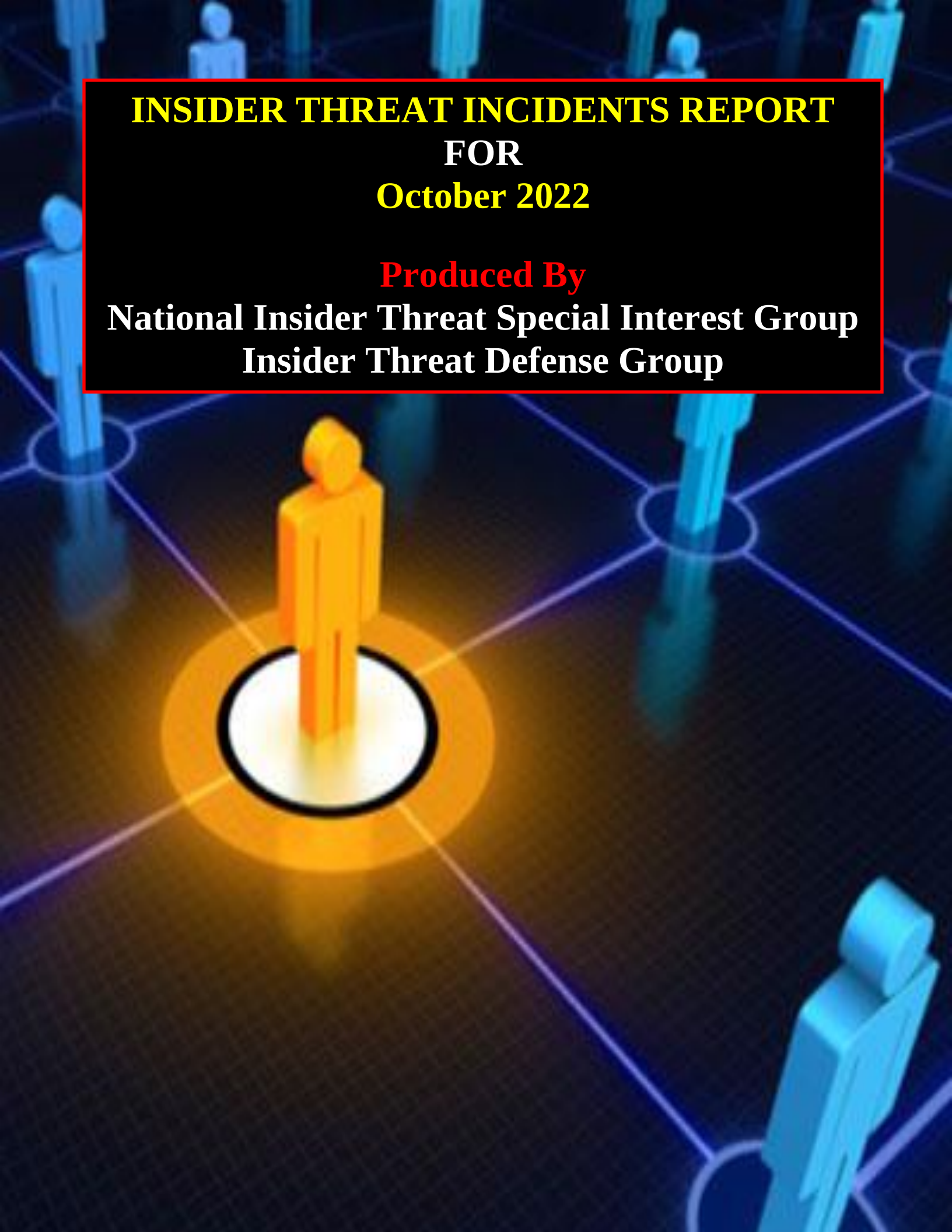

INSIDER THREAT INCIDENTS REPORT
FOR
October 2022

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 **4,100+** 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 25 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 OCTOBER 2022

FOREIGN GOVERNMENT INSIDER THREAT INCIDENTS
No Incidents To Report

U.S. GOVERNMENT
5 Current Or Former IRS Employees Charged With Defrauding Federal COVID-19 Relief Programs - October 4, 2022

5 current or former IRS employees have been charged with schemes to defraud the Paycheck Protection Program (PPP) and Economic Injury Disaster Loan (EIDL) Program, federal stimulus programs authorized as part of the Coronavirus Aid, Relief, and Economic Security (CARES) Act.

The defendants allegedly obtained funds under the PPP and EIDL Program by submitting false and fraudulent loan applications that collectively sought over $1 million. They then used the loan funds for purposes not authorized by the PPP or EIDL Program, but instead for cars, luxury goods, and personal travel, including trips to Las Vegas. (Source)

Former U.S. Postal Service Employee Sentenced To Prison For Stealing Nearly $400,000 In Federal Tax Refund Checks From The Mail - October 24, 2022

Kevin Streeter was employed by the U.S. Postal Service at a mail processing center in Sarasota, Florida.

He exploited his position by stealing approximately 40 federal tax refund checks from the U.S. mail that were enroute to the intended taxpayers living in the Middle District of Florida. Streeter and others then sold or attempted to sell the checks to third parties. The tax refund checks, issued by the U.S. Department of Treasury, ranged in amounts from $4,000 to over $100,000, with an aggregate value of over $398,000. (Source)

U.S. Postal Carrier Charged For Cocaine Distribution Stemming From Using Her Official Position - October 11, 2022

Nathasha Prieto was a United States Postal Carrier, who provided addresses on her postal route to Angel Coss, who arranged for the shipment of packages containing kilograms of cocaine from Puerto Rico to those addresses.

Instead of delivering the packages, Prieto removed the packages from the mail stream so that the cocaine within them could be distributed by Coss. On August 15, 2022, the investigation resulted in the seizure, from Prieto, of packages shipped from Puerto Rico containing kilograms of cocaine. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Owner Of Software Engineering Company Paid Civilian Employee At Randolph Air Force Base $2.3 Million+ In Bribes For 11 Years To Obtain Government Contracts - October 13, 2022

QuantaDyn Corporation is a software engineering company based in Virginia.

