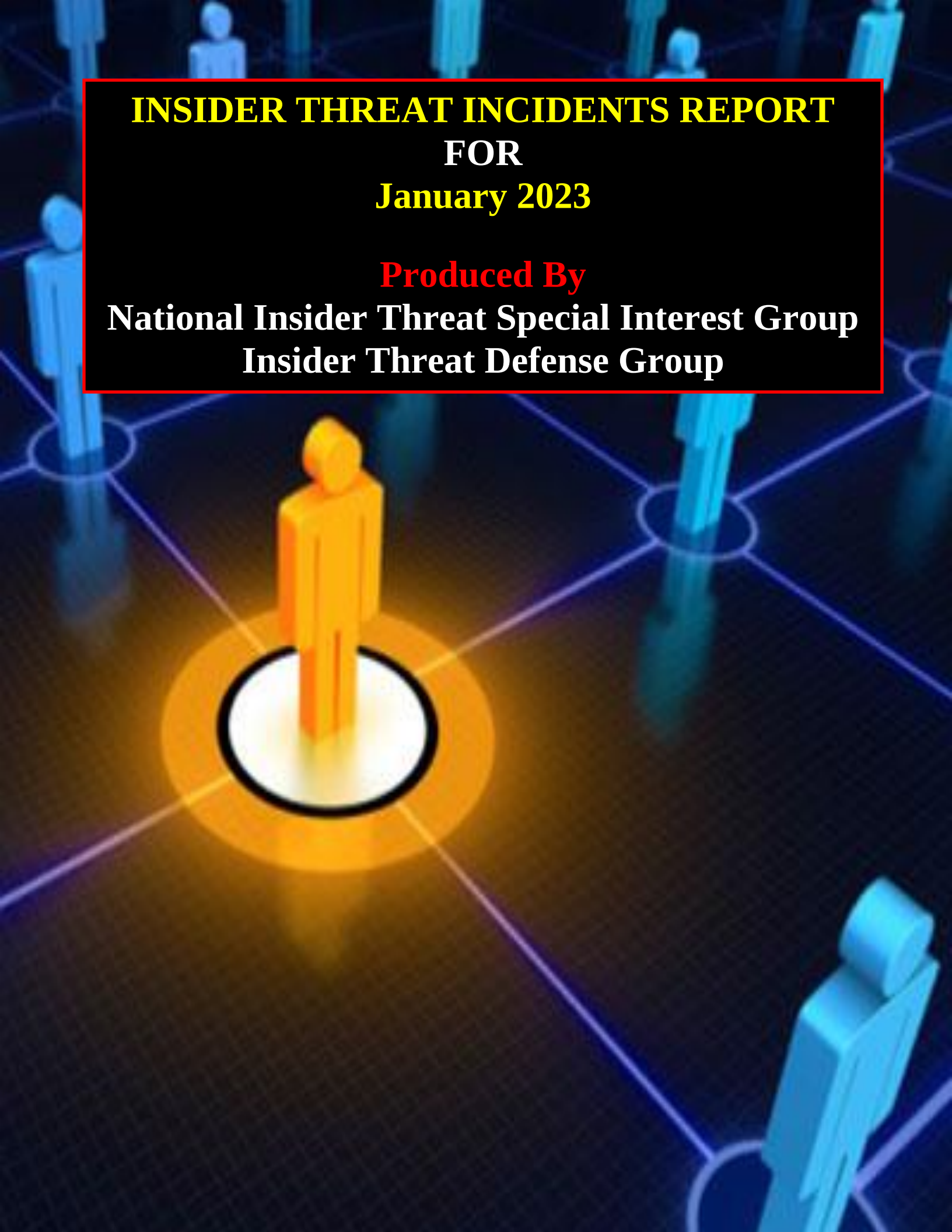

INSIDER THREAT INCIDENTS REPORT

FOR

January 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 **4,300+** 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 21 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

INSIDER THREAT INCIDENTS
FOR JANUARY 2023

FOREIGN GOVERNMENT INSIDER THREAT INCIDENTS

Former President of Venezuelan Supreme Court Charged With Accepting $10 Million+ In Bribes To Resolve Court Cases - January 26, 2023

A Miami federal grand jury has indicted Maikel Jose Moreno Perez, who was the former President of the Venezuelan Supreme Court, and current Venezuelan Supreme Court Justice, with conspiring to launder and laundering bribes he received in exchange for using his position to resolve civil and criminal cases in Venezuela to favor bribe payers.

According to the criminal charging documents, as President of the Venezuelan Supreme Court, Perez had the power to influence judicial decisions in Venezuela because he had the authority to determine the panel of judges hearing cases at the Supreme Court and the power to appoint or remove lower court judges on the trial and appellate level in Venezuela. This activity went on from 2014 through March 2019.

It is alleged that Perez received more than $10 million dollars in bribes, typically from Venezuelan contractors who had received contracts from Venezuelan government-owned entities. In 2014, prior to his appointment as president of the Supreme Court, he received $1 million via wire transfers to his personal bank account in Miami from a Venezuelan contractor. This money was for agreeing to resolve future Venezuelan criminal cases in favor of this contractor. (Source)

Delhi Police Detain Contract Employee For Breach Of Confidential Information In Connection With Financial Ministry Espionage - January 18, 2023

The Delhi Police have charged a contract employee for the Finance Ministry with violating the Officials Secret Act in advance of the Union Budget, which will be unveiled on February 1. Data entry operator Sumit has been recognised as a contract employee. He was detained, according to the authorities, for selling espionage services to other countries and disclosing secret information to them.

The espionage network that was leaking private information about the Finance Ministry was dismantled by the Delhi Police Crime Branch. Sumit was found to be in possession of one mobile phone, which he was using to communicate top-secret information concerning the Ministry of Finance. (Source)

Former Mexican Secretary Of Public Security Accused Of Working With Cartel And Taking Millions Of Dollars In Bribes - January 17, 2023

Genaro Garcia Luna was Mexico's former Secretary of Public Security.

