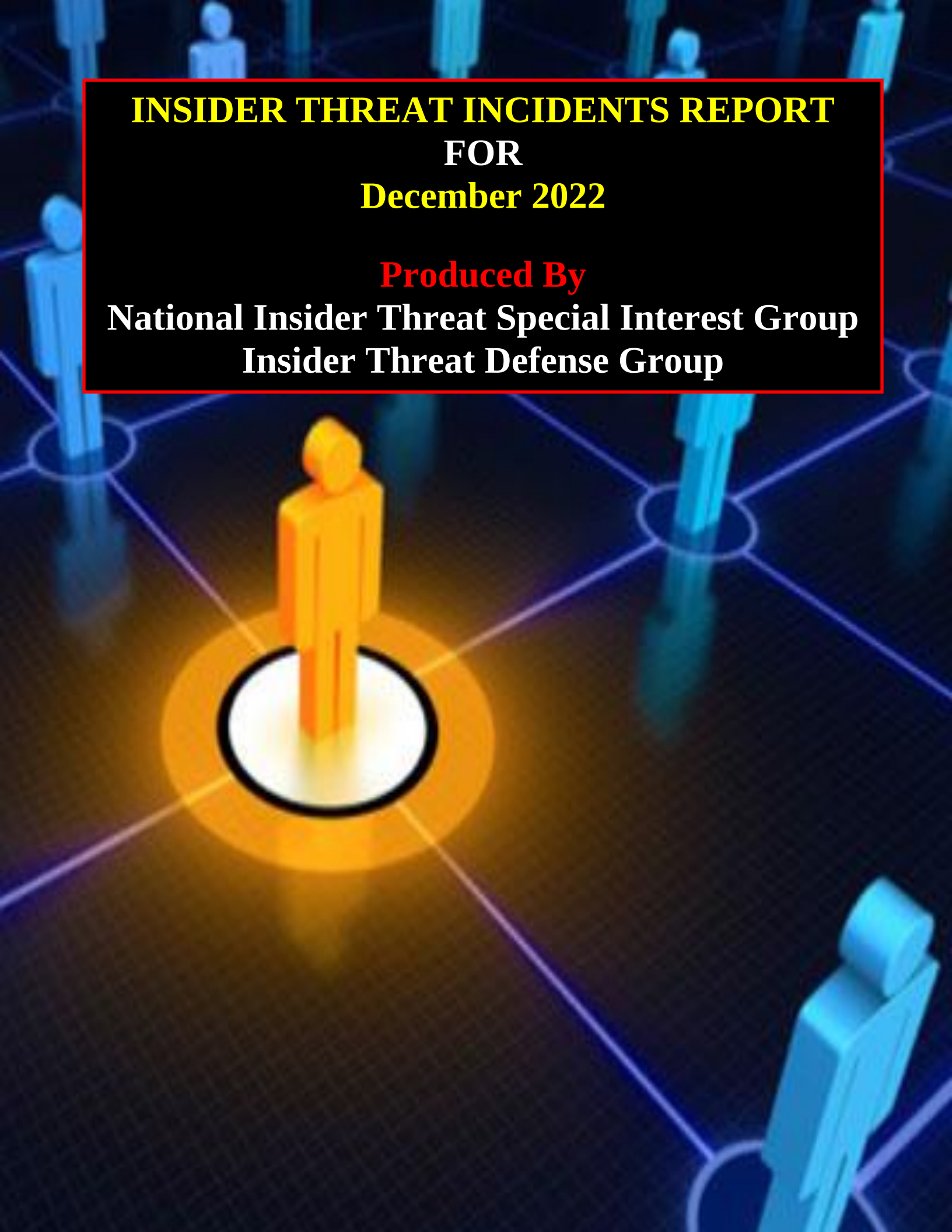

INSIDER THREAT INCIDENTS REPORT
FOR
December 2022

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 **4,200+** 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 24 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 DECEMBER 2022

FOREIGN GOVERNMENT INSIDER THREAT INCIDENTS

Former Venezuelan National Treasurer & Husband Convicted In BILLION DOLLAR International Bribery Scheme - December 15, 2022

Claudia Guillen was the former National Treasurer of Venezuela. and her husband on Dec. 13 for their roles in a billion-dollar currency exchange, bribery, and money laundering scheme.