One of the owners, and David Bolduc paid Keith Seguin a former civilian employee at Randolph Air Force Base in San Antonio, more than $2.3 million in bribes from 2007 to 2018 to obtain government contracts and government pricing information.

As part of the fraudulent scheme, Bolduc conspired with another employees Karen Paulsen, John Hancock and Seguin to defraud the United States by overcharging to offset the bribe payments and inflate profits for the benefit of Bolduc, QuantaDyn, and the prime contractor that employed Hancock and Paulsen.

From 2007 to 2018, the conspirators fixed the contract award and pricing on Air Force and General Services Administration (GSA) contracts, which caused the United States to overpay for flight simulator technology and simulator services. (Source)

2 Former Robins Air Force Base Daycare Employees Charged For Cruelty To Children, Simple Battery, Failure to Report Suspected Child Abuse - October 12, 2022

The indictment alleges a variety of felony cruelty to children actions committed by Zhanay Flynn and Antanesha Fritz, two former Robins Air Force Base daycare employees, during Jan. and Feb. 2021.

The charges allege various forms of abuse, to include striking children, causing children to fight each other, forcing children to hit one another, spraying children in the face with a cleaning liquid, seizing and shaking a child while threatening to strike them, striking a child in the head with a book, kicking a child into a wall, and stepping on and applying weight to a child's leg. Flynn and Fritz are also accused of committing simple battery against children, with the indictment alleging that they lifted a cot with a child sleeping on it, causing the child to fall on the ground, struck a toy out of a child's hand and then forced the child into a small enclosure, and sprayed two children in the head and face with a cleaning solution. Latona Lambert the former daycare director, Flynn and Fritz are each charged with one count of failing to report suspected child abuse when they did not notify the proper authorities of the abuse after allegedly witnessing it or having reason to suspect that abuse was occurring.

Zhanay Flynn is charged with 18 counts of cruelty to children in the first degree, six counts of cruelty to children in the second degree, three counts of simple battery and one count of failure to report suspected child abuse.

Antanesha Fritz is charged with 18 counts of cruelty to children in the first degree, six counts of cruelty to children in the second degree, three counts of simple battery and one count of failure to report suspected child abuse.

Latona Lambert is charged with one count of failure to report suspected child abuse. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

665 FBI Employees Left Agency After Misconduct Investigations According To Whistleblower Disclosure - October 6, 2022

Sen. Chuck Grassley (R-Iowa) said he obtained internal records from a whistleblower alleging 665 FBI employees retired or resigned following misconduct investigations to avoid receiving final disciplinary letters.

Grassley said the whistleblower provided an internal Justice Department report that indicated the employees left between 2004 and 2020 and included 45 senior-level employees.

"The allegations and records paint a disgraceful picture of abuse that women within the FBI have had to live with for many years," Grassley wrote in a letter to FBI Director Christopher Wray and Attorney General Merrick Garland. "This abuse and misconduct is outrageous and beyond unacceptable," Grassley continued.

Grassley's office said Justice Department officials created the report following an Associated Press story in 2020 that revealed sexual conduct allegations among senior officials in the bureau.

The alleged report states the 665 employees left following "alleged misconduct," but it did not specify it as sexual misconduct, although the document is titled as such.

His office suggested the actual figure could be larger, because the data doesn't include departures that occurred during or just prior to the start of misconduct investigations.

The Associated Press investigation that apparently spawned the report's creation found that the bureau opted to transfer those facing accusations or allow them to retire.

"Congress has an obligation to perform an objective and independent review of the Justice Department's and FBI's failures and determine the accuracy of the data contained in the documents so that the American people know and understand what, if any, changes have been made to solve these significant problems," Grassley wrote in his letter. (Source)

Former FBI Special Agent Found Guilty Of Accepting $150,000 In Bribes Paid By Lawyer Who Is Linked To Armenian Organized Crime Figure - October 4, 2022

Babak Broumand was an FBI special agent from January 1999 until shortly after search warrants were served on his home and businesses in 2018. He was responsible for national security investigations and was assigned to the FBI Field Office in San Francisco.

Broumand accepted $150,000 in cash bribes and other items of value in exchange for providing sensitive law enforcement information to a corrupt lawyer with ties to Armenian organized crime.

From January 2015 to December 2018, Broumand accepted cash, checks, private jet flights, a Ducati motorcycle, hotel stays, escorts, meals, and other items of value from the organized crime linked lawyer.

In return for the bribe payments and other items of value, Broumand conducted law enforcement database inquiries and used those inquiries to help the lawyer and his associates avoid prosecution and law enforcement monitoring. (Source)

Former Detroit Police Officer Pleads Guilty To Role In Tow Truck Refferal Scheme - October 20, 2022
Daniel Vickers spent his career as a police officer in Detroit.

Vickers admitted to conspiring with Detroit Police Lieutenant John Kennedy. The two conspired to commit bribery by accepting money and other items of value in exchange for Kennedy using and promising to use his influence as a supervisor to persuade other officers to make tow referrals to a towing company in violation of the city's ordinance and Detroit Police Department policy.

Vickers also admitted that he and Kennedy conspired to solicit and accept thousands of dollars in cash, cars, car parts, car repairs, and new carpeting for Vickers' home, in exchange for providing the towing company that Kennedy was investigating with information about the status of the Public Integrity Unit's case.

In total, between February 2018, and June 2018, Vickers accepted over $3,400 in bribe payments from the towing company. In addition, Kennedy accepted bribes amounting to $14,950 during the course of the conspiracy. (Source)

Police Officer Used Law Enforcement Access To Database To Help Hack Woman's Snapcat Accounts To Access Sexually Explicit Photos - October 15, 2022
A former Louisville Metro Police Department officer used law enforcement technology as part of a scheme that involved hacking the Snapchat accounts of young women and using sexually explicit photos and videos they had taken to extort them.

Bryan Wilson used his law enforcement access to Accurint, a powerful data-combing software used by police departments to assist in investigations, to obtain information about potential victims. He would then share that information with a hacker, who would hack into private Snapchat accounts to obtain sexually explicit photos and videos.