Luna was arrested in December 2019. He is the highest-ranking Mexican official to ever face trial in the U.S. on drug trafficking charges. Luna was once Mexico’s top security official and in charge of fighting the drug cartels. He is scheduled to go on trial on charges for accepting millions of dollars in bribes in exchange for helping the powerful Sinaloa Cartel move drugs and its members avoid capture. (Source)

U.S. GOVERNMENT

Former United States Postal Service Employee Sentenced To Prison For Stealing Blank Money Orders Valued At Over $4 Million - January 4, 2023

In February 2021, 10,000 blank money orders were reported missing from a USPS post office on Utica Avenue in Brooklyn, New York where Jaleesa Wallace worked. The money orders can be deposited with a financial institution for up to $1,000 each.

Agents recovered over 3,000 of the stolen money orders from Wallace's residence. Over $4 million worth of the stolen money orders have been cashed at various financial institutions throughout the country. Agents also recovered prepaid Department of Labor unemployment benefit cards and approximately $43,000 in cash from Wallace's apartment. Additionally, Wallace was in possession of approximately 42 pieces of mail from the Department of Labor that were not in her name.

Wallace was terminated by the USPS in August 2021. She forfeited the cash seized from her apartment to the United States Postal Inspection Service. A related defendant, Willie Cook, pleaded guilty to mail theft in March 2022 and is awaiting sentencing. (Source)

Department of Transportation Border Investigator Pleads Guilty To Extortion Of Trucking Company - January 13, 2023

Patrick Gorena was a Border Investigator for Department of Transportation (DOT)'s Federal Motor Carrier Safety Administration.

Gorena admitted that when auditing a trucking company, he did not report safety violations that would have exposed the company to potential fines and the loss of their DOT license. In return, Gorena demanded $3,500.

However, he ultimately accepted $2,000 from an undercover law enforcement officer posing as a representative of the trucking company. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Fort Stewart Soldier Sentenced To Prison For Role In $3.5 Million+ COVID-19 Fraud Scheme - January 9, 2023

Dara Buck, a U.S. Army Chief Warrant Officer, stationed at Fort Stewart, has been sentenced to federal prison for leading a prolific fraud scheme in which she and others illegally raked in millions of dollars from COVID-19 relief programs and federal student loan forgiveness.

From August 2017 through May 2021, Buck led a conspiracy to fraudulently obtain funding from the Coronavirus Aid, Relief, and Economic Security (CARES) Act's Paycheck Protection Program (PPP), and to secure the fraudulent discharge of federal student loans using falsified disability claims.

Buck admitted submitting more than 150 fraudulent PPP loan applications to the Small Business Administrating for herself and others in the conspiracy, resulting in more than $3 million in fraudulent disbursements from banks to members of the conspiracy. Buck directly received fraudulently obtained PPP funding, or was paid by conspirators for submitting their fraudulent applications.

In addition, conspirators paid Buck to submit falsified U.S. Department of Veterans Affairs certifications for total and permanent disability to the U.S. Department of Education in order to fraudulently secure the discharge of more than a dozen student loans totaling more than $1 million. (Source)

Veterans Affairs Medical Center Pharmacy Employee Pleads Guilty To Role In Stealing $400,00+ Of Diabetic Test Strips - January 11, 2023

Jennifer Robertson spent over 20 years in procurement for the Battle Creek Veterans Affairs Medical Center Pharmacy. She was responsible for ordering supplies for veterans in need of medical care.

In June 2017, Robertson stole 10 boxes of diabetic test strips from the pharmacy's inventory, and arranged online to meet Michelle McAllister and sell them for cash. After completing that transaction and several similar ones, McAllister realized that Robertson's test strips were stolen, but decided to keep buying from her. Robertson and McAllister conducted hundreds of such transactions. Throughout the scheme, Robertson admitted stealing over 7,500 boxes of diabetic test strips, costing the Battle Creek VA Pharmacy over $400,000. (Source)

Retired Air Force Captain & 3 Active Duty Air Force / Navy Officers Detained In Espionage Case Involving China - January 4, 2023

A retired Air Force Captain and 3 active military officers in the Air Force and Navy were detained in Taiwan on suspicion of spying for communist China, while 3 other active officers in the military were released on bail.

Prosecutors and investigators with the Investigation Bureau had been collecting evidence of their alleged involvement in spying, and they brought the seven individuals in for questioning on Tuesday to the Kaohsiung Branch of the Taiwan High Prosecutors Office.

After the questioning, the prosecutors in charge of the case filed a motion to detain the retired caption, surnamed Liu (劉), a commander surnamed Sun (孫), and two lieutenant commanders identified by their surnames Liu and Kung (龔).

The investigation into the case remains ongoing, as investigators continue to look into whether more military officers were involved.

According to the investigation's findings to date, Liu began doing business in China after retiring from the Air Force in 2013.

He was then recruited by the Chinese side to serve as a spy and, using his personnel connections in the military, help recruit active military officers in the Navy and Air Force to join in the spying activities, according to prosecutors.

Prosecutors believe Liu recruited at least six officers into his spy ring and received rewards of between NT$200,000 and NT$700,000 from the Chinese side through a shell company he set up for each individual brought into the fold.

In a statement, the Ministry of National Defense said the case was exposed by some military personnel who offered tip-offs and took the initiative to investigate the espionage allegations. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

Retired FBI Special Agent Charged With Concealing $225,000 In Cash Received From An Outside Source While Being Employeed By FBI - January 23, 2022

Charles McGonigal is former Federal Bureau of Investigation (FBI) Special Agent in Charge of the New York Field Office.

