, Massarsky used the dentistry practice's name to defraud the United States. In July 2020, he submitted a fraudulent application to the Health Resources and Services Administration Provider Relief Fund (HRSA PRF) in the name of the dentistry practice. The HRSA is an agency of the United States Department of Health and Human Services that provides health care to people who are geographically isolated or otherwise vulnerable. During the COVID-19 pandemic, the HRSA PRF provided economic assistance to qualifying healthcare providers, including certain dentistry practices. By submitting the fraudulent application to the HRSA PRF, Massarsky obtained over $52,000 in pandemic relief funds that were deposited in the secret bank account Massarsky had opened in the name of his employer. (Source)

Former Finance / Operations Manager Pleads Guilty To Defrauding Charitable Non-Profit Of $871,000+ - May 23, 2023

From about March 19, 2020, through about September 28, 2022, Benjamin Cisco devised and executed his scheme to defraud the charitable non-profit organization while employed as its Finance and Operations Manager in Belle and Charleston West Virginia. Through his position, Cisco had control over the victim charity's finances and access to its debit cards, and regularly worked with its accountant.

Cisco's duties included preparing the victim charity's biweekly payroll, depositing payments into its bank accounts and providing its Board of Directors with updates regarding its finances.

Cisco admitted that his fraud scheme followed a two-step process. First, Cisco electronically transferred money from the victim charity's debit cards to its account with the Flipcause crowd-funding platform, which recorded those transfers as donations. Second, Cisco electronically transferred money from the victim charity's Flipcause account to his personal bank account, which he had falsely labeled as belonging to the victim charity.

Cisco admitted that these fraudulent transactions included electronic transfers from the victim charity's Flipcause account to his personal bank account of $4,724 on January 28, 2022, and $2,874 on May 6, 2022. Both transfers traveled in interstate commerce between Charleston, West Virginia, and California. Cisco further admitted to executing the fraudulent two-step process more than 100 times.

Cisco's fraudulent scheme specifically caused at least $518,101.70 of loss to the victim charity. Cisco also admitted to defrauding the victim charity of an additional $285,626.64 in travel reimbursements he was not authorized to receive and $67,560 by purchasing gift cards with victim charity funds without authorization. The total loss is $871,288.34. (Source)

Former Administrative Assistant Pleads Guilty To $250,000 Of Bank Fraud - May 16, 2023

From January 15, 2015, through November 2018, Kathy Strickmaker devised a scheme to defraud a financial institution by writing fraudulent checks on accounts of a business where she was employed as an Administrative Assistant.

Strickmaker's duties as administrative assistant included paying bills on behalf of the business, which maintained multiple accounts at a bank and managing the business's payroll and accounts payable. Strickmaker admitted that she wrote at least 80 unauthorized checks drawn from the business's bank accounts and forged her employer's signature on them. Strickmaker further admitted that she made the unauthorized checks payable to three individuals in amounts of between approximately $800 to $3,300. These individuals cashed or deposited the checks at local banks keeping $100 per check and transferring the balance to another individual at Strickmaker's direction.

Strickmaker also admitted to writing fraudulent and unauthorized checks from the business's bank accounts from 2016 through 2018 that she made payable to herself. Strickmaker also forged her employer's signature on those checks.

Strickmaker must pay a $1 Million fine and owes at least $250,000 in restitution. (Source)

Bookkeeper For 2 Businesses Charged With Embezzling $200,000+ From 2 Businesses To Pay Her Debts & Family Members Debts - May 11, 2023

Tara Durnell, while working as a Bookkeeper. She embezzled from Kronebusch Electric, Inc. (KEI), an electrical services company and then from Mitchell's Crash Repair, an auto repair shop, after she left KEI's employment.

From at least November 2013 to 2019, Durnell used her access to KEI's business bank accounts and software to direct pre-signed checks to cover her personal expenses and then miscode the payments in the software to make the personal payments look like legitimate KEI business expenses. The indictment further alleges Durnell embezzled more than $200,000 from KEI to pay personal credit card debt, personal car loan payments and debts of family members.

While employed at Mitchell's Crash Repair, Durnell allegedly embezzled approximately $15,000 by using pre-signed checks to make unauthorized payments for personal expenses, including taxes on her home and a bar she owned in Conrad. (Source)

EMPLOYEES' WHO EMBEZZLE / STEAL MONEY FOR PERSONAL ENRICHMET AND TO LIVE ENHANCED LIFESTYLE

Former Morgan Stanley Financial Advisor Sentenced To Prison For Executing A $7 Million Ponzi Scheme / Used Funds For Personal Use - May 24, 2023

Shawn Good was sentenced today to 87 months in prison followed by three years of supervised release for carrying out a $7 million dollar investment fraud scheme. Good pleaded guilty to wire fraud and money laundering on September 15, 2022. Good was also ordered to pay $3,619,594 in restitution to victims.

Good was employed as a registered representative and investment advisor for Morgan Stanley Smith Barney, LLC in Wilmington. From 2012 to February 2022, Good executed a scheme to obtain money through an investment fraud commonly known as a Ponzi scheme. Specifically, Good solicited investments from business clients and others for purported real estate projects and tax-free municipal bonds, touting these opportunities as low-risk investments that would pay returns of between 6% and 10% over three- or six-month terms.

At least 12 victims invested approximately $7,246,300 based on false statements and misrepresentations made by Good. Instead of investing in land development or bonds, Good used the money for personal expenditures including his Wilmington residence; a condominium in Florida; luxury vehicles including a Mercedes Benz, a Porsche Boxster, a Tesla Model 3, an Alpha Romeo Stelvio, and a Lexus RX350; fine dining; and vacations to Paris, France; Cinca Terra, Italy; Jackson, Wyoming; Las Vegas, Nevada; and other destinations. To lend credibility to the Ponzi scheme and to elude detection, Good also used a portion of investor funds to make payments to earlier investors. (Source)

Former Finance Director Pleads Guilty To Embezzling $3 Million+ From 2 Non-Profit Organizations / Used Funds For Mortgage, Gambling, Vacations, Etc. - May 16, 2023

In 1999 Susana Tantico began working for a non-profit that provides healthcare to underserved populations. Ultimately, Tantico became the non-profit's Finance Director. Between 2011 and June 2020, Tantico embezzled nearly $2.3 million from the healthcare non-profit. She used the non-profit's debit and credit cards to withdraw $1.6 million at casinos for gambling. She also used the debit and credit cards to pay for personal vacations, such as a $26,000 family trip to Disneyworld, and trips to Las Vegas and San Diego. Tantico also used the medical non-profit's debit and credit cards for more than $83,000 worth of purchases at Nordstrom and $40,000 worth of purchases at Apple stores.

After running up the big bills, Tantico used the non-profit's funds to pay the credit card bills and disguised the payments as legitimate expenses, such as medical supplies. Throughout this timeframe, Tantico told the non-profit auditors that she was aware of no fraud at the non-profit.

In 2020, Tantico went to work as Finance Director for a different non-profit, one with a focus on criminal justice issues. Tantico used more than $485,000 of the non-profit's funds for gambling at casinos. She transferred $21,000 from the non-profit to her mortgage servicer to pay her home mortgage. She also transferred money to her personal bank account. Tantico then altered the bank records to hide the embezzlement. At one point, she was questioned by one of the organization's banks about all the withdrawals at casinos. She claimed that the non-profit held youth programs at the casinos and claimed the withdrawals were for cash prize giveaways. In all, Tantico stole nearly $893,000 from the non-profit.

The non-profit has incurred $132,000 in costs to forensically audit its books, fix its accounting procedures and records, and reply to vendors. (Source)

Former Board Member of Connecticut Energy Cooperative Sentenced To Prison For Role In Misusing $800,000+ Of Funds For Lavish Trips - May 18, 2023

Between 2010 and 2015 the Connecticut Municipal Electric Energy Corporation (CMEEC) received more than $9 million dollars from the U.S. Department of Energy. CMEEC member towns also received funds from federal grants.

John Bilda was the former City of Norwich representative on the CMEEC Board of Directors. He was sentenced to prison for misusing CMEEC funds.

According to the evidence and testimony presented during a trial in 2021, Drew Rankin, who was the former Chief Executive Officer of CMEEC, Bilda, and other members of the CMEEC Board of Directors, planned, organized, and directed lavish trips outside of Connecticut, including trips to the Kentucky Derby in 2015 and 2016, and to a luxury golf resort in West Virginia in 2015. These trips did not relate to CMEEC business, but were intended to personally benefit, compensate and reward Rankin, Bilda, CMEEC Board members, their family members, friends, and associates.

Costs for the trips, which totaled more than $800,000, included travel expenses, private chartered airfare, first-class hotel accommodations, meals, tickets to sporting events, golf fees, souvenirs and gifts. (Source)

Former Company Financial Controller Sentenced To Prison For Embezzling $690,000+ For 9 Years / Used Money For Vacations. Paying Debts, Home Improvements, Etc. -May 4, 2023

From 2012 to December of 2021, Tammy Scudder devised and participated in a scheme to defraud her employer of more than $600,000. Scudder served as the Controller for a company located in Shelbyville, Indiana for nine years. As Controller, Scudder was the company's top accountant and maintained its accounting ledgers, managed payroll, and had access to online bank accounts. Scudder also had access to the company's accounting software, which she used to generate checks in Plymate's name.