If sexually explicit material was obtained, Wilson would then contact the women, threatening to post the photos and videos online and share them with their friends, family, employer and co-workers unless more sexually explicit material was provided to him.

The FBI determined that Wilson was involved in the hacking of 25 accounts and made contact with eight women. While Wilson said another person did the hacking, no hacker is named in federal court documents. (Source)

Former Correctional Officer Sentenced To Prison For Conspiring With Inmates To Smuggle Drugs And Cell Phones Into Jail - October 4, 2022
Eric Christian was a Washington State Correctional Officer.

Christian along with six inmates smuggled multiple cell phones, methamphetamine, heroin, suboxone strips, and other contraband into the Benton County Jail. As part of the conspiracy, which began in January and continued until April 2020, Christian and his coconspirators also provided access to dangerous offenders and gang members so that they could identify, assault, and retaliate against cooperating defendants as well as inmates charged with certain types of offenses. (Source)

Federal Prison Nurse Charged With Smuggling Drug-Laced Documents To Inmates In Exchange For Bribes - October 21, 2022

Ruben Montanez-Mirabal is a licensed Registered Nurse who has worked for the Federal Bureau of Prisons at the Federal Detention Center in Miami (FDC-Miami), since February 2020.

From November 2021 to August 2002, Montanez-Mirabal smuggled drug-laced legal documents and other prohibited items to inmates at FDC-Miami.

Montanez-Mirabal smuggled in exchange for thousands of dollars in bribes and other things of value. Montanez-Mirabal delivered to inmates sheets of paper that had been soaked in liquids containing illegal drugs, then dried. The inmates who received the laced paper from Montanez-Mirabal then resold it to other inmates at FDC-Miami.

It is alleged that in addition to money, Montanez-Mirabal accepted other bribes, such as the free use of a Lamborghini and a Rolls-Royce. (Source)

STATE / CITY GOVERNMENTS

Former County Employee Charged For Role In Embezzling $1.7+ In Government Funds - October 26, 2022

John Gibson is charged with one count of conspiring to embezzle county funds and three counts stealing county funds.

Gibson and his supervisor, Kevin Gunn defrauded Wayne County out of nearly $2 million in taxpayer funds. Gunn, Gibson, and others were 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 then sold for personal profit. (Source)

Former State Attorney & County Attorney Sentenced To Prison For Extortion And Other Crimes - October 18, 2022

Marion O'Steen was a criminal defense attorney who represented clients being prosecuted by former State Attorney Jeffrey Siegmeister's office in the Third Judicial Circuit in Jacksonville, Florida.

O'Steen requested official acts from Siegmeister including the favorable disposition of charges filed against his client, and the delay of official actions in order to enable O'Steen to obtain additional "fees" from at least one of his clients.

On August 17, 2018, O'Steen extorted one of his clients, telling him that if the client paid him an additional $60,000, O'Steen would use up a "favor" with the state attorney to make "everything go away," representing that O'Steen had favors with Siegmeister for which people would pay him. O'Steen told his client he could "go to trial and fight em' out, which I don't think you can win." O'Steen further advised his client that he would not get the same results from another attorney.

O'Steen received two payments of $30,000 each from his client. (Source)

Former County Executive Sentenced To Prison For $650,000 COVID-19 Relief Fund Fraud - October 6, 2022

Between May 2020 and February 2021, George Thacker submitted three separate fraudulent applications for a total of over $650,000 in PPP and EIDL relief funds. At the time, he served as the elected County Executive for Rhea County, Tennessee, and the owner of Thacker Corporation, a business headquartered in the Eastern District of Tennessee.

As part of the loan application process, he certified that he would use the money for specific business-related purposes such as paying Thacker Corporation's rent and continuing to pay his employees' salaries. But instead of putting the relief funds to their intended purposes, Thacker used them to enrich himself. Among other things, he used the money to buy Bitcoin, Ether, and other cryptocurrencies and to fund his personal investment accounts. (Source)

Former Employee Of D.C. Project Empowerment Program Charged With Embezzling $300,000 – October 4, 2022

The D.C. government's Project Empowerment Program provides employment services to D.C. residents who had multiple barriers to employment, such as a history of substance abuse, a history of job cycling (not maintaining steady employment), and either a felony conviction or previous incarceration. One phase of the program consists of subsidized employment, which involves the D.C. government paying the wages of participants while they work at worksites. During this phase, worksites were responsible for entering participants' work hours into an electronic system used by Project Empowerment. In turn, the government would then have payments corresponding with those hours issued to accounts associated with participants, usually in the form of pre-paid bank debit cards.

Rhayda Thomas was a Project Empowerment Program participant beginning in August 2013 and ultimately got hired by the program as a Program Support Assistant in February 2014.

From May 2015 through April 2018, she is alleged to have embezzled funds by reviving 16 former Project Empowerment participants' profiles and modifying entries in a database to falsely show them as working for a non-profit organization, which was not true.

She also is alleged to have used the name of a former employee from the non-profit organization to enter and approve time in the database showing individuals as working when they were not. She ordered or caused to be ordered replacement and new prepaid debit cards on behalf of the former Project Empowerment participants whose profiles she fraudulently revived. As a result of her conduct she caused the D.C. government to request that Wells Fargo Bank load funds onto those prepaid debit cards, which she controlled.

Thomas conduct is believed to have caused between approximately $314,000 and $350,000 in losses. (Source)

State Department Of Labor Employee Accused Of Stealing $140,500 In Unemployment Insurance Funds For Friends & Relatives - October 14, 2022

Vicky Hefner began work with Missouri's Department of Labor and Industrial Relations, Division of Employment Security as a benefit program specialist in 2009. She worked out of her home and an office in St. Louis helping people file their claims over the phone and adjudicating issues people were having with unemployment claims.

From July to December of 2020, Hefner logged into the accounts of multiple friends, relatives or associates. She changed their status and used her credentials in ways that either made them eligible for unemployment benefits or increased their benefits.

She also triggered unemployment payments to people who were still working. Hefner's friends and relatives then paid her kickbacks. Hefner used her position to send about $140,500 in unearned unemployment benefits to friends, relatives and others. (Source)

Former State Housing Authority Official Pleads Guilty To Embezzling $28,000+ For Over 10 Years - October 17, 2022

Pamela McDaniel had been employed by the Charleston-Kanawha Housing Authority (CKHA) in West Virginia since 2006, and was serving as a Housing Manager in 2018.