Claudia Patricia Diaz Guillen and her spouse Adrian Jose Velasquez Figueroa, both Venezuelan citizens, were extradited from Madrid, Spain, earlier this year, for their roles in a billion-dollar currency exchange, bribery, and money laundering scheme.

Diaz and Velasquez accepted over $100 million in bribes from co-conspirator Raul Gorrin Belisario, a Venezuelan billionaire businessman, who owned Globovision news network. Gorrin paid bribes to Diaz, including through her husband Velasquez, in order to obtain access to purchase bonds from the Venezuela National Treasury at a favorable exchange rate, resulting in hundreds of millions of dollars of profit. The conspiracy involved bulk cash hidden in cardboard boxes, offshore shell companies, Swiss bank accounts, and international wire transfers sent by Gorrin to purchase multiple private jets, yachts, and to fund a high-end fashion line started by Diaz and Velasquez in Southern Florida. (Source)

Former Finance Department Employee Sentenced To Prison For Data Theft / Passing Data To Criminals - December 22, 2022

The Antwerp Correctional Court has convicted a 43-year-old former employee of the Federal Finance Department for looking up the private data of at least 25 people and passing it on to criminals.

Nathalie D.P. was sentenced to 30 months in prison, of which 20 months were suspended. She was also fined €24,000, of which €16,000 was suspended. Further, the court seized €5,000 in illegally obtained assets from her.

The facts came to light last year during an investigation into the cracked messaging service Sky ECC. Intercepted messages from a group chat revealed that people in the criminal world were looking for someone who could get hold of the private data of certain persons.

One of the participants reported that he knew someone and asked for €500 per search. Later, screenshots were shared of tax sheets, clearly made by someone within the Finance Department. That is how Nathalie D.P., who had worked at the Finance Department in Antwerp for 21 years, came into the picture.

The participant in the Sky ECC chat turned out to be her ex-partner, Larbi K. Further investigation of the seized cellphones, among other things, revealed that she had been doing searches for him since 2015 and that she asked him for money each time.

She also searched for private data for her childhood friend Foad R. and for José F.G. She had a fourth client, but he could not be identified.

Foad R. and José F.G. received prison terms of 15 and 12 months respectively and a €4,000 fine each. (Source)

U.S. GOVERNMENT

Former Mail Carrier Pleads Guilty To Role In Stealing $145,000+ In Jobless Benefit Debit Cards From Mail - December 14, 2022

From January 2019 to May 2020, Toya Hunter stole mail, including letters with jobless benefit debit cards, sent by the California Employment Development Department (EDD), which administers the state's unemployment insurance program, which. Hunter then gave the stolen EDD debit cards as well as other credit cards and financial instruments to her co-schemer. The co-schemer then activated and fraudulently used the cards to commit bank fraud.

In March 2020, Hunter stole mail from her assigned route, including an EDD debit card belonging to a victim. Hunter also stole correspondence in the mail that contained the victim's name and the last four digits of the victim's Social Security number, which she later gave to her accomplice in exchange for cash and gifts, knowing the accomplice intended to activate and fraudulently use the victim's debit card.

Hunter's co-schemer used the debit card and the last four digits of the victim's Social Security number to fraudulently activate the card and create a personal identification number (PIN) to access funds from the victim's account, which was held at Bank of America. The co-schemer then used the victim's stolen EDD card to withdraw cash from a Bank of America ATM located in Corona.

During the scheme Hunter aided and abetted her accomplice in making fraudulent and unauthorized cash withdrawals from 68 separate victims' accounts and stole approximately $145,191 from Bank of America.

In July 2021, Hunter stole from the mail and fraudulently activated a stolen debit card containing COVID-19 pandemic unemployment relief money belonging to another victim. Hunter used the card to make fraudulent purchases and cash withdrawals, thereby stealing approximately $1,400 from Fiserv Bank. (Source)

U.S. Postal Employee Pleads Guilty To Stealing Narcotics From Mail - December 30, 2022

From February 5 to March 4, 2021, Jonisha Williams worked as a Mail Handler Assistant at the National Distribution Center in Jacksonville.