Scudder abused her position of trust as Controller to exploit a vulnerability in the company's accounting system. Scudder knew that the company's Group Health Plan bank account was difficult to double-check because it was funded based upon the total amount of the weekly claims on the list it received from another company, rather than by each claim individually. Scudder accessed the victim company's accounting software to generate and print a company check to herself, signed using another employee's signature stamp. After Scudder printed the check, she concealed the theft by altering and falsifying the victim company's accounting records.

Scudder used the stolen money to take vacations, pay off personal debts, fund her children's educational expenditures, and by make improvements to her Shelbyville residence. Between February 2, 2012, and December 17, 2020, Scudder generated 154 false and fraudulent checks totaling $693,708.75. (Source)

Former Office Manager Pleads Guilty To Embezzling $1.4 Million+ For Personal Use - May 4, 2023

From 2018 until April 2021, Stephanie Fannin served as the Office Manager of General Lighting and Sign Services (GLSS). In her role as the office manager, Fannin had complete access to GLSS's operating account and managed accounts payable and receivable for GLSS's business transactions.

She also created and disbursed invoices, tracked licenses of employed contracted workers, and managed the payroll of GLSS employees.

Fannin admitted that between early 2018 and April 2021, she issued approximately 294 unauthorized checks made payable to her drawn on GLSS's operating account, and deposited each of these checks into her personal bank account to pay for personal items and services. She further admitted that she used computer software to make it appear that the unauthorized checks had been made to GLSS's vendors. Fannin admitted that she embezzled approximately $1,432,260.03 from GLSS. (Source)

Former Accounting Clerk For Non-Profit Organization Charged With Embezzling $560,000 To Purchase Properties - May 15, 2023

John Van Vught performed contract accounting work for ValleyNet between 2010 and July 2022.

During that timeframe, Van Vught transferred $560,000 out of ValleyNet's accounts into his personal bank account. Van Vught hid the transfers by underreporting the income ValleyNet received according to his accounting submissions. Van Vught also obfuscated his possession of the embezzled funds by purchasing properties in Georgia and Florida. (Source)

Former Executive Director Of Miss Florida Scholarship Program Sentenced To Prison For Stealing $243,000 For Personal Use - May 3, 2023

Mary Wickersham to 15 months in prison and ordered her to pay $243,000 in restitution for stealing money intended for the Miss Florida Scholarship Program over the course of seven years. Wickersham pleaded guilty earlier this year.

Since 2002, Mary Wickersham served as the Executive Director of the Miss Florida Scholarship Program. The Miss Florida Scholarship Program offers educational and financial assistance to young women across the state.

In 2011, Wickersham formed a Florida corporation named "Miss Florida LLC" and used it to open a bank account in the same name.

She did so without the knowledge or consent of the Miss Florida Scholarship Program.

Wickersham then redirected hundreds of thousands of dollars into the Miss Florida LLC bank account, which she controlled, by using her position as Executive Director to solicit donations from the program's recurring business sponsors and donors, all while representing that those monies would be used to fund scholarships for the Miss Florida Program women. In fact, Wickersham used the money for her own personal use and gain. (Source)

Former Executive Director For Charity Charged For Embezzling $230,000+ / Used Fund For Gambling - May 12, 2023

Kyle Fisher was the Executive Director of a charity. He had full access to the charity's finances, including its QuickBooks accounting records, PayPal account, and bank account.

Between February 2021 and September 2022, Fisher embezzled more than $230,000 from the charity. He wrote unauthorized checks to himself and transferred funds from the charity's PayPal account to his own personal bank account. Fisher created fake invoices and receipts and altered the charity's accounting records. He gambled a large amount of the stolen funds away at the MGM casino in Springfield, Massachusetts. (Source)

Former Manager For Dialysis Clinics Sentenced To Prison For $204,000+ Of Bank Fraud And Identity Theft / Used Funds For Personal Expenses / Family - May 16, 2023

Jeanne Rather was charged in May 2021 for stealing the personally identifying information of at least ten people who worked under her at dialysis clinics. Between September 2019 and March 2020, she used the information to fraudulently open credit accounts and charge expenses for her family. She also stole and deposited checks from the clinics into her own bank accounts.

Rather was the Manager of two dialysis clinics. In addition to stealing the identities of her subordinates, she stole 20 checks from insurance companies written to one of the clinics and deposited the checks into her personal bank accounts. She defrauded the clinic of $98,511 and ran up credit card charges that defrauded a bank of $106,089 for a total loss amount of more than $204,000. In her plea agreement in February 2022, Rather agreed to make full restitution to the bank and clinic. (Source)

Former City Clerk Sentenced To Prison For Stealing $159,000+ From City / Used Funds For Gambling - May 17, 2023

Donna Thompson is the second former employee to be sentenced to prison for stealing $159,000 from the city, which is roughly six blocks square, has an annual budget of about $400,000 and a population of about 800. More than half of those residents live below the poverty line.

Maureen Woodson was also sentenced to prison and ordered her to repay the $487,673 that she stole.

Both women wrote roughly 614 city checks to themselves from about February 2016 to April 2022, forging the signature of the Mayor and / or Treasurer and either cashing the checks or depositing them into their personal bank accounts. The Mayor, the Treasurer and the board of aldermen had no knowledge of the checks being written on city accounts. Woodson and Thompson used the cash for personal expenses and gambled the rest away. On about 381 occasions, Woodson and Thompson usedcity funds to directly pay for their own personal expenses, by either writing checks or wiring city funds directly to third party vendors for entertainment, restaurants, home rental payments, and personal taxes owed to the Internal Revenue Service. (Source)

Former Bookkeeper Charged With Unauthorized Credit Card Purchasing & Making Payroll Payments To Herself - May 20, 2023

The Indictment alleges that beginning on or about June 1, 2018, and continuing through May 17, 2022, Michelle Warner, who was employed as a bookkeeper / accountant, and later as a business administrator, devised and intended to devise a scheme and artifice to defraud and obtain money and property from others by means of false and fraudulent pretenses, representations, and promises.

The Indictment alleges that Warner, in her capacity as bookkeeper / accountant and business administrator, falsely and fraudulently paid herself additional and unauthorized payroll payments and then used the funds for her own purposes. Warner also caused her employer to remit payroll tax to the Internal Revenue Service on her behalf. Such funds purportedly came from withholding from Warner's payroll check, when in fact, as Warner then and there knew, she did not actually withhold those funds from her payroll check. Additionally, Warner used her employer's credit card without authority for her own personal use. (Source)

Former Property Manager Pleads Guilty To Stealing $16,500+ Of Government Funds For Personal Use - May 25, 2023

Oliver King was the Property Manager for an apartment complex that received Section 8 project-based rental assistance funding from the Department of Housing and Urban Development (HUD). As property manager, King had access to the HUD funding and misappropriated the government funds for his own unjust enrichment.

King has agreed to forfeit $16,618.91, the amount he obtained as a result of the offense. (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

Former Accounting Manager Pleads Guilty To Embezzling $2.5 Million+ Over 10 Years By Creating Fake Company - May 11, 2023

Christin Guillory was an Accounting Manager at an manufacturing company. She stole more than $2.5 Million from her employer by transferring funds to accounts Guillory set up in the names of fake companies and then routing the funds to her own bank accounts.

In April 2013, Christin Guillory set up an account with payment processor Square that used a display name that made it appear it was an account of a commercial shipping company.

Between 2014 and 2019, Guillory secretly paid $1,695,591 to that account and then transferred the money to her own bank accounts. She made false entries in the company books to conceal the theft.

In 2019, Guillory stopped using Square for her fraud and instead used two PayPal accounts. She gave one of the PayPal accounts a display name similar to that of her employer. For the second account, she used the name of a shipping company with which she had no affiliation. In 2020 and 2021, she caused the transfer of $604,000 to the PayPal accounts and made false accounting entries to cover her tracks. She then transferred the bulk of the money for her own use. Becoming more brazen, between August and November 2021, Guillory transferred $247,000 directly from company accounts to her own bank accounts.

Again, she made fraudulent accounting entries and reused legitimate invoices to make it appear the payments were for appropriate business purposes. In all, Guillory made at least 867 secret transactions using interstate wires that totaled $2,536,086.

The scheme was detected when a financial institution reported irregularities. (Source)

NETWORK / IT SABOTAGE / OTHER FORMS OF SABOTAGE / UN-AUTHORIZED ACCESS TO COMPUTER SYSTEMS & NETWORKS

Former Bankruptcy Court Employee Pleads Guilty To Sabotaging IPad Remotely After Termination - May 3, 2023

Robert Brittain was previously employed by the United States Bankruptcy Court for the Middle District of North Carolina as a Court Management Analyst, where he managed and configured computer products operated by the court's employees.

Brittain resigned from this position in April 2022 after an internal investigation into his conduct. Before leaving his position, Brittain allegedly established a VPN connection from his home to the court's network which, after his termination, he illegally used to access another employee's passwords and remotely wipe an iPad belonging to the Bankruptcy Court. (Source)

Former Employee Charged With Sabotaging Employers Database After Being Notified He Would Be Terminated - May 30, 2023

Vamsikrishna Naganathanahall accessed a computer system belonging to his former employer, Vituity, after his company login privileges had been revoked. Naganathanahalli used his access to the computer system to replace real data with masked data causing damage to an important Vituity database.