McDaniel's duties included collecting tenant rental payments and forwarding them to the CKHA accounts clerk. On January 10, 2018, McDaniel received a $235 postal money order from a CKHA tenant intended for rental payment. McDaniel admitted to adding her own name to the postal money order to make it appear as though McDaniel was the intended beneficiary of the payment. McDaniel deposited the postal money order into her personal checking account.

McDaniel further admitted that from 2007 to 2018, she used her position as a CKHA housing manager to embezzle $28,523.30. McDaniel altered money orders she received from tenants attempting to pay dues that they owed CKHA and deposited the altered money orders into her personal checking account. McDaniel offset some of the money she stole by repaying a portion of the embezzled funds. (Source)

2 Former Directors Of Public Works Sentenced To Prison For Accepting Bribes Totaling $55,000 - October 27, 2022

Ramon Conde-Melendez was the Director of Public Works in the municipality of Guayama, Puerto Rico from 2013 until 2022.

In 2019 and 2021, Conde-Melendez agreed to receive and received cash payments from an individual (Individual A) in exchange for certifying that the asphalt and paving company (Company A) completed asphalt projects in the municipality.

The certification was required for the approval of invoices for payments from the municipality of Guayama to Company A. In 2019 and 2021, Conde-Melendez received kickback payments, equaling $1 per each square meter of asphalt removed by Company A, which totaled more than $15,000.

Pedro Marrero-Miranda was the Director of Public Works in the municipality of Cataño, Puerto Rico from 2017 until 2021.

In 2019, 2020, and 2021, Marrero-Miranda agreed to receive and received cash payments from Individual A and another individual (Individual B) in exchange for the distribution of asphalt removal projects by the municipality of Cataño to Company A, and the certification of invoices for payments from the municipality of Cataño to Company A. Specifically, Marrero-Miranda received multiple kickback payments equaling approximately $1 for each square meter of asphalt removed by Company A in the municipality of Cataño, which totaled more than $40,000. (Source)

Former California City Mayor Sentenced To Prison For Accepting $10,000 Bribe And Attempting To Burn Down His Own Restaurant - October 3, 2022

Jermaine Wright was a former Mayor for the City Of Adelanto.

Wright was sentenced prison for accepting a $10,000 cash bribe and hiring a man to burn down his restaurant so he could fraudulently collect hundreds of thousands of dollars in insurance proceeds. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

269 K-12 SCHOOL EDUCATORS ARRESTED FOR CHILD SEX CRIMES IN FIRST 9 MONTHS OF 2022 - October 14, 2022

Nearly 269 public educators were arrested on child sex-related crimes in the U.S. in the first nine months of 2022 year, ranging from grooming to raping underage students.

The 269 educators included four principals, two assistant principals, 226 teachers, 20 teacher's aides and 17 substitute teachers.

At least 199 of the arrests, or 74%, involved alleged crimes against students.

The analysis looked at local news stories week by week featuring arrests of K-12 principals, assistant principals, teachers, substitute teachers and teachers' aides on child sex-related crimes in school districts across the country. Arrests that weren't publicized were not counted in the analysis, meaning the true number may well be higher.

Only 43 of the alleged crimes, or 16%, did not involve students. It is not known whether another 10% of the alleged crimes involved students. Men also made up the vast majority, with over 80% of the arrests.

Moreover, only 14 states require employers to check an applicant's eligibility for employment or certification, and only 11 require applicants to disclose information regarding investigations or disciplinary actions related to sexual abuse or misconduct. (Source)

Indiana Teacher Arrested After Admitting To Making Kill List Targeting Students - October 14, 2022

An Indiana teacher was arrested on Thursday after allegedly telling a fifth-grader that she made a "kill list" targeting students and staff members, police said.

St. Stanislaus School teacher, Angelica Carrasquillo - Torres, reportedly mentioned the plans to a 5th grade student around noon on Wednesday. East Chicago police officers were dispatched to the Catholic school later that afternoon. The 5th grade student told their Counselor that their 5th grade teacher made comments to him / her about killing herself, students, and staff at St. Stanislaus School. The teacher further told the 5th garde student that she has a list and that they were on the bottom of that list.

The principal then asked Carrasquillo-Torres to leave the school and not return. Police officers, who were not aware of the situation until four hours later, arrived at 5 p.m. They took the teacher into custody without incident the next morning. Parents have expressed frustration that the school allowed the teacher to leave and failed to call police right away. (Source)

Former Northeastern University Employee Arrested For Staging Hoax Explosion - October 4, 2022
Jason Duhaime was charged with one count of intentionally conveying false and misleading information related to an explosive device and one count of making materially false statements to a federal law enforcement agent.

Jason Duhaime was at the time employed as the New Technology Manager and Director of the Immersive Media Lab (Lab) at Northeastern University.

Duhaime placed a 911 call at approximately 7 p.m. on Sept. 13, 2022, to report that he was injured by "sharp" objects expelled from a plastic case he opened inside the Lab that evening. Duhaime told the 911 operator that he and a Northeastern student who was working in the Lab had collected several packages from a mail area earlier that evening and brought them into the Lab. Among the packages were two Pelican cases, which Duhaime brought into a storage closet inside the Lab. Duhaime allegedly told the 911 operator that when he opened one of the cases inside the closet, very sharp objects flew out of the case and under his shirt sleeves, causing injuries to his arms. Duhaime also reported that the case contained an anonymous violent note directed at the Lab.

During subsequent interviews with law enforcement, Duhaime allegedly provided statements about the incident that were consistent with his report to the 911 operator. He expressly denied fabricating his story about the case, the letter and his injuries. (Source)

Former Charter School Board President Sentenced To Prison for Embezzling $390,000 / Used Funds For Vehicle Payment, Rent, Etc. - October 27, 2022
Jimika Williams was the President of Advancement of Education in Scholars Corporation (AESC), a Florida non-profit that operated Paramount Charter School (PCS) located in Broward County. PCS received federal funding through Title 1, which is only paid to a school if more than 50% of the students are eligible for free or reduced cost lunches. PCS also received state funding, paid through the School Board of Broward County.