From August 2017, and continuing through and beyond his retirement from the FBI in September 2018, McGonigal concealed from the FBI the nature of his relationship with a former foreign security officer and businessperson who had ongoing business interests in foreign countries and before foreign governments. Specifically, McGonigal requested and received at least $225,000 in cash from the individual and traveled abroad with the individual and met with foreign nationals. The individual later served as an FBI source in a criminal investigation involving foreign political lobbying over which McGonigal had official supervisory responsibility. McGonigal is accused of engaging in other conduct in his official capacity as an FBI Special Agent in Charge that he believed would benefit the businessperson financially. (Source)

Former Correctional Officer Convicted For Role In Accepting Bribes To Smuggle Contraband Into Detention Facility - January 20, 2023

Eight Co-Defendants Previously Pleaded Guilty to Their Roles in the Conspiracy

A former Correctional Officer Andre Davis was convicted for a racketeering conspiracy at the Chesapeake Detention Facility (CDF), in Baltimore, Maryland. Two other correctional officers (COs), four detainees, and two outside facilitators previously pleaded guilty to their roles in the conspiracy, which involved paying bribes to correctional officers to smuggle contraband, including narcotics, tobacco, and cell phones, into the prison. (Source)

The detainees and facilitators paid Davis and his co-defendant COs for smuggled contraband using cash and electronic payment platforms, including Cash App. (Source)

STATE / CITY GOVERNMENTS

Former New Jersey Official Admits Role In Defrauding Health Care Benefit Program Of More Than $4.5 Million For Romantic / Sexual Relationships - January 4, 2023

The former Manager (Harry Pizutelli) of the New Jersey Traumatic Brain Injury Fund (TBI Fund) and one of his conspirators today admitted their roles in a long-running scheme to defraud the fund, a publicly funded health care benefit program, of more than $4.5 million.

Pizutelli was the manager of the TBI Fund and was responsible for its day-to-day operation. He supervised, managed, and oversaw the process by which third-party vendors were paid for services rendered to eligible TBI Fund patients. From 2009 through June 2019, Pizutelli, C.R. Kraus, Maritza Flores, and others conspired to defraud the TBI Fund by misappropriating more than $4.5 million in fraudulent vendor payments for purported services that were never actually provided. Pizutelli orchestrated the distribution of fraudulent vendor payments to Flores, Kraus, and others by generating and processing false invoices and internal payment vouchers. Pizutelli generated these invoices and vouchers to give the appearance that Flores, Kraus, and other conspirators had provided approved services to eligible patients when, in fact, they had not provided any services. Pizutelli then approved and transmitted the internal payment vouchers.

Pizutelli orchestrated these fraudulent payments to maintain and further romantic and / or sexual relationships with Flores and other conspirators.

Pizutelli orchestrated the fraudulent payment of more than $4.5 million from the TBI Fund to members of the conspiracy, including more than $940,000 in fraudulent distributions to Flores and more than $3.245 million in fraudulent distributions to Kraus, which they used for their own personal benefit and enrichment. (Source)

Former County Employee Pleads Guilty To Stealing $1.7+ Million In County Funds By Falsifying Invoices - January 3, 2023

Kevin Gunn pleaded guilty to defrauding Wayne County in Detriot, out of nearly $2 million in taxpayer funds. Gunn, and fellow Wayne County employee John Gibson engaged in a scheme to use taxpayer dollars to make unauthorized purchases of generators and other power equipment from retailers in southeast Michigan which they sold for personal profit.

As part of the scheme to defraud, between January 2019, and August 2021, Gunn and Gibson solicited approved Wayne County vendors to purchase generators and other power equipment from local retailers on behalf of Wayne County. The vendors would then submit invoices for these items to Wayne County.

In order to conceal the scheme to defraud, Gunn instructed the vendors to falsify the invoices they submitted to the Roads Division, and list items the vendors were authorized to sell to the county under their contracts, rather than the generators and power equipment they were unlawfully acquiring at Gunn's and Gibson's request. Roads Division employees would then approve and pay each vendor's invoice with taxpayer funds.

After these fraudulent purchases were verified and approved by Roads Division employees, Gibson took possession of the equipment, paid Gunn for the items, and resold the generators and other items for personal profit.

A review of invoices from Wayne County vendors revealed that between January 16, 2019, and August 3, 2021, Wayne County vendors purchased 596 generators, and a variety of other power equipment including lawnmowers, chainsaws, and backpack blowers. The purchase of these items was not authorized under any vendor contract with Wayne County nor were the items ever provided to or used by Wayne County. The total value of equipment purchased as part of the scheme was approximately $1.7 million in taxpayer funds. (Source)

3 Family Members Of The Former Director Housing Commission Sentenced To Prison for Defrauding HUD Of $336,000 - January 30, 2023

3 family members of the former Executive Director (Lorena Loren) of the St. Clair Housing Commission in Detroit, were sentenced to federal prison after having pleaded guilty to various federal offenses due to their involvement in Loren's fraudulent scheme to steal money from the Section 8 program of the U.S. Department of Housing and Urban Development (HUD).

Lorena Loren (Now Deceased) had previously pleaded guilty and been sentenced to 37 months in prison for conspiring with several family members to steal federal funds provided to the St. Clair Housing Commission by HUD to administer low-income housing programs within St. Clair County. Loren stole approximately $336,000 in federal funds, including money earmarked for HUD's Housing Choice Voucher program, commonly known as Section 8 housing, which allows low-income families to lease privately owned rental properties with the assistance of HUD rental subsidies. (Source)

Former Santa Ana, Califorinia Mayor Pleads Guilty To Accepting $57,000 In Bribes To Support Of Commercial Marijuana Activity - January 13, 2023

The former Mayor of Adelanto has agreed to plead guilty to a federal criminal charge for accepting more than $57,000 in bribes and kickbacks in exchange for approving ordinances authorizing commercial marijuana activity within the city, and ensuring his co-schemers obtained city licenses or permits for their commercial marijuana activities.

From at least November 2015 to June 2018, Richard Kerr executed a scheme to and secretly used his official position to enrich himself and his co-schemers, by passing ordinances authorizing various types of commercial marijuana activities, including marijuana cultivation, marijuana distribution and transportation, and retail sales of marijuana via a dispensary.