Vituity comprises a group of related companies based in Emeryville, Calif., including physician partnerships and other entities. Vituity maintained a computer database that was central to its business and was connected to systems responsible for hiring and payroll, among other functions.

In late May of 2022 Naganathanahalli was informed that his employment with Vituity would be terminated in mid-June. After he was informed his employment would be terminated, but before his last day on the job, he changed a password to another employee's account so he would be able to gain access to a Vituity computer system after access to Vituity's computers using his own password was revoked. In September 2022, Naganathanahalli used the changed password to access a Vituity computer system remotely, change yet another employee's password, and then use that employee's account to overwrite the company's personnel data. (Source)

THEFT OF ORGANIZATIONS ASSESTS

Former Information Technology Manager Pleads Guilty To Theft Of $1.4 Million+ Of IT Equipment / Used Money For Personal Use - May 4, 2023

mer information technology manager of a Quebec City, Canada-based telecommunications company has been charged and has agreed to plead guilty in connection with a fraud scheme that involved the theft of over $1.4 million in computer equipment from his employer.

Todd Erickson served as the Information Technology (IT) Manager at a telecommunications company that, until February 2019, had an office located in Chelmsford, Mass. As the IT Manager, Erikson was responsible for submitting requests to purchase equipment , such as computers and hard drives.

From at least January 2012 through February 2019, Erickson fraudulently submitted purchase requests for computer equipment that the company did not need. Thereafter, without the knowledge or approval of his employer, Erickson allegedly sold the items to third parties and used the illicit proceeds for his personal benefit. (Source)

Former Parts Manager Sentenced To Prison For Stealing $400,000+ Of Parts And Selling On EBay - May 24, 2023

James Cox worked as the Parts Manager for a multi-state business from March 2015 to November 2020. During that time, Cox was responsible for ordering parts, signing for them when they arrived, and logging them into inventory.

From 2018 to 2020, Cox used his position to fraudulently order parts and products that the business did not need using funds belonging to the business. Cox then stole the products, including HVAC units and LED display kits, from the business and sold them on eBay without authorization. He received payment via PayPal and used the proceeds from the sales for his own personal benefit. Cox also failed to disclose to potential buyers that the listed products were stolen, which violates eBay's User Agreement.

In total, Cox sold approximately 400 stolen items on eBay, resulting in a total loss of $431,557.61 to his employer. (Source)

Former YMCA Employee Sentenced To Prison For Fraudulently Ordering Cell 1,000 Phones For YMCA And Then Reselling Them For $600,000 In Cash - May 5, 2023

Celeste Santifer was a former employee of the YMCA of Metropolitan Washington (YMCA-DC). Santifer worked as an Office Manager at YMCA-DC from approximately 2007 until her termination in May of 2019.

While working at the YMCA-DC, Santifer devised a scheme to defraud Verizon Wireless by taking advantage of an arrangement with Verizon to sell YMCA-DC cell phones for its employees at a discounted price.

From at least January 2016 through April 2019, Santifer placed online orders for discounted cell phones from Verizon that she personally received, disconnected from service, and sold to companies that buy and sell new or slightly used phones. Santifer ultimately ordered over 1,000 phones purportedly for YMCA-DC employees that she sold to third-party companies for money. The value of the phones to Verizon was $618,090. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

Former President Of Building And Construction Trades Council Sentenced To Prison For Accepting $140,000+ In Bribes / 10 Other Union Officials Sentenced For Accepting Bribes And Illegal Payments - May 18, 2023

James Cahill was the President of the New York State Building and Construction Trades Council (NYS Trades Council), which represents over 200,000 unionized construction workers, a member of the Executive Council for the New York State American Federation of Labor and Congress of Industrial Organizations (NYS AFL-CIO), and formerly a union representative of the United Association of Journeymen and Apprentices of the Plumbing and Pipefitting Industry of the United States and Canada (UA).

From about October 2018 to October 2020, Cahill accepted approximately $44,500 in bribes from Employer-1, as well as other benefits, including home appliances and free labor on Cahill's vacation home. Cahill acknowledged having previously accepted at least approximately $100,000 of additional bribes from Employer-1 in connection with Cahill's union positions.

As the leader of the conspiracy, Cahill introduced Employer-1 to many of the other defendants, while advising Employer-1 that Employer-1 could reap the benefits of being associated with the unions without actually signing union agreements or employing union workers. (Source)

Former Department of Planning & Permitting Supervisor Sentenced To Prison For Role In Accepting $100,000 In Bribery Scheme - May 24, 2023

Wayne Inouye was sentenced to 60 months in prison, two years supervised release, and a $100,000 fine for taking more than $103,000 in bribes in exchange for expediting the approval of permits issued by the Department of Planning and Permitting (DPP) of the City and County of Honolulu and for making false statements to federal investigators with intent to conceal his crimes.

After a lengthy investigation by the Federal Bureau of Investigation (FBI) into corruption at the DPP, honest services wire fraud charges were filed against six individuals, including Inouye, arising out of schemes in which employees of the DPP took bribes in exchange for performing official acts at DPP.

According to information presented to the court, while employed by DPP as the Chief Building Inspector with supervisory responsibility for approximately 20 employees, Inouye solicited bribes from architects, contractors, and others in exchange for expediting the approval of building permits by DPP. Those who paid bribes to Inouye had their permit applications sped through the DPP approval process ahead of other applications. From September 2016 to September 2017, Inouye solicited and accepted bribes of at least $89,205 from Wong.

From February 2012 to August 2017, Inouye solicited and accepted bribes of at least $3,425 from a signage contractor. From April 2012 to January 2016, Inouye solicited and accepted bribes of at least $9,685 from a building contractor. From February 2012 to December 2017, Inouye solicited and accepted bribes of at least $1,825 from a second signage contractor. (Source)

EMPLOYEE DRUG RELATED INCIDENTS

Former Hospital Registered Nurse Sentenced To Prison For Stealing Painkillers From Hospital For Her Use - May 2, 2023

According to court records, in 2020, Mary Cheatham was employed as a Licensed Registered Nurse at a local hospital in Detroit.

Cheatham admitted she tampered with vials and syringes containing the painkiller hydromorphone, which she knew were intended to be administered to patients for the purpose of pain relief in the critical care unit of the hospital. She removed the hydromorphone from the vials and syringes, replaced the hydromorphone with saline solution, and returned the adulterated containers knowing they could be administered to patients at the hospital. In total, Cheatham stole 116 vials and syringes of hydromorphone, which she then used on herself. (Source)

Former Nurse Sentenced To Prison For Stealing Drugs From 2 Hospitals For Personal Use - May 8,2023

In August 2018, Lisa Tarr was a Student Nurse working at a Boston area hospital. Tarr admitted to investigators at the hospital that she had stolen and self-injected fentanyl, a Schedule II controlled substance, from the hospital.

In 2020, while working for another Boston-area hospital, Tarr stole an infusion bag containing fentanyl that was being used to treat a patient. On another occasion in 2020, while still working at the second hospital, Tarr stole multiple syringes of hydromorphone, a Schedule II controlled substance, from a locked drug cabinet. (Source)

Former Hospital Registered Nurse Pleads Guilty To Product Fentanyl Tampering Charge - May 8, 2023

Dawn Drum wase employed as a Registered Nurse at SSM Health St. Mary's Hospital in Janesville in November 2021.

Drum tampered with vials of fentanyl by withdrawing the drug from the vials and replacing it with saline and then resealing the vial stopper with what appeared to be superglue.

Drum then put the tampered vials back into a Pyxis machine, an automated medication dispensing system, so that the tampered fentanyl vials would be available for use with other patients at the hospital. An audit of the Pyxis transactions in Drum's name revealed that she had an excessive pattern of fentanyl overrides and wastes when compared to other employees in 2021.

In November 2021, hospital management confronted Drum with this discrepancy and asked her to take a drug test. Drum refused and instead resigned from her position at the hospital. (Source)

OTHER FORMS OF INSIDER THREATS

No Incidents To Report

MASS LAYOFF OF EMPLOYEES' AND RESULTING INCIDENTS

No Incidents To Report

EMPLOYEES' MALICIOUS ACTIONS CAUSING COMPANY TO CEASE OPERATIONS

No Incidents To Report

WORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES'

No Incidents To Report

EMPLOYEES' INVOLVED IN TERRORISM

No Incidents To Report

PREVIOUS INSIDER THREAT INCIDENTS REPORTS
https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

SEVERE IMPACTS FROM INSIDER THREATS INCIDENTS

EMPLOYEE EXTORTION

Former IT Employee Pleads Guilty To Stealing Confidential Data And Extorting Company For $2 Million In Ransom / He Also Publishes Misleading News Articles Costing Company $4 BILLION+ In Market Capitalization - February 2, 2023

Nickolas Sharp was employed by his company (Ubiquiti Networks) from August 2018 through April 1, 2021. Sharp was a Senior Developer who had administrative to credentials for company's Amazon Web Services (AWS) and GitHub servers.