During this time, the United States Postal Service Office of Inspector General received a complaint that Williams was stealing narcotics from the mail and taking them out of the facility. After investigating the complaint, agents captured Williams on video surveillance placing vacuumed sealed bags—similar to how narcotics are packaged—and other mail parcels into her backpack. During an interview with agents, Williams admitted her involvement and that she used her backpack to remove marijuana from the mailing facility. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Former Government Contractor Owner Sentenced To Prison For Paying $460,000+ In Bribes To Air Force Contracting Official - December 8, 2022

Ryan Dalbec is the owner of Best Choice Construction LLC (Best Choice).

Dalbec agreed to pay over $460,000 in bribes to former U.S. Air Force Contracting Official, Brian Nash II, in exchange for confidential bidding information on over $8,250,000 in U.S. Department of Defense contracts at Eielson Air Force Base and Joint Base Elmendorf-Richardson (JBER).

The confidential bidding information Nash provided helped Dalbec and Best Choice win some of those contracts, including a $6,850,000 construction contract related to the F-35 aircraft program at Eielson Air Force Base. Dalbec and his wife, Raihana Nadem, also helped Nash launder the bribery proceeds through family members and third-party bank accounts to conceal the nature and source of the funds.

Nash was previously sentenced to serve 30 months imprisonment and ordered to forfeit $47,000 in unlawful gains. (Source)

Former Veterans Affairs Psychologist Charged With Submitting False Medical Documents & $54,000 Of Medicare Fraud - December 12, 2022

Theresa Kelly, a Licensed Clinical Psychologist, was employed by the Veterans Administration at its medical center in Marion, Illinois.

Between November 2016 and August 2020, Kelly submitted fraudulent medical documentation in the name of real and fake medical providers as part of the approval process for reasonable accommodations and medical leave, including FMLA leave.

In addition to her submission of fraudulent medical documents, the indictment alleges that between May 2016 and January 2018, Kelly engaged in a scheme to defraud Medicare and obtain payment for psychiatric services that she did not provide to residents of a Southern Illinois nursing home. In addition to her full-time job at the VA, Kelly owned a company by the name of TS Onsite Mental Health through which she claimed to provide psychotherapy sessions to patients at Shawnee Christian Nursing Center in Herrin, Illinois. Kelly billed Medicare for over 400 claims, worth more than $54,000 for services that she did not provide. Kelly billed for at least some of the services on days she was on approved medical leave from the VA. (Source)

2 U.S. Army Soldiers Admit To Murdering Another Soldier - December 1, 2022

Byron Booker, a former U.S. Army Sergeant, admitted he and Jordan Brown, a former U.S. Army Specialist, discussed "silencing" Specialist Austin Hawk, 21 at the Fort Stewart Military Reservation.

Hawk's murder was in retaliation for Hawk reporting Brown to U.S. Army leadership for marijuana use that resulted in a preliminary inquiry for a court martial proceeding against Brown. After conspiring with Brown, Booker admitted that he gained entry to Hawk's barracks room shortly after midnight on June 17, 2020, where he "slashed and stabbed Hawk repeatedly with a sharp-edged weapon." A medical examiner later noted that Hawk received 40 separate stab or slash wounds. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

D.C. Corrections Officer Charged With Embezzling $11,000+ / Used Funds For Trip W/ Friends - December 19, 2022

Between June 2018 and May 2019, Andra Parker served as Chairman of the D.C. Department of Corrections Labor Committee, a labor organization that represents all members of the D.C. Department of Corrections.

As chairman, Parker had full access to the Labor Committee's bank accounts and was issued a debit card. He is accused of defrauding the Labor Committee by using Committee funds to pay for personal travel, lodging, and entertainment expenses. For example, charging documents allege that he spent more than $7,000 on a trip to New York city for his friends and him, including $4,000 on rooms and expenses at a Times Square hotel, more than $370 on tickets to a New York Knicks game, and an additional $616 on tickets to Summer: The Donna Summer Musical. (Source)

Former Border Patrol Agent Sentenced To Prison For Bribery, Firearms, Narcotics Charges - December 27, 2022

Between July and August 2018, Monreal-Rodriguez, a former U.S. Border Patrol (USBP) agent, was involved in two firearm-related conspiracies wherein he both unlawfully purchased firearms from federally licensed firearms dealers on behalf of other individuals and provided firearms to felons, who are prohibited from possessing firearms.