Kerr also drafted zones for commercial marijuana activities to include locations used by his supporters, ensured his supporters obtained the licenses or permits they sought; all in violation of conflict-of-interest prohibitions applying to Kerr, in exchange for bribes, kickbacks, gifts, payments, and other things of value. (Source)

Former City Employee Pleads Guilty To Embezzlement / Using City Credit Card For Unauthorized Purchases - January 2, 2023

Trent Fallica who is a former Boulder City, Colorado employee pleaded guilty to an embezzlement charge after being accused of purchasing tools for his own personal use over a period of several years.

The City of Boulder said Fallica had worked for the city in various roles for nearly 20 years. Most recently, he was a Traffic Signal Maintenance Supervisor.

The city said that someone reported that a Transportation and Mobility Department employee was using his city credit card to buy equipment for personal use. The purchases in question appeared to date back to 2017. After an investigation, a warrant was issued for Fallica's arrest and he turned himself in.

The city said Fallica was placed on administrative leave and subsequently resigned. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

CHICAGO SCHOOLS WATCHDOG FINDS HUNDREDS OF EMPLOYEES GROOMED, SEXUALLY ASSAULTED STUDENTS - JANUARY 6, 2023

WARNING: Distrubing Content

In the U.S. Government and corporate world we use words like: Disgruntled Employees, Malicious Employees, Employee Threats, Insider Threats, Insider Risks.

Do school boards across the nation need to implement Insider Threat Programs to protect children from the stories referenced below?

Hundreds of Chicago teachers and school officials sexually groomed and sexually assaulted students or engaged in policy violations over the past four years, according to a report released this week.

The Chicago Public Schools Office of the Inspector General released its annual report Sunday, saying it substantiated more than 70 misconduct allegations out of more than 600 complaints for the 2021-22 school year. Since October 2018, the watchdog said policy violations were found in 302 investigations.

One OIG investigation concluded one teacher groomed and sexually assaulted a 17-year-old student three times. That teacher was charged with multiple counts of sexual assault. After a November 2022 trial, the teacher was acquitted on all counts, the report said, despite evidence provided by the student and social media records.

Another investigation revealed a former JROTC staff member had sex with a high school girl over the course of a year when she was 16 to 17 years old, the report said. The girl was also given alcohol and marijuana and purchased marijuana for him, the OIG said. When the staff member became aware he might be under investigation, he allegedly threatened to kill the girl and her family. He was arrested and eventually sentenced to time served and four years probation after pleading guilty to sexual assault and criminal sexual abuse.

One high school teacher allegedly exchanged 4,000 text messages with a female student, including 400 in one day. The teacher said he was in an open marriage and was "attracted to other people." (Source)

Former School District Official Admits To Role In Embezzling $137,000+ By Paying Kickbacks For Fraudulent Overtime Payments - January 26, 2023

Anthony DeLuca, was a long-term employee of the Hillsborough Township School District, and was promoted to the position of Director of Buildings and Grounds in approximately July 2019. This was a salaried position that did not entitle him to overtime pay.

Shortly after assuming this position, the School District employee to whom DeLuca reported (Referred To As Individual 1), began directing DeLuca to claim that DeLuca was entitled receive overtime payments, including for hours which substantially exceeded those that DeLuca actually worked. DeLuca submitted these claims to Individual 1 who then authorized overtime payments for DeLuca in return for cash kickbacks.

DeLuca admitted that upon receiving the overtime payments approved by Individual 1, DeLuca would typically withdraw cash from his bank account to provide kickbacks to Individual 1.
DeLuca stated that Individual 1 would designate the location to which DeLuca should deliver envelopes containing the cash kickbacks, including the console of Individual 1's vehicle and a drawer in Individual 1's office desk.

DeLuca admitted that through this scheme he received in excess of $137,000 in overtime payments to which he was not entitled and that he provided Individual 1 with at least $39,800 in kickbacks between July 2019 and January 2022. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

Church Treasurer Sentenced To Prison For Embezzling $512,000+ To Pay Credit Card Bills - January 10, 2023

Ralph Tackett was the Treasurer of a church.

Tackett embezzled a total of $512,042.00, in part through the commission of wire fraud. Tackett admitted, among other facts, that from December 2015 until July of 2019, he stole money directly from the church, by transferring funds to pay on his personal credit cards, by issuing checks which he deposited into his own personal and business accounts for his own benefit, and by unlawfully transferring money in other ways, to meet the demands of a third-party. The church endured substantial financial hardship as a result of Tackett's theft. (Source)

BANKING / FINANCIAL INSTITUTIONS

Former Bank Manager Pleads Guilty To Role In Stealing $1.2 Million From Elderly Customers' Account / Used Funds For Personal Expenses - January 6, 2023

During the summer of 2020,Lana Pothos worked as a Relationship Manager at a Bank of America branch in Yorba Linda, California. Pothos an accomplice worked together to steal the savings of approximately $1.2 million from two married senior citizen clients who shared an account with the bank.

In June 2020, Pothos used one victim's personal identifiable information to create an online banking profile for the victim without the victim's knowledge or permission. Using Bank of America's internal computer system, Pothos then changed the victims' mailing address to a hair salon in Yorba Linda that Pothos frequented and also changed their telephone number to a phone number she used. Using that phone number, Pothos called the bank several times while impersonating one of the victims. In July 2020, Pothos' co-schemer opened a new bank account and email address in one victim's name.

On seven occasions from July 2020 to October 2020, approximately $1,212,144 was transferred out of the victims' bank account into the fraudulently opened account Pothos and her accomplice controlled, then transferred again to an account used by the co-schemer at a different bank. The stolen money was then used for personal expenses, including $47,000 that was transferred to a Pothos-controlled entity. (Source)

Former Bank Employee Admits Role In $300,000 Counterfeit Checks Conspiracy - January 24, 2023

Isha-Lee Savage admitted that, while employed by Santander Bank, she accessed customer information and sent screenshots of that information to co-conspirators. The information was used to create fraudulent checks that the leader of the fraud conspiracy, Richard Koboi, provided to other individuals that he solicited on Facebook and paid to deposit the checks into bank accounts that they controlled. Savage also used her position working in the bank's call center to ask customers to provide their debit card information which Savage then provided to her co-conspirators so that they could make fraudulent purchases.