Sharp pled guilty to multiple federal crimes in connection with a scheme he perpetrated to secretly steal gigabytes of confidential files from his technology company where he was employed.

While purportedly working to remediate the security breach for his company, that he caused, Sharp extorted the company for nearly $2 million for the return of the files and the identification of a remaining purported vulnerability.

Sharp subsequently re-victimized his employer by causing the publication of misleading news articles about the company's handling of the breach that he perpetrated, which were followed by the loss of over $4 billion in market capitalization.

Several days after the FBI executed the search warrant at Sharps's residence, Sharp caused false news stories to be published about the incident and his company's response to the Incident and related disclosures. In those stories, Sharp identified himself as an anonymous whistleblower within company, who had worked on remediating the Incident. Sharp falsely claimed that his company had been hacked by an unidentified perpetrator who maliciously acquired root administrator access to his company's AWS accounts. Sharp in fact had taken the his company's data using credentials to which he had access in his role as his company AWS Cloud Administrator. Sharp used the data in a failed attempt to his company for $2 Million. (Source)

EMPLOYEES' WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

Former Bank President Found Guilty Of $1 BILLION Of Fraud Resulting In Failure Of Bank - February 10, 2023

A federal jury has returned a verdict of guilty on all 46 counts against former First NBC Bank President and CEO Ashton J. Ryan, Jr. and not guilty on all 7 counts against former First NBC Bank Senior Vice President Fred V. Beebe.

From 2006 through April 2017, Ryan and others conspired to defraud First NBC Bank through a variety of schemes. Ryan was the President and CEO of the Bank for most of its existence. Ryan and others, conspired to defraud First NBC Bank by disguising the true financial status of certain borrowers and their troubled loans, concealing the true financial condition of the Bank from the Board of Directors, auditors, and examiners.

When members of the Board or the Bank's outside auditors or examiners asked about loans to these borrowers, Ryan and others made false statements about the borrowers and their loans, omitting the truth about the borrowers' inability to pay their debts without getting new loans. As a result, the balance on these borrowers' loans continued to grow resulting, ultimately, in the failure of First NBC. The Bank's failure cost the Federal Deposit Insurance Corporation's deposit insurance fund slightly under $1 billion. (Source)

Former Vice President Of Discovery Tours Pleads Guilty To Embezzling $600,000 Causing Company To Cease Operations & File For Bankruptcy - June 15, 2022

Joseph Cipolletti was employed as Vice President of Discovery Tours, Inc., a business that offered educational trips for students. Cipolletti managed the organization's finances, general ledger entries, accounts payable and accounts receivable. Cipolletti also had signature authority on Discovery Tours' business bank accounts.

From June 2014 to May 2018, Cipolletti devised a scheme to defraud parents and other student trip purchasers by diverting payments intended for these trips to his own personal use on items such as home renovations and vehicles.

As a result of Cipolletti's actions and subsequent attempts to cover up the scheme, in May 2018, Discovery Tours abruptly ended operations and filed for bankruptcy. Student trips to Washington, D.C. were canceled for dozens of schools across Ohio and more than 5,000 families lost the money they had previously paid for trip fees.

Cipolletti embezzled more than $600,000 from his place of business and made false entries in the general ledger. (Source)

Former Credit Union CEO Sentenced To Prison For Involvement In Fraud Scheme That Resulted In $10 Million In Losses, Forcing Credit Union To Close - April 5, 2022

Helen Godfrey-Smith's was employed by the Shreveport Federal Credit Union (SFCU) from 1983 to 2017, and during much of that time was employed as the Chief Executive Officer (CEO) of the SFCU.

In October 2016, the SFCU, through Godfrey-Smith, entered into an agreement with the United States Department of the Treasury to buy back certain securities that were part of the Department's Troubled Asset Relief Program (TARP). Godfrey-Smith signed and submitted to the United States Department of the Treasury an Officer's Certificate which certified that all conditions precedent to the closing had been satisfied.

In reality, SFCU had not met all conditions precedent to closing and had suffered a material adverse effect. Unbeknownst to the United States Department of the Treasury, the SFCU was in a financial crisis. From 2015 through 2017, another individual who was the Chief Financial Officer (CFO) of SFCU had been falsifying reports. In addition, she was creating fictitious entries in the banks records to support the false reports. This created the illusion that SFCU was profitable when, in fact, the bank was failing. The CFO embezzled approximately $1.5 million from the credit union.

By the time Godfrey-Smith signed the CFO's statement, she had become aware of deficiencies at the credit union. Godfrey-Smith investigated and discovered that there were millions of dollars of fictitious entries on SFCU's general ledger, and the credit union's books were not balanced. But she failed to disclose this information to the United States Department of the Treasury and signed the false Officer's Statement.

In the Spring of 2017, the credit union failed. An investigation by revealed that SFCU had amassed in excess of $10 million in losses by December 2016. (Source)

Packaging Company Controller Sentenced To Prison For Stealing Funds Forcing Company Out Of Business (2021)

Victoria Mazur was employed as the Controller for Gateway Packaging Corporation, which was located in Export, PA.

From December 2012 until December 2017, she issued herself and her husband a total of approximately 189 fraudulent credit card refunds, totaling $195,063.80, through the company's point of sale terminal. Her thefts were so extensive, they caused the failure of the company, which is now out of business. In order to conceal her fraud, Mazur supplied the owners with false financial statements that understated the company's true sales figures. (Source)

Former Controller Of Oil & Gas Company Sentenced To Prison For $65 Million Bank Fraud Scheme Over 21 Years / 275 Employees' Lost Jobs (2016)

In September 2020, Judith Avilez, the former Controller of Worley & Obetz, pleaded guilty to her role in a scheme that defrauded Fulton Bank of over $65 million. Avilez admitted that from 2016 through May 2018, she helped Worley & Obetz's CEO, Jeffrey Lyons, defraud Fulton Bank by creating fraudulent financial statements that grossly inflated accounts receivable for Worley & Obetz's largest customer, Giant Food. Worley & Obetz was an oil and gas company in Manheim, PA, that provided home heating oil, gasoline, diesel, and propane to its customers.

Lyons initiated the fraud shortly after he became CEO in 1999. In order to make Worley & Obetz appear more profitable and himself appear successful as the CEO, Lyons asked the previous Worley & Obetz Controller, Karen Connelly, to falsify the company's financial statements to make it appear to have millions more in revenue and accounts receivable than it did.

Lyons and Connelly continued the fraud scheme from 2003 until 2016, when Connelly retired and Avilez became the Controller and joined the fraud. Avilez and Lyons continued the scheme in the same manner that Lyons and Connelly had. Each month, Avilez created false Worley & Obetz financial statements that Lyons presented to Fulton Bank in support of his request for additional loans or extensions on existing lines of credit. In total, Lyons, Connelly, and Avilez defrauded Fulton Bank out of $65,000,000 in loans.

After the scheme was discovered, Worley & Obetz and its related companies did not have the assets to repay the massive amount of Fulton loans Lyons had accumulated.

In June 2018, Worley & Obetz declared bankruptcy and notified its approximately 275 employees' that they no longer had jobs. After 72 years, the Obetz's family-owned company closed its doors forever.

The fraud Lyons committed with the help of Avilez and Connelly caused many families in the Manheim community to suffer financially and emotionally. Fulton Bank received some repayments from the bankruptcy proceedings but is still owed over $50,000,000. (Source)

Former Engineering Supervisor Costs Company $1 Billion In Shareholder Equity / 700 Employees' Lost Jobs (2011)

AMSC formed a partnership with Chinese wind turbine company Sinovel in 2010. In 2011, an Automation Engineering Supervisor at AMSC secretly downloaded AMSC source code and turned it over to Sinovell. Sinovel then used this same source code in its wind turbines.

2 Sinovel employees' and 1 AMSC employee were charged with stealing proprietary wind turbine technology from AMSC in order to produce their own turbines powered by stolen intellectual property.

Rather than pay AMSC for more than $800 million in products and services it had agreed to purchase, Sinovel instead hatched a scheme to brazenly steal AMSC's proprietary wind turbine technology, causing the loss of almost 700 jobs which accounted for more than half of its global workforce, and more than $1 billion in shareholder equity at AMSC. (Source)

DATA / COMPUTER - NETWORK SABOTAGE & MISUSE

Information Technology Professional Pleads Guility To Sabotaging Employer's Computer Network After Quitting Company - September 28, 2022

Casey Umetsu worked as an Information Technology Professional for a prominent Hawaii-based financial company between 2017 and 2019. In that role, Umetsu was responsible for administering the company's computer network and assisting other employees' with computer and technology problems.

Umetsu admitted that, shortly after severing all ties with the company, he accessed a website the company used to manage its internet domain. After using his former employer's credentials to access the company's configuration settings on that website, Umetsu made numerous changes, including purposefully misdirecting web and email traffic to computers unaffiliated with the company, thereby incapacitating the company's web presence and email. Umetsu then prolonged the outage for several days by taking a variety of steps to keep the company locked out of the website. Umetsu admitted he caused the damage as part of a scheme to convince the company it should hire him back at a higher salary. (Source)

IT Systems Administrator Receives Poor Bonus And Sabotages 2000 IT Servers / 17,000 Workstations - Cost Company $3 Million+ (2002)

A former system administrator that was employed by UBS PaineWebber, a financial services firm, infected the company's network with malicious code. He was apparently irate about a poor salary bonus he received of $32,000. He was expecting $50,000.