While the investigations into the firearms conspiracies were ongoing, Monreal-Rodriguez also conspired to import narcotics into the United States from Mexico, from January 8, 2018, until his arrest on September 25, 2018. During this time, a drug trafficking organization he worked with smuggled narcotics across the border. Monreal-Rodriguez would retrieve the narcotics and take them past the checkpoint several miles from the border, often in his USBP vehicle and then transport the drugs to the Tucson area. He admitted to distributing 116 kilograms of cocaine and 107 kilograms of marijuana as part of the conspiracy.

Additionally, Monreal-Rodriguez admitted to receiving cash proceeds from narcotics sales totaling at least $1.2 million, which he transported to the United States-Mexico border and then handed off to other individuals so the cash could be smuggled into Mexico. In exchange for his role in the narcotics conspiracy, Monreal-Rodriguez received cash payments. (Source)

STATE / CITY GOVERNMENTS

Ex Husband Conspired With State Of Georgia Employee (Wife) - Pleads Guilty To Stealing $1.3 Million+ By Creating Fake Students With Disabilities - December 1, 2022

Kevin Gregory has pleaded guilty to conspiring with ex-wife who wa the former Georgia Vocational Rehabilitation Agency counselor Karen C. Lyke 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.

Karen Gregory has been sentenced to five years in prison for forging educational records and creating fake students with non-existent disabilities and illnesses in an elaborate, multi-year scheme to steal more than $1.3 Million. (Source)

Former Tax Office Supervisor Charged With Committing Fraud While ,Waiting To Report To Prison For Accepting $35,000+ In Bribes To Unlawfully Register / Renew Vehicle Registrations - December 16, 2022

Gerald Harris is a former Supervisor in DeKalb County's Tax Commissioner's Office, in Atlanta, Georgia.

From July 2017 to November 2019, Harris served as the Supervisor of Tax Tag Clerks for the Tax Commissioner's Office. Harris unlawfully exploited his position by accepting more than $35,000 bribe payments from customers to unlawfully register vehicles or renew vehicle registrations.

After being fired from the Tax Commissioner's Office, Harris also attempted to blackmail one of the individuals who had been paying him bribe money. In December 2019, Harris sent a series of text messages to the individual stating that he was under investigation by the FBI; that the FBI had a video of Harris with the individual; that "all of us can be in trouble"; that Harris needed to know "how much" money he would receive to not share this information to the FBI; and that Harris was "not going to prison empty handed. It's that simple."

In early March 2021, while awaiting his report to federal prison, Harris met an individual (Person 1). Even though Harris had been terminated from his position with the Tax Commissioner's Office, Harris claimed that he had the key to the office and that he ran the office.

Harris also falsely claimed to Person 1 that in exchange for a payment of between $1,200 and $1,500 per vehicle Harris could obtain vehicle tags for stolen vehicles, and that for a payment of $4,000 Harris could obtain a Commercial Driver's License for Person 1.

On March 22, 2021, Person 1 asked Harris about obtaining a tag for a vehicle, even though Person 1 did not have the vehicle's title or any other documentation required to register the vehicle. In response, Harris falsely stated that he knew a woman who could register the vehicle if Person 1 paid the woman a $1,000 bribe payment.

On March 23, 2021, Harris again falsely claimed to Person 1 that the woman wanted a $1,000 bribe payment to register the vehicle. As a result, Person 1 gave Harris $1,000 in cash. But Harris then kept the $1,000 in cash, stopped all communications with Person 1, and never obtained a vehicle tag for Person 1. (Source)

Former Chairman For City Housing Authority Pleads Guilty To Extortion For Accepting $9,400 In Kickback Payments - December 16, 2022

Around April 2019, Delvin Thomas was the Chairman of the Riviera Beach Housing Authority, during which time the authority sought to purchase real-estate located in Riviera Beach for a low-income rental property. Thomas introduced a real estate broker to the person at Riviera Beach Housing Authority responsible for purchasing the property and Riviera Beach Housing Authority entered into a contract with the broker to purchase the property.