On January 19, 2023, Savonnah Briggs, 28, a now former employee of Citizens Bank, admitted that, while employed by the bank, she similarly accessed customer banking information and check images and provided them to Kobi, who similarly used the information to create fraudulent checks for deposit by himself or others. After the checks were deposited, Koboi and others made, or attempted to make, rapid withdrawals of cash from ATMs or bank tellers.

According to information presented to the court, members of the conspiracy created and deposited approximately $330,000 worth of counterfeit checks. (Source)

Former Bank Employee Admits Role In $300,000+ Fraud Conspiracy Using Fraudulent Personal & Business Checks - January 20, 2023

Savonnah Briggs was previously employed by Citizens Bank.

Briggs admitted to a federal judge that she stole the banking information of unsuspecting individuals, businesses, and a law firm, and then provided that information to the leader of a bank fraud conspiracy, who used it to create fraudulent personal and business checks.

Briggs admitted that while employed by the bank, she accessed customer information and check images, and provided screenshots of that information to Richard Kobi. Kobi then used the stolen information to create fraudulent checks that he deposited into his own bank, or that he provided to other individuals that he solicited

on Facebook and paid to deposit the checks into bank accounts they controlled. After the checks were deposited, Koboi and others made, or attempted to make, rapid withdrawals of cash from ATMs or bank tellers.

The members of the conspiracy created and deposited approximately $330,000 worth of counterfeit checks. (Source)

Former Navy Federal Credit Union Employee Arrested For Dark Web Fraud Scheme - January 3, 2023
Wade Helms was arrested for allegedly participating in a dark web fraud scheme as he worked at Navy Federal Credit Union in Pensacola, Florida.

Law Enforcement Agents discovered that Helms misused his employee access to compromise dozens of credit union member accounts, taking the members' personal identification information and providing it to third parties via the dark web. He also assisted the third parties to gain access to the credit union member accounts, resulting in the third parties stealing funds from the accounts. (Source)

TRADE UNIONS

Former President Of NYPD Sergeants Union Pleads Guilty To Stealing $600,000 From Sergeants Benevolent Association For Luxury Items, Meals - January 21, 2023
Edward Mullins is the former President of the Sergeants Benevolent Association (SBA). This union represents all current and former Sergeants of the New York City Police Department..

Mullins pled guilty to one count of wire fraud in connection with a scheme to steal hundreds of thousands of dollars from the SBA through the submission of fraudulent expense reports.

Beginning in 2017, Mullins devised a scheme to steal hundreds of thousands of dollars from the SBA. Mullins used his personal credit card to pay for meals at high-end restaurants and to purchase luxury personal items, among other things, and then submitted false and inflated expense reports to the SBA, representing that his charges were legitimate SBA expenditures when in fact they were not. Mullins routinely included meals on his expense reports that were not SBA-related. Mullins also inflated the costs of his meals, whether SBA related or not. For example, if the actual cost of a meal was $522.55, Mullins would seek reimbursement from the SBA for $822.55 and pocket the difference. Mullins would also take personal expenses like supermarket bills and claim them on his expense reports as SBA-related meals for which he also sought reimbursement.

Mullins fraudulent expenses were paid through the SBA's Contingent Fund, which is funded primarily through annual dues paid by SBA members. In total, Mullins stole at least $600,000 from the SBA through the filing of hundreds of fraudulent expense reports. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Terminated Employee Arrested For Stealing Medical Records, Extortion, Cyberstalking - December 31, 2022
A former employee at a Selma Animal Hospital has been charged with extortion and cyberstalking. Eduardo Figueroa was arrested December 14 at his residence by Smithfield Police. Stolen medical records from the animal hospital were also recovered at his home, police said.

On December 9, Selma Police were dispatched to For Pet's Sake Animal Hospital. According to a police report, the owner, Dr. Barbara Cotten, told police she had just fired Figueroa earlier that day.

Figueroa had previously made comments the business could be turned to ash if he wished, the report stated. A couple of months earlier, he allegedly made unsettling comments when Dr. Cotten took away his key to the business.

After his termination, staff discovered old medical records belonging to the business were missing. Police obtained an email Figueroa sent to Dr. Cotten demanding a $50 per month fee to prevent him from releasing their customers' private information on the "darknet." The email stated the business had until December 16 to make good on his demands, according to the police report. (Source)

CHINESE ESPIONAGE TARGETING U.S. COMPANIES / UNIVERSITY TRADE SECRETS

Former GE Power Engineer Sentenced To Prison For Stealing Trade Secrets To Benefit China - January 3, 2023

Xiaoqing Zheng was convicted of conspiracy to commit economic espionage. Zheng was employed at GE Power in Schenectady, New York, as an Engineer specializing in turbine sealing technology. He worked at GE from 2008 until the summer of 2018.

The trial evidence demonstrated that Zheng and others in China conspired to steal GE's trade secrets surrounding GE's ground-based and aviation-based turbine technologies, knowing or intending to benefit the People's Republic of China (PRC) and one or more foreign instrumentalities, including China-based companies and universities that research, develop, and manufacture parts for turbines. (Source)

PHARMACEUTICAL COMPANINES / PHARMICIES / HOSPITALS / HEALTHCARE CENTERS / DOCTORS OFFICES

Medical Professional Staffing Company Employee Sentenced To Prison For Role In $127,000 Identity Theft Scheme - January 17, 2023

Roseanna Taylor worked for a medical professional staffing company based in Mobile, Alabama from about May 2017 through January 2019.