The malicious code he used is said to have cost UBS $3.1 million in recovery expenses and thousands of lost man hours.

The malicious code was executed through a logic bomb which is a program on a timer set to execute at predetermined date and time. The attack impaired trading, while impacting over 2,000 servers and 17,000 individual workstations in the home office and 370 branch offices. Some of the information was never fully restored.

After installing the malicious code, he quit his job. Following, he bought puts against UBS. If the stock price for UBS went down, because of the malicious code for example, he would profit from that purchase. (Source)

Former Employee Sentenced To Prison For Sabotaging Cisco's Network With Damages Costing $2.4 Million (2018)

Sudhish Ramesh admitted to intentionally accessing Cisco Systems' cloud infrastructure that was hosted by Amazon Web Services without Cisco's permission on September 24, 2018.

Ramesh worked for Cisco and resigned in approximately April 2018. During his unauthorized access, Ramesh admitted that he deployed a code from his Google Cloud Project account that resulted in the deletion of 456 virtual machines for Cisco's WebEx Teams application, which provided video meetings, video messaging, file sharing, and other collaboration tools. He further admitted that he acted recklessly in deploying the code, and consciously disregarded the substantial risk that his conduct could harm to Cisco.

As a result of Ramesh's conduct, over 16,000 WebEx Teams accounts were shut down for up to two weeks, and caused Cisco to spend approximately $1,400,000 in employee time to restore the damage to the application and refund over $1,000,000 to affected customers. No customer data was compromised as a result of the defendant's conduct. (Source)

Former Credit Union Employee Pleads Guilty To Unauthorized Access To Computer System After Termination & Sabotage Of 20+GB's Of Data/ Causing $10,000 In Damages (2021)

Juliana Barile was fired from her position as a part-time employee with a New York Credit Union on May 19, 2021.

Two days later, on May 21, 2021, Barile remotely accessed the Credit Union's file server and deleted more than 20,000 files and almost 3,500 directories, totaling approximately 21.3 gigabytes of data. The deleted data included files related to mortgage loan applications and the Credit Union's anti-ransomware protection software. Barile also opened confidential files.

After she accessed the computer server without authorization and destroyed files, Barile sent text messages to a friend explaining that "I deleted their shared network documents," referring to the Credit Union's share drive. To date, the Credit Union has spent approximately $10,000 in remediation expenses for Barile's unauthorized intrusion and destruction of data. (Source)

Fired IT System Administrator Sabotages Railway Network - February 14, 2018

Christopher Grupe was suspended for 12 days back in December 2015 for insubordination while working for the Canadian Pacific Railway (CPR). When he returned the CPR had already decided they no longer wanted to work with Grupe and fired him. Grupe argued and got them to agree to let him resign. Little did CPR know, Grupe had no intention of going quietly.

As an IT System Administrator, Grupe had in his possession a work laptop, remote access authentication token, and access badge. Before returning these, he decided to sabotage the railway's computer network. Logging into the system using his still-active credentials, Grupe removed admin-level access from other accounts, deleted important files from the network, and changed passwords so other employees' could no longer gain access. He also deleted any logs showing what he had done.

The laptop was then returned, Grupe left, and all hell broke loose. Other CPR employees' couldn't log into the computer network and the system quickly stopped working. The fix involved rebooting the network and performing the equivalent of a factory reset to regain access.

Grupe may have been smirking to himself knowing what was going on, but CPR's management decided to find out exactly what happened. They called in computer forensic experts who found the evidence needed to prosecute Grupe. Grupe was found guilty of carrying out the network sabotage and handed a 366 day prison term. (Source)

Former IT Systems Administrator Sentenced To Prison For Hacking Computer Systems Of His Former Employer - Causing Company To Go Out Of Business (2010)

Dariusz Prugar worked as a IT Systems Administrator for an Internet Service Provider (Pa Online) until June 2010. But after a series of personal issues, he was let go.

Prugar logged into PA Online's network, using his old username and password. With his network privileges he was able to install backdoors and retrieve code that he had been working on while employed at the ISP.

Prugar tried to cover his tracks, running a script that deleted logs, but this caused the ISP's systems to crash, impacting 500 businesses and over 5,000 residential customers of PA Online, causing them to lose access to the internet and their email accounts.

According to court documents, that could have had some pretty serious consequences: "Some of the customers were involved in the transportation of hazardous materials as well as the online distribution of pharmaceuticals."

Unaware that Prugar was responsible for the damage, PA Online contacted their former employee requesting his help. However, when Prugar requested the rights to software and scripts he had created while working at the firm in lieu of payment. Pa Online got suspicious and called in the FBI.

A third-party contractor was hired to fix the problem, but the damage to PA Online's reputation was done and the ISP lost multiple clients.

Prugar ultimately pleaded guilty to computer hacking and wire fraud charges, and received a two year prison sentence alongside a $26,000 fine.

And PA Online? Well, they went out of business in October 2015. (Source)

Former IT Administrator Sentenced To Prison For Attempting Computer Sabotage On 70 Company Servers / Feared He Was Going To Be Laid Off (2005)

Yung-Hsun Lin was a former Unix System Administrator at Medco Health Solutions Inc.'s Fair Lawn, N.J. He pleaded guilty in federal court to attempting to sabotage critical data, including individual prescription drug data, on more than 70 servers.

Lin was one of several systems administrators at Medco who feared they would get laid off when their company was being spun off from drug maker Merck & Co. in 2003, according to a statement released by federal law enforcement authorities. Apparently angered by the prospect of losing his job, Lin on Oct. 2, 2003, created a "logic bomb" by modifying existing computer code and inserting new code into Medco's servers.

The bomb was originally set to go off on April 23, 2004, on Lin's birthday. When it failed to deploy because of a programming error, Lin reset the logic bomb to deploy on April 23, 2005, despite the fact that he had not been laid off as feared. The bomb was discovered and neutralized in early January 2005, after it was discovered by a Medco computer systems administrator investigating a system error.

Had it gone off as scheduled, the malicious code would have wiped out data stored on 70 servers. Among the databases that would have been affected was a critical one that maintained patient-specific drug interaction information that pharmacists use to determine whether conflicts exist among an individual's prescribed drugs. Also affected would have been information on clinical analyses, rebate applications, billing, new prescription call-ins from doctors, coverage determination applications and employee payroll data. (Source)

Chicago Airport Contractor Employee Sets Fire To FAA Telecommunications Infrastructure System - September 26, 2014

In the early morning hours of September 26, 2014, the Federal Aviation Administration's (FAA) Chicago Air Route Traffic Control Center (ARTCC) declared ATC Zero after an employee of the Harris Corporation deliberately set a fire in a critical area of the facility. The fire destroyed the Center's FAA Telecommunications Infrastructure (FTI) system – the telecommunications structure that enables communication between controllers and aircraft and the processing of flight plan data.

Over the course of 17 days, FAA technical teams worked 24 hours a day alongside the Harris Corporation to completely rebuild and replace the destroyed communications equipment. They restored, installed and tested more than 20 racks of equipment, 835 telecommunications circuits and more than 10 miles of cables. (Source)

Lottery Official Tried To Rig $14 Million+ Jackpot By Inserting Software Code Into Computer That Picked Numbers - Largest Lottery Fraud In U.S. History - 2010

This incident happened in 2010, but the articles on the links below are worth reading, and are great examples of all the indicators that were ignored.

Eddie Tipton was a Lottery Official in Iowa. Tipton had been working for the Des Moines based Multi-State Lottery Association (MSLA) since 2003, and was promoted to the Information Security Director in 2013.

Tipton was first convicted in October 2015 of rigging a $14.3 Million drawing of the MSLA lottery game Hot Lotto. Tipton never got his hands on the winning total, but was sentenced to prison. Tipton was released on parole in July 2022.

Tipton and his brother Tommy Tipton were subsequently accused of rigging other lottery drawings, dating back as far as 2005. Based on forensic examination of the random number generator that had been used in a 2007 Wisconsin lottery incident, investigators discovered that Eddie Tipton programmed a lottery random number generator to produce special results if the lottery numbers were drawn on certain days of the year.

That software code was replicated on as many as 17 state lottery systems, as the MSLA random-number software was designed by Tipton. For nearly a decade, it allowed Tipton to rig the drawings for games played on three dates each year: May 27, Nov. 23 and Dec. 29.

Tipton ultimately confessed to rigging other lottery drawings in Colorado, Wisconsin, Kansas and Oklahoma.

UNDERAPPRECIATED / OVERWORKED / NO OVERSIGHT

Eddie Tipton was making almost $100,000 a year. But he felt underappreciated and overworked at the time he wrote the code to hack into the national lottery system.

He was working 50- to 60-hour weeks and often was in the office until 11 p.m. His managers expected him to take on far more roles than were practical, he complained.

Tipton Stated: "I wrote software. I worked on Web pages. I did network security. I did firewalls," he said in his confession. "And then I did my regular auditing job on top of all that. They just found no limits to what they wanted to make me do. It even got to the point where the word 'slave' was used."