Williams was the President of another Florida corporation, Florida Scholars Educational Services Corporation (FSESC).

Between 2015 and June 2017, Williams unlawfully made payments to herself from AESC's business account totaling nearly $390,000. This money's intended use was to operate PCS. Instead, the funds were transferred / deposited into an FSESC account and used for Williams' personal purchases, which included vehicle payments, a private school, rent, and other personal expenses. (Source)

Assistant Vice President of Finance For College Sentenced To Prison For Embezzling $66,000+ / Used Funds For Personal Purchases - October 26, 2022
Renee Crawford was employed as the Assistant Vice President of Finance for the College. In her role, Crawford had authority to manage invoice approvals, enter vendor information, and had oversight of the Finance Office's credit card program.

Crawford used her access to submit fraudulent invoices for a company that she created, receiving more than $44,000 from the College which she used for personal purchases. In addition, Crawford used two College issued credit cards to make personal purchases, such as family vacations and theme park tickets, totaling nearly $22,000. (Source)

Former Community School Bookkeeper Charged With Embezzling $975,000+ Over More Than 5 Years / Used Funds For Gambling, Etc. - October 11, 2022

The Anderson Community School Corporation (ACSC) is a public school corporation in charge of at least 10 public schools in Anderson, Indiana. As part of its operations, ACSC employs teachers, administrators, coaches, custodians, and other professionals, and is responsible for the education of more than 6,000 children.

Carla Burke was the ACSC Food Service Department's Bookkeeper. Burke maintained the financial records for the Food Service Department. Burke was also responsible for issuing checks on behalf of ACSC approved by her supervisor.

Between January 1, 2014, and June 30, 2019, Burke used her position as a bookkeeper for ACSC to embezzle nearly $1 million from the school corporation. Rather than submit legitimate vendor expenses, Burke issued approximately 312 checks to herself from ACSC totaling $976,773.29.

To conceal her theft, Burke falsified ACSC records making it appear that the payments were to an ACSC vendor. Burke used the stolen funds for her own personal expenditures, including gambling at several casinos. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

BANKING / FINANCIAL INSTITUTIONS

No Incidents To Report

TRADE UNIONS

No Incidents To Report

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Former Uber CISO Found Guilty Of Hiding 2016 Data Breach And Paying Hush Money To Hackers - October 5, 2022

Joe Sullivan who headed security for Facebook before joining Uber, was found guilty in San Francisco federal court. It marked a rare instance where a corporate Chief Information Security Officer was criminally charged with failing to disclose a hacking.

The Department of Justice said Sullivan arranged to pay $100,000 in hush money to two hackers, while also trying to hide the hacking from drivers, passengers, and the Federal Trade Commission. (Source)

Engineer Sentenced To Prison For Leading Conspiracy To Steal Aircraft Design Secrets - October 20, 2022

Gilbert Basaldua worked as a numerical control engineer contractor for an aircraft manufacturer from October 2016 through November 2018.

During that time, Basaldua conspired with his co-conspirators to steal valuable proprietary aircraft wing designs and anti-icing testing information from various aircraft manufacturers, including the company where Basaldua worked. The conspirators intended to use the stolen information to quicken the process of obtaining Federal Aviation Administration certification for another company's product. (Source)

Former Aircraft Maintenance Mechanic Pleads Guilty To Illegally Accessing FAA Database To Obtain Certificate To Falsely Certify Him As Licensed Mechanic - October 7, 2022

Gordon Bellamy was employed by Ally Aerospace Services as a contractor for AAR Corporation.

Bellamy worked as an Aircraft Maintenance Mechanic at the Will Rogers World Airport in Oklahoma City and that he supervised mechanic crews responsible for removing and reattaching panels as part of the maintenance of commercial aircraft. Under Federal Aviation Administration (FAA) regulations, supervising employees must be certified Airframe and Powerplant mechanics. In October of 2018, Bellamy illegally accessed an FAA database that contained records of all Airframe and Powerplant mechanic's certificates, obtained a certificate belonging to another licensed mechanic, and falsely presented it to his employer as his own. (Source)

PHARMACEUTICAL COMPANINES / PHARMICIES / HOSPITALS / HEALTHCARE CENTERS / Home Based Healthcare Provider & 2 Senior Managers Agree To Pay $7.1+ Million To Resolve False Claims Act Allegations For False Florida Home Health Billings - October 18, 2022

Carter Healthcare LLC, an Oklahoma-based for-profit home health provider, its affiliates CHC Holdings and Carter-Florida, and their President Stanley Carter and Chief Operations Officer Bradley Carter have agreed to pay $7.175 million to resolve allegations that they violated the False Claims Act by billing the Medicare program for medically unnecessary therapy provided to patients in Florida. Bradley Carter will pay $175,000, Stanley Carter will pay $75,000, and Carter Healthcare will pay the remaining $6.925 million of the settlement.

Between 2014 and 2016, Carter Healthcare allegedly billed the Medicare Program knowingly and improperly for home healthcare to patients in Florida based on therapy provided without regard to medical necessity and over billed for therapy by up coding patients' diagnoses. (Source)

Sales Representative For Medical Diagnostic Laboratory Sentenced To Prison Role In $4.6+ Million Health Care Fraud Scheme - October 3, 2022

Steven Monaco was a leader of two related fraud schemes that resulted in millions of dollars of loss to public health insurance plans. In the first scheme, Monaco, as a Sales Representative for a medical diagnostic laboratory, orchestrated a kickback scheme with a Dr. Daniel Oswari.

Monaco arranged for Oswari's medical assistant to be placed on the payroll of the laboratory while continuing to work as a medical assistant for Oswari's practice. In exchange, Oswari referred all his lab work to the laboratory for testing between late 2013 and 2016, and Monaco received $36,000 in commissions from the laboratory.

In the second fraud scheme, Monaco and his conspirator, pharmaceutical sales representative Richard Zappala, discovered that certain insurance plans including New Jersey state and local government plans, paid for very expensive compounded prescription medications between 2014 and 2016.