Taylor obtained personal information of certain medical professionals. Beginning around 2018, Taylor began creating fake identification documents using this information, along with fraudulent documents, to be used to obtain fraudulent loans. Taylor provided both means of identification and fraudulent loan documents to other members of the conspiracy to assist them in obtaining fraudulent loans. Taylor was ordered to pay restitution to her victims in the amount of $127,663.26. (Source)

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

Former Chief Financial Officer Pleads Guilty To $50 Million Scheme To Defraud Investors And Lenders - January 12, 2023

Nihat Cardak was the former Chief Financial Officer (CFO) of the Virginia-based email security company GigaMedia Access Corporation (DBA GigaTrust).

Cardak pled guilty in connection with a scheme to defraud investors and lenders of millions of dollars through false and misleading misrepresentations, including fabricated bank statements and audit reports, and by impersonating a purported customer, auditor, and GigaTrust lawyer.

From in or about 2016 through at least in or about 2019, GigaTrust was a private company headquartered in Virginia that purported to be a market-leading provider of cloud-based content security solutions.

Robert Bernardi founded GigaTrust and served as its Chief Executive Officer, while Cardak and Sunil Chandra were GigaTrust's CFO and Vice President of Business Development.

The defendants devised a scheme to defraud investors and lenders by (1) fabricating and disseminating false and misleading bank account statements that overstated GigaTrust's cash deposits; (2) fabricating and disseminating false and misleading audit materials that purported to have been issued by GigaTrust's auditors and overstated GigaTrust's performance; (3) forging and disseminating a false and misleading letter purporting to be from GigaTrust's New York-based counsel; and (4) impersonating or causing others to impersonate a purported customer and auditor of GigaTrust on telephone calls with a prospective lender. (Source)

Former Energy Company Executive Sentenced To Prison For $15 Million Investment Fraud / Used Funds For Personal Expenses - January 24, 2023

Between November 2012 and May 2015, Joey Dodson engaged in a scheme to defraud investors while serving as the Executive Chairman and Managing Partner of Citadel Energy (Citadel), which purported to provide fluid-management services to oil and gas companies.

In his role, Dodson was responsible for raising funds, controlling the bank accounts, and disseminating financial information to investors for three limited partnerships affiliated with Citadel. As part of the scheme, Dodson made materially false and misleading representations and omissions to prospective and existing investors about the intended use of investor funds, the status of a potential acquisition by a private-equity firm, and Dodson's own compensation.

After inducing victims to invest, Dodson pooled the funds from the limited partnerships and conducted multiple transfers between Citadel-related accounts in order to divert investor funds for his own benefit and to conceal his actions. In total, Dodson fraudulently raised over $15.6 million from more than 50 investors and misappropriated $1.3 million in investor funds, which he used to pay for his personal expenses and to repay earlier investors in unrelated entities known collectively as Duke Equity. After Dodson's misappropriation was discovered, the limited partnerships were placed into bankruptcy and the investors suffered a total loss of their investments. (Source)

Former Chief Financial Officer Pleads Guilty To $5 Million+ Fraud Scheme - January 3, 2023

Between June 2021 and August 2022, Cooper Morgenthau was the former Chief Financial Officer of two special purpose acquisition companies (SPAC-1, SPAC-2).

Morgenthau embezzled more than $5 million from the two companies. SPAC-1 had recently had its initial public offering, while SPAC-2 was raising money from private investors in preparation for its anticipated IPO. Morgenthau used the embezzled funds to trade equities and options of so-called meme stocks and cryptocurrencies, losing almost all of the money that he stole.

To conceal and facilitate his embezzlement from SPAC-1, Morgenthau fabricated bank statements, which he provided to SPAC-1's Accountant and Auditor. He made material misstatements in SPAC-1's public filings with the Securities and Exchange Commission (SEC), and transferred some of SPAC-2's funds to SPAC-1 to cover up the funds he had misappropriated from SPAC-1. (Source)

Chief Financial Officer Sentenced To Prison for Defrauding Employer And Lender Of $700,000+ - January 10, 2023

Margaret Boisture functioned as the Chief Financial employee of ZoneFlow Reactor Technologies, a pre-revenue company in the business of developing and commercializing a new technology that improves the efficiency of the production of hydrogen.

PayPal marketed and serviced commercial loans from WebBank, a third-party lender. Between approximately October 2016 and February 2020, Boisture defrauded ZoneFlow, PayPal and WebBank by diverting ZoneFlow money to herself; taking unauthorized loans that caused ZoneFlow to pay additional interest expense; and making misrepresentations to PayPal and WebBank to induce them to make unauthorized loans to ZoneFlow that expanded the pool of money from which Boisture could take.

In total, Boisture's criminal conduct caused losses of $632,159.78 to ZoneFlow and $78,088.76 to PayPal and WebBank. (Source)

Former CEO Of Anti-Poverty Nonprofit Organization Pleads Guilty To Embezzling $600,000+ - January 17, 2023

The former President and CEO of an anti-poverty nonprofit agency has agreed to plead guilty to charges for embezzling money from the nonprofit for his personal benefit and intentionally misapplying more than $600,000 in grant money to pay for unauthorized expenses and lying on his tax returns.

From 1996 until he was fired in September 2019, Howard Slingerland was the president and CEO of Youth Policy Institute Inc. (YPI), a nonprofit agency that worked to eradicate poverty in some of the highest needs neighborhoods in Los Angeles.

From January 2015 to February 2019, Slingerland caused at least $71,533 of YPI funds to be spent on unauthorized expenditures, including Slingerland's personal property tax bill that exceeded $14,000, more than $6,000 for a family dinner at a New York City restaurant, nearly $11,000 for a family member's tutoring, and nearly $2,000 on a home computer and software.