Nobody at the MSLA oversaw his complete body of work, and few people truly cared about security, he said. That lack of oversight allowed Tipton to write, install and use his secret code without discovery.
Video Complete Story Indicators Overlooked / Ignored

WORKPLACE VIOLENCE

Spectrum Cable Company Ordered By Judge To Pay $1.1 BILLION After Customer Was Murdered By Spectrum Employee - September 20, 2022

A Texas judge ruled that Charter Spectrum must pay about $1.1 billion in damages to the estate and family members of 83 year old Betty Thomas, who was murdered by a cable repairman inside her home in 2019.

A jury initially awarded more than $7 billion in damages in July, but the judge lowered that number to roughly $1.1 Billion.

Roy Holden, the former employee who murdered Thomas, performed a service call at her home in December 2019. The next day, while off-duty, he went back to her house and stole her credit cards as he was fixing her fax machine, then stabbed her to death before going on a spending spree with the stolen cards.

The attorneys also argued that Charter Spectrum hired Holden without reviewing his work history and ignored red flags during his employment. (Source)

Doctor Working At Surgical Facility Arrested For Injecting Poison Into IV Bags Of 11 Patients / Resulting In 1 Death / Was In Retaliation For Medical Misconduct Probe - September 27, 2022

Raynaldo Rivera Ortiz Jr., is a Texas Anesthesiologist. He was arrested on criminal charges related to allegedly injecting nerve blocking and bronchodilation drugs into patient IV bags at a local surgical center, resulting in at least one death and multiple cardiac emergencies.

On or around June 21, 2022 a 55 year old female coworker of Ortiz, experienced a medical emergency and died immediately after treating herself for dehydration using an IV bag of saline taken from the surgical center. An autopsy report revealed that she died from a lethal dose of bupivacaine, a nerve blocking agent.

Two months later, on or around Aug. 24, 2022 an 18 year old male patient experienced a cardiac emergency during a scheduled surgery. The teen was intubated and transferred to a local ICU. Chemical analysis of the fluid from a saline bag used during his surgery revealed the presence of epinephrine, bupicavaine, and lidocaine.

Surgical center personnel concluded that the incidents listed above suggested a pattern of intentional adulteration of IV bags used at the surgical center. They identified about 10 additional unexpected cardiac emergencies that occurred during otherwise unremarkable surgeries between May and August 2022 .

The complaint alleges that none of the cardiac incidents occurred during Dr. Ortiz's surgeries, and that they began just two days after Dr. Oritz was notified of a disciplinary inquiry stemming from an incident during which he allegedly "deviated from the standard of care" during an anesthesia procedure when a patient experienced a medical emergency. The complaint alleges that all of the incidents occurred around the time Dr. Ortiz performed services at the facility, and no incidents occurred while Dr. Ortiz was on vacation.

The complaint further alleges that Dr. Ortiz had a history of disciplinary actions against him, and he had expressed his concern to other physicians over disciplinary action at the facility, and complained the center was trying to "crucify" him.

A nurse who worked on one of Dr. Ortiz's surgeries told law enforcement that Dr. Ortiz refused to use an IV bag she retrieved from the warmer, physically waving the bag off. A surveillance video from the center's operating room hallway showed Dr. Ortiz placing IV bags into the stainless-steel bag warmer shortly before other doctors' patients experienced cardiac emergencies.

The complaint alleges that in one instance captured in the surveillance video, Dr. Ortiz was observed walking quickly from an operating room to the bag warmer, placing a single IV bag inside, visually scanning the empty hallway, and quickly walking away. Just over an hour later, according to the complaint, a 56-year-old woman suffered a cardiac emergency during a scheduled cosmetic surgery after a bag from the warmer was used during her procedure. The complaint alleges that in another instance, agents observed Dr. Ortiz exit his operating room carrying an IV bag concealed in what appeared to be a paper folder, swap the bag with another bag from the warmer, and walk away. Roughly half an hour later, a 54-year-old woman suffered a cardiac emergency during a scheduled cosmetic surgery after a bag from the warmer was used during her procedure. (Source)

Former Nurse Charged With Murder Of 2 Patients At Hospital, Nearly Killing 3rd By Administering Lethal Doses Of Insulin - October 26, 2022

Jonathan Hayes, a 47-year-old former Nurse at Atrium Health Wake Forest Baptist Medical Center in Winston-Salem, North Carolina, has been charged with 2 counts of murder and 1 count of attempted murder.

O'Neill said that on March 21, a team of investigators at the hospital presented him with information that Hayes may have administered a lethal dose of insulin to one patient and indicated there may be other victims.

The 1 count of murder against Hayes is related to the death of 61 year old Jen Crawford. Hayes administered a lethal dose of insulin to Crawford on Jan. 5. She died three days later.

The 2 count of murder is in connection with the death of 62-year-old Vickie Lingerfelt, who was administered a lethal dose of insulin on Jan. 22. She died on Jan. 27.

Hayes is also charged with administering a near-lethal dose of insulin to 62-year-old Pamela Little on Dec. 1, 2021. Little survived and Hayes faces one count of attempted murder.

Hayes was terminated from the hospital in March 2022, and he was arrested In October 2022. (Source)

Hospital Nurse Alleged Killer Of 7 Babies / 15 Attempted Murders - October 13, 2022

A neonatal nurse in the U.K. who allegedly murdered 7 babies and attempted to kill 10 more wrote notes reading, "I don't deserve to live," "I killed them on purpose because I'm not good enough to care for them. I am a horrible evil person."

Lucy Letby, 32, who worked in the Neonatal Unit of the Countess of Chester Hospital, left handwritten notes in her home that police found when they searched it in 2018, prosecutor Nick Johnson stated during her trial in October 2022.

Johnson argued that Letby was a constant, malevolent presence in the neonatal unit. Of the babies Letby allegedly murdered or attempted to murder between 2015 and 2016, the prosecution said she injected some with insulin or milk, while another she injected with air. She allegedly attempted to kill one baby three times.

Johnson told jurors the hospital had been marked by a significant rise in the number of babies who were dying and in the number of serious catastrophic collapses" after January 2015, before which he said its rates of infant mortality were comparable to other busy hospitals.

Investigators found Letby was the "common denominator," and that the infant deaths aligned with her shifting work hours.

Letby pleaded not guilty to seven counts of murder and 15 counts of attempted murder. Her trial is slated to last for up to six months. (Source)

Former Veterans Affairs Medical Center Nursing Assistant Sentenced To 7 Consecutive Life Sentences For Murdering 7 Veterans - May 11, 2021

Reta Mays was sentenced to 7 consecutive life sentences, one for each murder, and an additional 240 months for the eight victim. Mays pleaded guilty in July 2020 to 7 counts of second-degree murder in the deaths of the veterans. She pleaded guilty to one count of assault with intent to commit murder involving the death of another veteran.

Mays was employed as a nursing assistant at the Veterans Affairs Medical Center (VAMC) in Clarksburg, West Virginia. She was working the night shift during the same period of time that the veterans in her care died of hypoglycemia while being treated at the hospital. Nursing assistants at the VAMC are not qualified or authorized to administer any medication to patients, including insulin. Mays would sit one-on-one with patients. She admitted to administering insulin to several patients with the intent to cause their deaths.

This investigation, which began in June 2018, involved more than 300 interviews; the review of thousands of pages of medical records and charts; the review of phone, social media, and computer records; countless hours of consulting with some of the most respected forensic experts and endocrinologists; the exhumation of some of the victims; and the review of hospital staff and visitor records to assess their potential interactions with the victims. (Source)

Indianapolis FedEx Shooter That Killed 8 People Was Former FedEx Employee With Mental Health Problems - April 20, 2021

Police say the 19 year old Indianapolis man who fatally shot 8 people at a southwest side FedEx Ground facility in April had planned the attack for at least nine months.

In a press conference, local and federal officials said the shooting was "an act of suicidal murder" in which Bandon Scott Hole decided to kill himself "in a way he believed would demonstrate his masculinity and capability while fulfilling a final desire to experience killing people."

Hole worked at the FedEx facility between August and October 2020. Police believe he targeted his former workplace not because he was trying to right a perceived injustice, but because he was familiar with the "pattern of activity" at the site.

FBI Indianapolis Special Agent in Charge Paul Keenan said Hole's focus on proving his masculinity was partially connected to a failed attempt to live on his own, which ended with him moving back into his old house. Investigators also learned Hole aspired to join the military. Authorities said he had been eating MREs, or meals ready-to-eat, like those consumed by members of the armed forces.

Keenan also said Hole had suicidal thoughts that "occurred almost daily" in the months leading up to the shooting. The police had previously responded to Hole's home in March 2020 on a mental health check. Hole was put under an immediate detention at a local hospital and a gun he had recently bought was confiscated. Hole would later buy more guns and use them in the FedEx shooting, according to police. (Source)

Former Xerox Employee Receives Life In Prison For Credit Union Robbery And Murder - September 22, 2020

On August 12, 2003, Richard Wilbern walked into Xerox Federal Credit Union, located on the Xerox Corporation campus, and committed robbery and murder. Wilbern was not caught until 2016 for robbery and murder, and was sentenced this week to life in prison.