Monaco and Zappala organized a scheme in which they received a percentage of the insurance reimbursement for compounded medication prescriptions that they arranged. As a result of this scheme, Monaco received approximately $350,000 and caused a loss of over $4.6 million to the insurance plans. (Source)

Former Employee Of County Health Care Facility Pleads Guilty To Role In Hate Crime Charges Related To Assaults Against Disabled Residents - October 13, 2022

According to admissions made during Zachary Dinell's plea hearing, he and co-defendant 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 liquid irritants in their eyes, spraying liquid irritants 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 and could not report the defendant's alleged abuse. Due to their physical disabilities, the residents also were not able to defend themselves against the alleged assaults. (Source)

Former Medical Practice Assistant Sentenced To Prison For Accepting $10,000 In Bribes For Role In Health Care Fraud Conspiracy - October 5, 2022

Aaron Jones was previously employed by a medical practice in Stratford, New Jersey, that was owned by Dr. Michael Goldis.

Jones was paid by a pharmaceutical sales representative, Richard Zappala, to identify patients at the medical practice who had insurance plans that would cover the compound prescription medications. Jones forged the signature of Goldis on numerous compound medication prescriptions, including on prescriptions for individuals who were not Goldis' patients. Jones also arranged for Goldis to sign prescriptions for the compound medications, regardless of whether or not the individuals receiving the prescriptions had a medical necessity for them. Jones received approximately $10,000 in cash for his role in the scheme.

Jones defrauded New Jersey state and local health benefits programs and other insurers of more than $1 million by submitting fraudulent claims for medically unnecessary prescriptions. (Source)

Former Employee Of AIDS Service Organization Pleads Guilty To Health Care Fraud - October 11, 2022
Erika James was a Denial Specialist at a Federally Qualified Health Center and AIDS Service Organization.

From March 2020 through April 2021, James created fraudulent invoices with falsified supporting documents, such as explanation of benefits documents from insurance companies. James endorsed checks that were issued to patients that were in higher amounts than the usual range of the refund amount. James made claims in the system that made it appear that patients came into company and paid out of pocket for services. James would have the Finance Department issue the patient refund check, and would then deposit the refund check into her personal bank account.

James filed additional claims with the Louisiana Health Access Program (LAHAP) in December 2020 and told LAHAP to mail the checks to her residence. The checks that were sent to James residence were made out to the company. James then proceeded to deposit those checks into her personal bank account. (Source)

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

Former Financial Controller Pleads Guilty To Embezzling $7 Million+ - October 6, 2022
Kevin Lee was the Financial Controller for his company. He had access to all the company's finances, recordkeeping, and operational accounts.

Between October 2018 and August 2021, Lee used his unique access to embezzle more than $7,000,000 through multiple transfers into his personal bank accounts. He disguised these transactions as payments to vendors and by falsifying information in the company's recordkeeping software. Lee also re-directed money from an existing line of credit in the company's name to cover revenue shortfalls created by his crime. (Source)

Former Chief Financial Officer Sentenced To Prison For Embezzling $2 Million+ - October 25, 2022
Samuel Mouzon worked as the Chief Financial Officer of a company in High Point, North Carolina for approximately twenty years.

Between approximately December 2018 and February 2021, Mouzon embezzled approximately $2,038,285 for his own personal benefit and to fund purchases for himself and his family without the company's knowledge or approval. (Source)

Former Financial Controller Sentenced To Prison For Embezzling $1.8 Million+ From Technology Company / Used Funds For Son's College Tuition, Vacations, Furniture, Etc. - October 11, 2022
At the time of the charged conduct, Donna Laansma was the Financial Controller of Astea, a global management software company based in Horsham, PA, and managed the company's finances worldwide.

Laansma obtained a corporate credit card that she kept hidden from senior management. Between November 2014 and November 2020, the defendant used this secret card to spend over $1.8 million on personal expenditures such as her son's college tuition, monthly payments on her personal bank accounts, vacations, shoes, groceries, furniture, and gift cards. She also utilized her position as Financial Controller to pay down the corporate card bills, falsely recording these payments as legitimate business expenses in company books. The secret corporate credit card was discovered in 2020, after Astea was acquired by another global enterprise software company. (Source)

Former Financial Controller Sentenced To Prison For Embezzling $1.4 Million+ Over 7 Years / Used Funds To Pay Credit Card - October 11, 2022

Gerald Burke was employed as the Financial Controller of a privately owned metal stamping company. Burke was responsible for the company's finances, including directing payroll and signing checks on behalf of the company.

From October 2011 until his termination in 2018, Burke embezzled $1.4 million by authorizing additional payroll payments to himself and by writing checks to himself and his credit card company from the company account. (Source)

Company General Manager Pleads Guilty To Embezzling $1.2 Million+ Over 16 Years - October 19, 2022

Darrell Pike was the General Manager of an Ontario, Calif. subsidiary of a supply and service company based in Wilmington, Mass.

Between approximately 2005 and 2021, Pike prepared and submitted fraudulent invoices to his employer on behalf of a fake temporary staffing company, Consumer Information Systems (CIS), for staffing services CIS purportedly provided at his employer's Ontario location. Pike added approving initials of company personnel to the invoices without their knowledge or consent. Through the fraudulent invoices, Pike caused the company to pay approximately $1,271,206 to CIS, which he deposited into a bank account he controlled. (Source)

Former Secretary Admits To Embezzling $1.2 Million+ To Purchase SUV, Pickup Truck, Vacations, Etc. - October 6, 2022

Stephanie Carper admitted taking advantage of her position as secretary of a family-owned agricultural business to write checks to herself.

From September 2013 to September 2019, Carper filled in her own name on at least 44 checks that had been pre-signed by the company's owner and his relatives so they could be used to pay vendors. Carper then wrote in false explanations on bank deposit slips and the check registry to conceal her thefts.