In July 2019, Slingerland caused approximately $401,561 in funds YPI had received from a federal grant to be used for the unauthorized payment of YPI payroll. That same month, he also caused approximately $201,466 in federal grant money to be illegally used to pay off YPI's credit card bill, including for expenses Slingerland had incurred. (Source)

Former Amtrak Employee Charged With $26,000 Wire Fraud Scheme Involving 40 Victims - January 9, 2023

Kenya Small was employed by Amtrak as an On-board Services Train Attendant. Small recruited more than 40 victims to purchase spots on a purported June 2019 trip from New Orleans to New York City. Small told the victims that she had booked roundtrip Amtrak train travel for the trip, as well as activities, such as shows and museum visits. In truth, Small had not booked the Amtrak travel or the activities.

When the date of the trip approached, Small told the victims, from whom she had taken a total of approximately $23,000 to $26,000, that Amtrak had canceled the trip because an incident occurred in which one of the trip's passengers assaulted an Amtrak employee and made a bomb threat. In truth, no such incident had occurred.
Small also submitted fraudulent sick benefit claims to the Railroad Retirement Board, a federal agency that provides benefits to Amtrak employees. Small claimed that she was too sick to work when, in truth, she was working another job. (Source)

Brother Of Cryptocurrency Company Employee Sentenced To Prison For Insider Trading Case - January 10, 2023

Beginning in approximately October 2020, Nikhil Wahi obtained information from his brother, an employee of Coinbase (Product Manager), who was working on highly confidential crypto asset listings, secret tips about which crypto assets would be listed on Coinbase. Using that insider information, Wahi used anonymous blockchain wallets and accounts held under pseudonyms at centralized cryptocurrency exchanges to acquire those crypto assets shortly before Coinbase publicly announced that it was listing these crypto assets on its exchanges. On multiple occasions following Coinbase's public listing announcements, Wahi sold the crypto assets for a profit.

In addition to the prison sentence, Wahi was ordered to pay $892,500 in forfeiture. (Source)

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

Executive Director Of Charity Sentenced To Prison For Role In Embezzling $1 Million To Live Lavish Lifestyle + - January 11, 2023

From January 2011 until her termination on May 27, 2016, Wafa Abboud was the Executive Director of Human First, a non-profit corporation that provided services to individuals with autism and other developmental disabilities. In that capacity, Abboud exercised nearly complete control over the charity's finances.

During Abboud's tenure, Human First received tens of millions of dollars annually from the New York State Office for People with Development Disabilities, which is funded in significant part by the Medicaid program.

The money was disbursed to Human First to support its mission of providing residential, rehabilitative, and other services to developmentally disabled youth.

Abboud used multiple fraud schemes to steal over $1 Million from Human First.

Abboud, who used the money to fund a lavish lifestyle, including expensive international vacations, visits to luxury spas and high-end beauty salons and restaurants, and elective cosmetic surgeries, and to finance the down payment and renovation of her residence. (Source)

Restaurant Manager Sentenced To Prison For Embezzling $300,000+ From Employer / Used Funds For Adult Entertainment Clubs - January 5, 2023

Scott Spilberg was hired as the manager at Houck's Grille in August 2020.

Beginning in October 2020, at the height of the COVID-19 pandemic, Spilberg began using his company issued debit card to pay for his visits to two adult entertainment clubs. Ultimately, he visited the clubs more than 50 times during an 11-month period, charging over $300,000 to the company debit card. The loss of this money caused a significant hardship to the restaurant and threatened the livelihood of its 40 employees and forced it to borrow COVID-relief funds to stay in business. (Source)

Former Chief Financial Officer Pleads Guilty For Failing To Pay $3.6M+ In Employee Tax Withholdings And Embezzling $130,000 For Personal Use - January 31, 2023

A former chief financial officer for a company with offices in Oklahoma pleaded guilty in federal court after failing to pay over to the IRS $3.6 million in income and FICA tax withholdings and for embezzling more than $130,000 from the company.

Paul Bowker was the Chief Financial Officer and Vice President of Ffinance at a company that maintained offices in the Northern District of Oklahoma. Bowker was responsible for withholding income taxes and FICA taxes from employees' paychecks and for paying the monies over to the IRS.

From April 2014 through January 2016, Bowker withheld the funds but willfully failed to file quarterly employment tax returns for the company and failed to pay over the majority of the employment taxes owed to the IRS, totaling nearly $3.6 million. During the investigation, agents discovered that the defendant had not embezzled the tax monies that he willfully neglected to pay, and the IRS was able to recover the funds.

Bowker also committed bank fraud as the company's Chief Financial Officer. In his position, Bowker was entrusted with a company's Visa credit card and was responsible for paying the monthly credit card bill by authorizing the electronic transfer of funds from the company's checking account to the company's Visa account. From January 2014 through December 2015, Bowker fraudulently used the Visa credit card to make $130,000 worth of purchases for his own benefit. Bowker purchased items at drug stores, department stores, online retailers, furniture stores, gas stations, and liquor stores. (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

Former Accounts Payable Clerk Sentenced To Prison For Embezzling $712,000 Using Fake Companies / Invoices / Used Money For Personal Expenses - January 20, 2023

Stephenie Stites worked as the Accounts Payable Clerk for Norbrook Inc. In 2020.

Norbrook noticed accounting discrepancies and when confronted, Stites admitted to making approximately $72,000 in unauthorized charges on the company's credit card. A full review showed she'd embezzled more than $712,000 from Norbrook by creating two fake companies and manipulating invoices. Stites spent the stolen money to pay for personal expenses such as home and vehicle expenses, travel, hotels, real estate, and other disbursements. (Source)

THEFT OF COMPANY PROPERTY

Former Government Contractor Sentenced To Probation / Home Confinement For Stealing $550,000 Worth Of Government Property And Selling On eBay - January 4, 2023

Dennis Gamarra was employed as a contractor working at the United States Department of Commerce (DOC) within the International Trade Administration (ITA), at an office in Washington, D.C.