Richard Wilbern walked into Xerox Federal Credit Union (XFCU) and was wearing a dark blue nylon jacket with the letters FBI written in yellow on the back of the jacket, sunglasses and a poorly fitting wig. Wilbern was also carrying a large briefcase, a green and gray-colored umbrella and had what appeared to be a United States Marshals badge hanging on a chain around his neck.

Wilbern was employed by Xerox between September 1996 and February 23, 2001 as which time he was terminated for repeated employment related infractions. In 2001, Wilbern filed a lawsuit against Xerox alleging that the company unlawfully discriminated against him with respect to the terms and conditions of his employment, subjected him to a hostile work environment, failed to hire him for a position for which he applied because of his race, and retaliated against him for complaining about Xerox's discriminatory treatment. Wilbern also maintained a checking and savings accounts at the Xerox Federal Credit Union. Evidence at trial demonstrated that Wilbern was in significant financial distress from roughly 2000 – 2003, including filing for bankruptcy.

In March 2016, a press conference was held to seek new leads in the investigation. Details of the crime were released as well as photographs of Wilbern committing the robbery. Anyone with information was asked to call a dedicated hotline.

On March 27, 2016, a concerned citizen contacted the Federal Bureau of Investigation and indicated that the person who committed the crime was likely a former Xerox employee named Richard Wilbern. The citizen indicated that the defendant worked for Xerox prior to the robbery but had been fired. The citizen also stated that they recognized Wilbern's face from the photos.

In July 20016, FBI agents met with Wilbern regarding a complaint he had made to the FBI regarding an alleged real estate scam. During one of their meetings, agents obtained a DNA sample from Wilbern after he licked and sealed an envelope. That envelope was sent to OCME, and after comparing the DNA profile from the envelope to the DNA profile previously developed from the umbrella, determined there was a positive match. (Source)

Florida Best Buy Driver Murders 75 Year Old Woman While Delivering Her Appliances - Lawyers Said The Murder Was Preventable If Best Buy Had Better Screened Employees' - September 30, 2019

A Boca Raton family has filed a wrongful death lawsuit against Best Buy. This comes after allegations a delivery man for the company killed a 75-year-old woman while delivering appliances.

The family of 75 year old Evelyn Udell has filed a wrongful death lawsuit to hold Best Buy, two delivery contractors and the two deliverymen, accountable for her death.

Lawyers say the fatal attack was preventable if the companies had further screened their employees'.

On August 19th, police say Jorge Lachazo and another man were delivering a washer and dryer the Udells had bought from Best Buy.

Police say Lachazo beat Udell with a mallet, poured acetone on her body and set her on fire. She died the next day. Lachazo was arrested and is charged with murder.

According to the lawsuit, Best buy stores did nothing to investigate, supervise, or oversee the personnel used to perform these services on their behalf. Worse, it did nothing to advise, inform, or warn Mrs. Udell that the delivery and installation services had been delegated to a third-party.

Lawyers are also calling for sweeping changes to how businesses screen workers who have to go inside a customers' home. (Source)

WORKPLACE VIOLENCE (WPV) INSIDER THREAT INCIDENTS E-MAGAZINE
This e-magazine contains WPV incidents that have occurred at organizations of all different types and sizes.

View On The Link Below Or Download The Flipboard App To View On Your Mobile Device
https://flipboard.com/@cybercops911/insider-threat-workplace-violence-incidents-e-magazine-last-update-8-1-22-r8avhdlcz

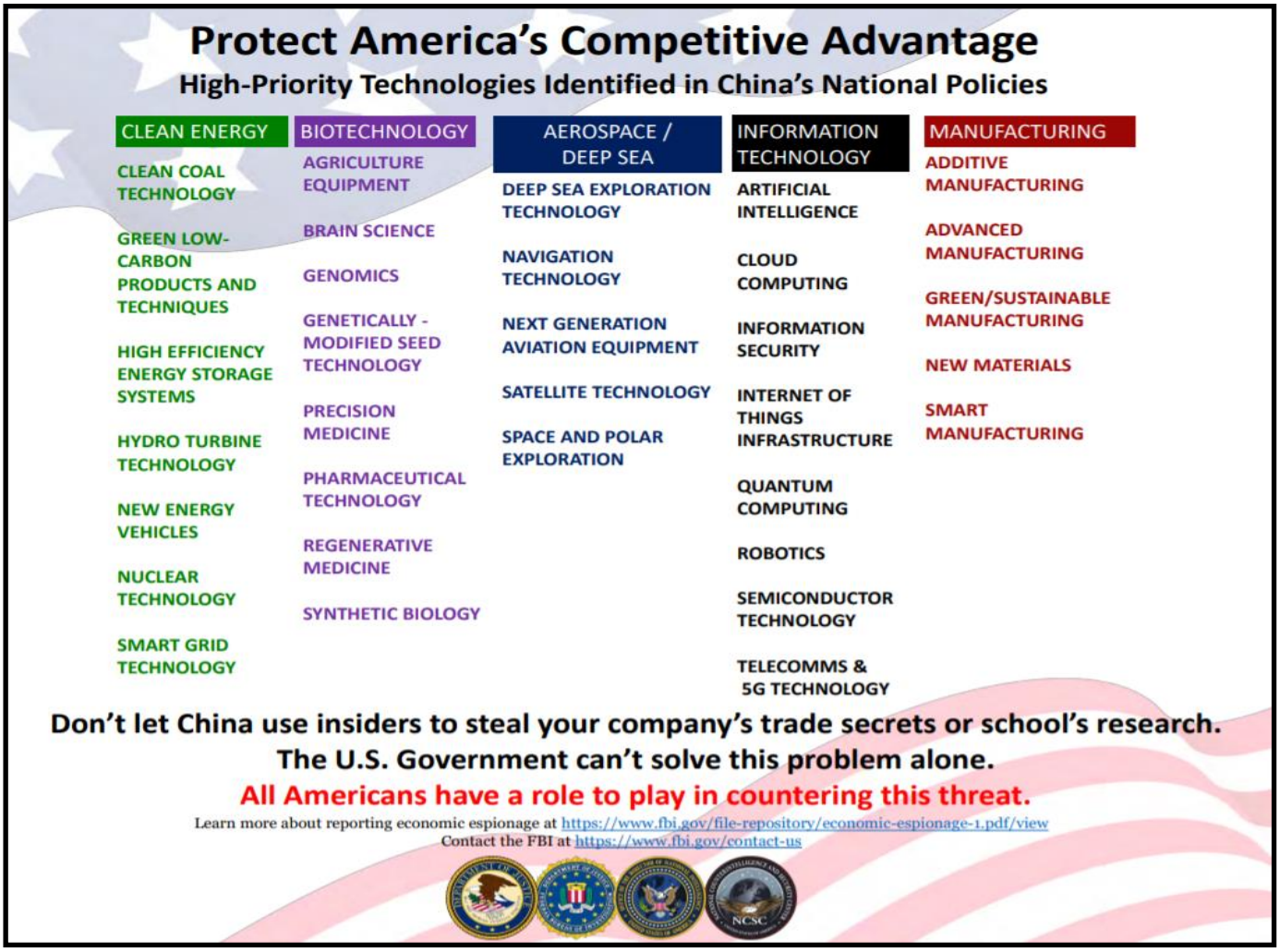
WORKPLACE VIOLENCE TODAY E-MAGAZINE
https://www.workplaceviolence911.com/node/994

INSIDERS WHO STOLE TRADE SECRETS / RESEARCH FOR CHINA / OR HAD TIES TO CHINA

CTTP = China Thousand Talents Plan

- NIH Reveals That 500+ U.S. Scientist's Are Under Investigation For Being Compromised By China And Other Foreign Powers
- U.S. Petroleum Company Scientist STP For $1 Billion Theft Of Trade Secrets - Was Starting New Job In China
- Cleveland Clinic Doctor Arrested For $3.6 Million Grant Funding Fraud Scheme Involving CTTP
- Hospital Researcher STP For Conspiring To Steal Trade Secrets And Sell Them in China With Help Of Husband
- Employee Of Research Institute Pleads Guilty To Steal Trade Secrets To Sell Them In China
- Raytheon Engineer STP For Exporting Sensitive Military Technology To China
- GE Power & Water Employee Charged With Stealing Turbine Technologies Trade Secrets Using Steganography For Data Exfiltration To Benefit People's Republic of China
- CIA Officer Charged With Espionage Over 10 Years Involving People's Republic of China
- Massachusetts Institute of Technology (MIT) Professor Charged With Grant Fraud Involving CTTP
- Employee At Los Alamos National Laboratory Receives Probation For Making False Statements About Being Employed By CTTP
- Texas A&M University Professor Arrested For Concealing His Association With CTTP
- West Virginia University Professor STP For Fraud And Participation In CTTP
- Harvard University Professor Charged With Receiving Financial Support From CTTP
- Visiting Chinese Professor At University of Texas Pleads Guilty To Lying To FBI About Stealing American Technology
- Researcher Who Worked At Nationwide Children's Hospital's Research Institute For 10 Years, Pleads Guilty To Stealing Scientific Trade Secrets To Sell To China
- U.S. University Researcher Charged With Illegally Using $4.1 Million In U.S. Grant Funds To Develop Scientific Expertise For China
- U.S. University Researcher Charged With VISA Fraud And Concealed Her Membership In Chinese Military
- Chinese Citizen Who Worked For U.S. Company Convicted Of Economic Espionage, Theft Of Trade Secrets To Start New Business In China
- Tennessee University Researcher Who Was Receiving Funding From NASA Arrested For Hiding Affiliation With A Chinese University
- Engineers Found Guilty Of Stealing Micron Secrets For China
- Corning Employee Accused Of Theft Of Trade Secrets To Help Start New Business In China
- Husband And Wife Scientists Working For American Pharmaceutical Company, Plead Guilty To Illegally Importing Potentially Toxic Lab Chemicals And Illegally Forwarding Confidential Vaccine Research to China
- Former Coca-Cola Company Chemist Sentenced To Prison For Stealing Trade Secrets To Setup New Business In China
- Former Scientist Convicted For Role With Sister To Steal Trade Secrets From GlaxoSmithKline Worth $10 BILLION To Setup Business In China
- University Of Kansas Researcher Convicted For Hiding Ties To Chinese Government
- Former Employee (Chinese National) Sentenced To Prison For Conspiring To Steal Trade Secret From U.S. Company
- Federal Indictment Charges People's Republic Of China Telecommunications Company With Conspiring With Former Motorola Solutions Employees' To Steal Technology