Carper used the money to buy a 2015 Nissan Murano SUV, a 2016 Toyota Tundra pickup, a Caterpillar 247 skid loader and vacations to Alaska and elsewhere. (Source)

Former Phoenix Suns Ticket Manager Sentenced To Prison For Illegally Selling 2,800+ Team Tickets Worth $458,000+ Tickets Through 3rd Party - October 13, 2022

Jeffrey Marcussen worked for the Suns from 2004 to 2019 as the Assistant Director For Suns Ticketing. He was charged in September 2020. Marcussen sold the tickets on StubHub, an online ticket retail site, without authorization. The Suns don't sell tickets on the platform.

Marcussen pled guilty and agreed to pay $458,218 to the Suns in restitution. He also agreed to pay $1,780 to the Arizona Attorney General's anti-racketeering revolving fund and $11,818 to the Arizona Department of Revenue. Those funds have been paid in full. (Source)

Former Company Marketing Manager Charged With $430,000 Of Wire Fraud For Personal Use - October 7, 2022

From January 2017 through July 2019, Ahmed-Elkilani misappropriated more than $430,000 in funds belonging to his former employer by taking advantage of his role as a Marketing Manager for the company and his access to other employees' operator codes, as well as the company's membership accounts to create and execute multiple false transactions. These transactions enabled Ahmed-Elkilani to misappropriate funds for his own personal use and benefit.

Ahmed-Elkilani misappropriated $417,075 in special order merchandise deposits held in the company's deposit account and caused approximately $275,000 of those funds to be transferred to his personal credit or debit cards. He also misappropriated $13,674 in additional company funds through other fraudulent methods. (Source)

Former Executive Director Of Children's Not-For-Profit Arrested For Embezzling $280,000+ - October 25, 2022

From at least 2018 through 2021, Philip Dallmann served as the Executive Director of a children's not-for-profit organization based in Manhattan.

In 2018, Dallmann began embezzling funds from the organization's bank account for unauthorized personal expenses. In or around 2019, the organization began receiving overdraft notices from the bank, which Dallmann claimed was caused by the bank's loss of donor checks. The following year, the organization switched banks, and Dallmann continued his embezzlement. A subsequent audit revealed that Dallmann stole a total of approximately $98,000.

While serving as the executive director, Dallmann married a teacher at the not-for-profit organization. In or around the spring of 2020, Dallmann's wife learned that Dallmann had stolen credit cards that belonged to her father and on which she was an authorized user and that Dallmann had used the credit cards to make unauthorized transactions, later found to total more than $143,000.

Dallmann claimed that he had used his wife's credit cards to cover operational expenses for the not-for-profit organization. Dallmann then impersonated the organization's treasurer by email to negotiate repayments by the organization to his wife. Based on Dallmann's representations, the organization then, in fact, entered into a contract to pay Dallmann's wife $30,000.

In sum, Dallmann made hundreds of unauthorized personal transactions using the not-for-profit organization's bank accounts, such as payments for pet grooming, food delivery, restaurants, groceries, alcohol, clothing, shoes, transportation, ESPN Plus and Netflix subscriptions, Amazon orders, and wedding photography services. He also withdrew thousands of dollars in cash from the not-for-profit organization's accounts. (Source)

Chief Financial Officer / Head Of Human Resources Sentenced To Prison For Embezzling $250,000 / Used Funds To Pay Student Loans, Credit Card & Vehicle Bills, Etc. - October 12, 2022

Noor Clements worked in the Houston office of a California-based company as a Chief Financial Officer and Head Of Human Resources from April 2016 to May 2018. In her role, she managed all accounting functions of the office including payroll and banking.

Clements admitted to paying herself unearned vacation and overtime pay. She also made unauthorized payments with company funds to pay her student loans, credit card and personal vehicle bills. In addition, she used her company credit card towards personal expenses such as travel, income taxes, car repairs and tickets to sporting events and concerts. Clements is also required to pay $250,000 in restitution to her employer. (Source)

Former Bookkeeper Pleads Guilty To Embezzling $200,000+ In Public Housing Rent Payments - October 12, 2022

Between January 2010 and July 18, 2018, Marcie Thumann worked as a Bookkeeper for the Albert Lea Housing and Redevelopment Authority (HRA), a government program that received both federal and state funding to remedy the shortage of available low-incoming housing units.

At the beginning of each month, the HRA's computer system generated a rent-due balance for each tenant. Thumann, who was responsible for recording and reconciling payments to the HRA, received tenants' rent payments via cash, check, or money order.

During her tenure as the HRA's bookkeeper, Thumann routinely embezzled HRA rent payments for her own personal use and benefit. She did so by pocketing cash payments and altering the payee information on payments made by check and money order. Thumann also manipulated the HRA's computer system to conceal the money she stole, avoid detection, and prolong her fraud scheme. In total, Thumann stole at least $213,217 in tenant payments. (Source)

Bookkeeper Charged With Stealing From Former Employer / Used Funds To Make Tens Of Thousands Of Dollars Of Personal Purchases - October 17, 2022

In September 2017, Bonnie Sweeten was hired as a bookkeeper for excavating company, because the president of the company had known her for many years. As the bookkeeper, Sweeten had access to company bank accounts, company checkbooks, the company mail, and other sensitive personal information belonging to the president and to the company.

Sweeten used her position to steal company funds: using her access to the company's checking account to issue dozens of company checks to herself; using her access to the company mail to steal checks that had been mailed to the company, which she then fraudulently endorsed over to herself; and using her access to the company credit card to make tens of thousands of dollars of personal purchases. (Source)

Former Bookkeeper Charged With Wire Fraud From 2 Businesses - October 24, 2022

The Indictment alleges that on or about January 2015 and continuing through February 2022, Reva Plunkett, who was the Bookkeeper for Doug's Anchor Marine, Inc., and for Brotherhood Arms, businesses located in Watertown, South Dakota, devised and intended to devise a scheme and artifice to defraud and to obtain money and property from others by means of false and fraudulent pretenses, representations, and promises.