Gamarra largely worked to provide information technology (IT) support to the ITA and through his employment had access to certain government-furnished equipment, including Microsoft Surface tablet devices belonging to DOC and issued to DOC employees

Gamarra stole at least one Microsoft Surface Tablet, worth $1,370, removing it from ITA's offices, advertising it for sale online through his eBay account, and ultimately re-selling it to another individual through eBay.

Starting in November 2019, Defendant Gamarra began working as a contractor for the Library of Congress (LOC), at an office in Washington, D.C. While at LOC, providing IT support services.

While at LOC, Gamarra removed at least 29 separate Dell laptops from LOC that he knew to belong to LOC, cumulatively worth a total of approximately USD $55,590, advertised them on eBay, and ultimately resold them to different customers through that account. (Source)

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

No Incidents To Report

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

No Incidents To Report

EMPLOYEE DRUG RELATED INCIDENTS

Airport Employee & Passenger Charged With Cocaine Possession - January 16, 2023

Customs and Border Protection (CBP) Officers at Cyril E. King Airport were screening passengers on a Spirit Airlines flight from St. Thomas to Orlando.

During the screening, Ahkoy Smith, a ticketed passenger the flight, attempted to flee but was apprehended by CBP officers. A CBP canine later alerted to Smith's backpack which was on his back when he was apprehended. Smith admitted that he packed his backpack and that it belonged to him. CBP officers inspected Smith's backpack and discovered two brick-shaped objects wrapped in black tape which later tested positive for the presence of cocaine and weighed approximately 2.25 kilograms.

Also on January 11, 2023, CBP officers observed Shakari Francis, a Cape Air ramp agent, entering the men's restroom located in the departure terminal shortly after Smith entered the same restroom. Francis admitted that he entered the restroom with two bricks of cocaine which he later delivered to Smith. (Source)

Police Chief Charged With Aiding And Abetting The Distribution Of Cocaine / Meth - January 27, 2023

A Police Chief in Pennsylvania was charged with various drug-related crimes, including aiding and abetting the distribution of cocaine and meth, as well as conspiracy, the Department of Justice announced.

Police Chief Shawn Denning is charged with two counts of aiding and abetting the distribution of a quantity of cocaine, three counts of aiding and abetting the distribution of a quantity of methamphetamine, and one count of conspiracy to possess with the intent to distribute and distribute controlled substances (Methamphetamine, Cocaine). (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

Fired Walmart Employee With Mental Health Problems, Walks Into Break Room And Starts Shooting / Wounding An Individual - January 20, 2023

One person was wounded in a shooting at a Walmart in Evansville, Indiana. The gunman was shot and killed by responding law enforcement, according to the Evansville Police Department.

Police identified the gunman as 25-year-old Ronald Ray Mosley II, who was fired from Walmart in May, according to police spokesperson Sgt. Anna Gray. Mosley was fired after being arrested for multiple battery charges against other employees, Gray said. Mosley had regularly attended mental health treatment after being arrested on battery charges.

Just before the shooting, Mosley left a suicide note at his house on Thursday night, Police Chief Billy Bolin said.

Mosley attended mental health court nearly every two weeks and had attended a hearing on Thursday afternoon related to the battery cases.

The shooting started after Mosley went into a break room in the back of the store when a meeting was about to begin. Roughly 40 shoppers were in the store at the time.

"He told everybody to line up against the wall, he had a gun in his hand, and he told two of them to stay in the middle. He ends up shooting a female at this point," the Police Chief Bolin stated.

The woman was shot in the face and is still being treated at a hospital in stable condition.

Bolin said there was another male in the room that was also an "intended target" but he took off running during the shooting.

When officers arrived, they encountered the Mosley who fired multiple times at officers. Officers fired back, killing the suspect. (Source)

Employee Charged With Killing 7 Co-Workers - January 25, 2023

Chunli Zhao, a farm worker is accused of killing seven of his co-workers in a case of workplace violence, He was charged with seven counts of murder and one count of attempted murder.

Authorities believe Zhao acted alone when he entered a mushroom farm where he worked, and shot and killed four people and seriously wounded a fifth. He then drove to a nearby farm where he worked previously and killed three more people.

One person stated "He was a good person. He was polite and friendly with everyone. He never had any problems with anyone. I don't understand why all this happened."

It would not have been Zhao's first fit of workplace rage, the San Francisco Chronicle reported. In 2013, Zhao was accused of threatening to split a coworker's head open with a knife and separately tried to suffocate the man with a pillow. (Source)

Former Employee Of Health Care Facility Sentenced To Prison For Role In Crimes To Assaults Against Disabled Residents - January 27, 2023

Zachary Dinell and Tyler Smith were employees of an in-patient health care facility located in New Brighton, Pennsylvania. Residents of the facility suffered from a range of severe physical, intellectual, and emotional disabilities, and required assistance with all activities of daily life, including bathing, using the bathroom, oral hygiene, feeding, and dressing. As members of the facility's Direct Care Staff, Dinell admitted that he and Smith were responsible for providing this daily assistance to residents.

From approximately June 2016 to September 2017, Dinell admitted that he and Smith engaged in a conspiracy to commit hate crimes against residents of the facility because of the residents' actual or perceived disabilities. Dinell and Smith carried out assaults in a variety of ways, including by punching and kicking residents, jumping on residents, rubbing hand sanitizer in their eyes, spraying liquid irritants, including mouthwash, in their eyes and mouths, and in one instance removing a resident's compression stocking in a manner intended to inflict pain. Several of these assaults were recorded on Dinell's cell phone.

As part of the conspiracy, Dinell acknowledged that he and Smith exchanged text messages in which they expressed their animus toward the disabled residents, shared pictures and videos of residents, described their assaults, and encouraged each other's continued abuse of residents.

Dinell further admitted that he and Smith were able to avoid detection by, among other things, exploiting their one-on-one access to residents of the facility and the fact that the victims were non-verbal. (Source)

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

EMPLOYEES WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

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)

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 (**4,200+ 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 due to the COVID outbreak. We are working on resuming meetings in the later part of 2021, and looking at holding the ITS&E in 2022.

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