- Former U.S. Navy Sailor Sentenced To Prison For Selling Export Controlled Military Equipment To China With Help Of Husband Who Was Also In Navy
- Former Broadcom Engineer Charged With Theft Of Trade Secrets - Provided Them To His New Employer A China Startup Company



SOURCES FOR INSIDER THREAT INCIDENT POSTINGS

Produced By: National Insider Threat Special Interest Group / Insider Threat Defense Group

The websites listed below are updated monthly with the latest incidents.

INSIDER THREAT INCIDENTS E-MAGAZINE

2014 To Present

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**4,400+ Incidents**).

View On This Link. Or Download The Flipboard App To View On Your Mobile Device

https://flipboard.com/@cybercops911/insider-threat-incidents-magazine-resource-guide-tkh6a9b1z

INSIDER THREAT INCIDENTS MONTHLY REPORTS

July 2021 To Present

http://www.insiderthreatincidents.com **or**
https://nationalinsiderthreatsig.org/nitsig-insiderthreatreportssurveys.html

INSIDER THREAT INCIDENTS POSTINGS WITH DETAILS

https://www.insiderthreatdefense.us/category/insider-threat-incidents/

Incident Posting Notifications

Enter your e-mail address in the Subscriptions box on the right of this page.
https://www.insiderthreatdefense.us/news/

INSIDER THREAT INCIDENTS COSTING $1 MILLION TO $1 BILLION +

https://www.linkedin.com/post/edit/6696456113925230592/

INSIDER THREAT INCIDENTS POSTINGS ON TWITTER

https://twitter.com/InsiderThreatDG
Follow Us On Twitter: @InsiderThreatDG

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS

https://www.nationalinsiderthreatsig.org/crticial-infrastructure-insider-threats.html

National Insider Threat Special Interest Group (NITSIG)

NITSIG Overview

The NITSIG was created in 2014 to function as a National Insider Threat Information Sharing & Analysis Center. The mission of the NITSIG is to provide organizations and individuals with a ***central source*** for Insider Threat Mitigation (ITM) guidance and collaboration.

The NITSIG Membership (**Free**) is the largest network (**1000+**) of ITM professionals in the U.S. and globally. We our proud to be a conduit for the collaboration of ITM information, so that our members can share and gain information and contribute to building a common body of knowledge for ITM. Our member's willingness to share information has been the driving force that has made the NITSIG very successful.

The NITSIG Provides Guidance And Training The Membership And Others On;

- ✓ Insider Threat Program (ITP) Development, Implementation & Management
- ✓ ITP Working Group / Hub Operation
- ✓ Insider Threat Awareness and Training
- ✓ ITM Risk Assessments & Mitigation Strategies
- ✓ User Activity Monitoring / Behavioral Analytics Tools (Requirements Analysis, Guidance)
- ✓ Protecting Controlled Unclassified Information / Sensitive Business Information
- ✓ Workplace Violence Guidance / Active Shooter Response Guidance & Training

The NITSIG has meetings primarily held at the John Hopkins University Applied Physics Lab in Laurel, Maryland and other locations (NITSIG Chapters, Sponsors). There is **NO CHARGE** to attend. See the link below for some of the great speakers we have had at our meetings.
http://www.nationalinsiderthreatsig.org/nitsigmeetings.html

The NITSIG has created a LinkedIn Group for individuals that interested in sharing and gaining in-depth knowledge regarding ITM and Insider Threat Program Management (ITPM). This group will also enable the NITSIG to share the latest news, upcoming events and information for ITM and ITPM. We invite you to join the group. https://www.linkedin.com/groups/12277699

The NITSIG is the creator of the "***Original***" Insider Threat Symposium & Expo (ITS&E). The ITS&E is recognized as the ***Go To Event*** for in-depth real world guidance from ITP Managers and others with extensive ***Hands On Experience*** in ITM.

At the expo are many great vendors that showcase their training, services and products. The link below provides all the vendors that exhibited at the 2019 ITS&E, and provides a description of their solutions for Insider Threat detection and mitigation.
https://nationalinsiderthreatsig.org/nitsiginsiderthreatvendors.html

The NITSIG had to suspend meetings and the ITS&E in 2020 to 2022 due to the COVID outbreak. We are working on resuming meetings in the later part of 2023, and looking at holding the ITS&E in 2024.

NITSIG Insider Threat Mitigation Resources
Posted on the NITSIG website are various documents, resources and training that will assist organizations with their Insider Threat Program Development / Management and Insider Threat Mitigation efforts.
http://www.nationalinsiderthreatsig.org/nitsig-insiderthreatsymposiumexporesources.html

Security Behind The Firewall Is Our Business

The Insider Threat Defense (ITDG) Group is considered a ***Trusted Source*** for Insider Threat Mitigation (ITM) training and consulting services to the: White House, U.S. Government Agencies, Department Of Homeland Security, TSA, Department Of Defense (U.S. Army, Navy, Air Force & Space Force, Marines,) Intelligence Community (DIA, NSA, NGA) Universities, FBI, U.S. Secret Service, DEA, Law Enforcement, Fortune 100 / 500 companies and others; Microsoft Corporation, Walmart, Home Depot, Nike, Tesla Automotive Company, Dell Technologies, Discovery Channel, United Parcel Service, FedEx Custom Critical, Visa, Capital One Bank, BB&T Bank, HSBC Bank, American Express, Equifax, TransUnion, JetBlue Airways, Delta Airlines and many more. The ITDG has provided training and consulting services to over **650+** organizations. (Client Listing)

Over **900+** individuals have attended our highly sought after Insider Threat Program (ITP) Development / Management Training Course (Classroom Instructor Led & Live Web Based) and received ITP Manager Certificates. (Training Brochure)

With over **10+** years of experience providing training and consulting services, we approach the Insider Threat problem and ITM from a realistic and holistic perspective. A primary centerpiece of providing our clients with a comprehensive ITM Framework is that we incorporate lessons learned based on our analysis of ITP's, and Insider Threat related incidents encountered from working with our clients.

Our training and consulting services have been recognized, endorsed and validated by the U.S. Government and businesses, as some of the most ***affordable, comprehensive and resourceful*** available. These are not the words of the ITDG, but of our clients. ***Our client satisfaction levels are in the exceptional range***. We encourage you to read the feedback from our students on this link.

ITDG Training / Consulting Services Offered

Training / Consulting Services (Conducted Via Live Instructor Led Classroom / Onsite / Web Based)

- ✓ ITM Training Workshops For CEO's, C-Suite & ITP Managers / Working Group, Insider Threat Analysts & Investigators
- ✓ ITP Development - Management / ITM / Insider Threat Investigator & Related Training Courses
- ✓ ITM Framework Training (For Organizations Not Interested In Developing An ITP)
- ✓ Insider Threat Vulnerability - ITP Maturity Assessment / Mitigation Guidance
- ✓ Malicious Insider Playbook Of Tactics Assessment / Mitigation Guidance
- ✓ Insider Threat Awareness Training For Employees'
- ✓ Insider Threat Detection Tool Guidance / Pre-Purchasing Evaluation Assistance
- ✓ Customized ITM Consulting Services For Our Clients

For additional information on our training, consulting services and noteworthy accomplishments please visit this link.

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense Group, Inc.
Insider Threat Program (ITP) Development / Management Training Course Instructor
Insider Threat Vulnerability - ITP Maturity Assessment / Mitigation Specialist
Insider Threat Researcher / Speaker
Founder / Chairman Of The National Insider Threat Special Interest Group (NITSIG)
NITSIG Insider Threat Symposium & Expo Director / Organizer
888-363-7241 / 561-809-6800
www.insiderthreatdefense.us / james.henderson@insiderthreatdefense.us
www.nationalinsiderthreatsig.org / jimhenderson@nationalinsiderthreatsig.org