On multiple occasions during the relevant time periods, Plunkett falsely and fraudulently wrote checks payable to herself that were drawn on business accounts belonging to Doug's Anchor Marine, Inc. and Brotherhood Arms. These checks were not for her wages or salary, nor were they for any other legitimate purpose. Plunkett also deposited the checks into her account and used the funds for her own purposes. Plunkett disguised her theft by falsely and fraudulently recording in the businesses' accounting system that the checks were payable to vendors, which made the checks appear to be legitimate business expenses. She also falsely and fraudulently adjusted the business inventory to make it appear that the money was actually spent on products for the businesses. (Source)

SHELL COMPANIES / FAKE INVOICE BILLING SCHEMES

No Incidents To Report

THEFT OF COMPANY PROPERTY

Former Yale Med School Employee Sentenced To Prison For Stealing And Selling $40 Million in Electronics / Used Money For Cars, Real Estate, Travel - October 13, 2022

Beginning in approximately 2008, Jamie Petrone was employed by the Yale University School of Medicine (Yale Med), Department of Emergency Medicine. He most recently served as the Director of Finance and Administration for the Department of Emergency Medicine. As part of her job responsibilities, Petrone had authority to make and authorize certain purchases for departmental needs as long as the purchase amount was below $10,000.

Beginning at least as early as 2013, Petrone engaged in a scheme whereby she ordered, or caused others working for her to order, millions of dollars of electronic hardware from Yale vendors using Yale Med funds and arranged to ship the stolen hardware to an out-of-state business in exchange for money.

Petrone falsely represented on Yale internal forms and in electronic communications that the hardware was for specified Yale Med needs, such as particular medical studies, and she broke up the fraudulent purchases into orders below the $10,000 threshold that would require additional approval. The out-of-state business, which resold the electronic equipment to customers, paid Petrone by wiring funds into an account of a company in which she is a principal, Maziv Entertainment LLC.

Petrone caused a loss of approximately $40,504,200 to Yale. Petrone used the proceeds of the sales of the stolen equipment for various personal expenses, including expensive cars, real estate and travel. (Source)

NETWORK / IT SABOTAGE / OTHER FORMS OF SABOTAGE

No Incidents To Report

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

Ex Husband Conspired With State Of Georgia Employee (Wife) - Pleads Guilty To Stealing $1.3 Million+ By Creating Fake Students With Disabilities - October 4, 2022

Kevin Gregory has pleaded guilty to conspiring with ex-wife (Karen Lyke) who was the former Georgia Vocational Rehabilitation Agency Counselor, to forge educational records and to create fake students with non-existent disabilities and illnesses, as part of their sophisticated, multi-year scheme to steal more than $1.3 million. (Source)

EMPLOYEE DRUG RELATED INCIDENTS

Former Hospital Nurse Pleads Guilty To Stealing Fentanyl For Her Own Use On Multiple Occasions - October 4, 2022

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

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

Airline Mechanics Sentenced To Prison For Conspiracy To Purchase Private Jet To Transport Cocaine Internationally - October 17, 2022

On May 28 and December 8, 2021, Homeland Security Investigations (HSI) used an undercover agent (UC) and a confidential source (CS) to negotiate with Jesus Pimentel and Tomas Mendez to purchase a private passenger jet for use in Mexico. During recorded conversations, Pimentel and Mendez told the UC and the CS that they needed to purchase the airplane in order to transport approximately 2,500 kilograms of cocaine. They explained that they would only be able to use the airplane once or twice. Then, the buyers would destroy the plane by intentionally crashing it in a jungle or the ocean. Pimentel and Mendez also attempted to bribe an individual, who they thought was an airport customs official, in order to allow cash and drugs to pass through the airport. The airport customs official was actually an undercover law enforcement officer.

To conclude the purchase of the airplane, Pimentel and Mendez traveled around the Southeastern United States over a one-month period and gathered more than $600,000 in cash and provided it to the undercover law enforcement officers. Shortly after providing the final payment for the airplane Pimentel and Mendez were interviewed and arrested. (Source)

State Government Worker Sentenced To Prison For Fraud, Distribution Of A Controlled Substance, Taking $6,000 Bribe - October 12, 2022

In January 2017, Joseph Ellicott was hired by a government agency in Seminole County (Government Agency) as a Special Projects Manager. The elected head of the Governmental Agency was a public official and Ellicott's friend (Public Official).

Beginning at least by January 2017, and continuing through 2019, Ellicot and a contractor with the Governmental Agency conspired with each other to commit wire fraud and honest services fraud. Ellicott's role in the conspiracy was to serve as the intermediary for the payment of a bribe and kickback of $6,000.

For at least two years, Ellicott illegally sold Adderall to others. Over the course of at least two years, one of Ellicott's customers paid him more than $5,000 for hundreds of Adderall pills. (Source)

Former Medical Assistant Pleads Guilty To Obtaining Controlled Substances By Fraud For Herself & Family - October 6, 2022

Debra Bossier worked as a Medical Assistant at the Desoto Regional Health System in Mansfield, Louisiana.

Desoto Regional used an Electronic Medical Records System to document patient encounters and generate electronic prescriptions. Bossier used the Electronic Medical Records System to falsely document telephone encounters to obtain controlled substances by fraud and forgery by generating controlled substance prescriptions for herself, her husband, her daughters, and a daughter's boyfriend. (Source)

OTHER FORMS OF INSIDER THREATS

Equifax Monitored 1,000 Remote Workers, Fired 24 Found Employee That Were Found To Be Juggling 2 Jobs - October 14, 2022

Equifax recently conducted an investigation into a number of employees suspected of holding dual, full-time employment that conflicted with their roles at our company, Equifax spokesperson Kate Walker said in a statement. As a result, several employees who violated our company code of conduct and outside employment policy, which were in effect at the time of the investigation, were recently terminated.

Equifax terminated an employee for holding 3 jobs at once. That employee had one part-time position that Equifax knew about, but another that he didn't disclose and actually did from Equifax's office. (Source)

MASS LAYOFF OF EMPLOYEES INCIDENTS

No Incidents To Report

EMPLOYEES MALICIOUS ACTIONS CAUSING COMPANY TO CEASE OPERATIONS

No Incidents To Report

WORKPLACE VIOLENCE

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 in Texas, 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 incubated 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)

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 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, has been charged with two counts of murder and one count of attempted murder, Forsyth County District Attorney Jim O'Neill announced during a news conference.

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)

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)

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)

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 (**4,100+ 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