The broker was to receive a 3% commission from the property's purchase. Once the contract to purchase the property was entered, Thomas told the broker that he, Thomas, was to receive 50% of the commission for its sale. At closing, the broker's company was paid a commission of $18,930. In order to hide the unlawful payment of Thomas' 50% share, Thomas contacted a straw party to act as a front for this illicit activity.

The straw party (or front) agreed to deposit two checks issued to the front's business bank account and then issue checks from said account to Sire Development Group LLC, a company Thomas owned. Two checks in the amounts of $6,400 and $3,065 were issued to the front's company account. This represented 50% of the commission received by the broker. The checks falsely stated in the memo section that the payments were for "company branding" and "marketing services."

The front then issued two checks to Thomas' company, Sire Development Group LLC, in the amounts of $6,400 and $3,000—falsely stating in the check's memo section that the payments were for "consulting services." (Source)

Former Police Chief, City Council Member & Additional Co-Conspirator Sentenced In Vote Buying Conspiracy - December 1, 2022

A former Police Chief in Amite City, Louisiana and a former Amite City Council Member were each sentenced yesterday to one year in prison for violating federal election laws as part of a conspiracy to pay, or offer to pay, voters for voting in a federal election.

In addition to the prison sentence, the former police chief was also ordered to pay a $10,000 fine. Today, an additional co-conspirator was sentenced to four months in prison for his role in the scheme.

Jerry Trabona is the former Chief of Police in Amite City, and Kristian Hart is a former Amite City Council Member.

Both agreed with each other and others to pay or offer to pay voters residing in Tangipahoa Parish, Louisiana, for voting during the 2016 Open Primary Election and the 2016 Open General Election, contests in which Trabona and Hart were candidates. Trabona and Hart's vote buying scheme included the solicitation and hiring of individuals responsible for identifying potential voters, the transportation of those voters to the polls, and payment and offer of payment to the voters for voting. In the 2016 election, co-conspirator Sidney Smith paid voters with money provided by Trabona and Hart.

Two other Louisiana men who previously pleaded guilty for their involvement in the vote buying scheme, Calvin Batiste and Louis Ruffino, will be sentenced at a later date. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

Texas Southern University Police Chief On Administrative Leave For Overtime & Payroll Abuse Scheme - December 12, 2022

Texas Southern University (TSU) Police Chief Mary Young is on administrative leave with pay amid fraud allegations, the school said.

TSU alleges that Young, "committed fraud against the university by implementing and sanctioning an overtime and payroll abuse scheme that cost the university and taxpayers thousands of dollars in officer hours that were not actually worked."

An internal audit shared within the documents said Young also authorized two types of compensation by verbally OK'ing the pay and when she signed the weekly time reporting packages provided by the DPS timekeeper. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

BANKING / FINANCIAL INSTITUTIONS

Former Bank Employee / Vault Manager Pleads Guilty To Embezzling At Least $120,000 - December 6, 2022

A Comerica Bank employee pleaded guilty to embezzling more than $120,000 from the bank. She admitted she repeatedly stole cash from the FDIC insured bank.

Sallie Lazzaro began as a teller and was later promoted to vault manager.

She purloined cash from her teller drawer, hid it in her pocket or purse, and input false information into the bank's computer system in order to manipulate teller and vault balances.

On May 20, 2021, when Ms. Lazzaro was on duty as vault manager, a cash count revealed that the bank was missing more than $100,000. (Source)

TRADE UNIONS

11 Union Officials Plead Guilty To Accepting Bribes And Illegal Payments - December 12, 2022

The United States Attorney for the Southern District of New York, and District Attorney for Suffolk County, announced today that 11 former union officials have pled guilty to charges stemming from their acceptance of bribes and illegal cash payments from a construction contractor from October 2018 to October 2020 while the defendants were serving as union officers.

The union officials accepted dozens of bribes to corruptly influence the construction industry at the expense of labor unions and members. (Source)

4 Union Employees Plead Guilty To Embezzling From Union For 6 Years - December 22, 2022

4 employees of the International Brotherhood of Electrical Workers (Local 98), entered pleas of guilty arising from their personal use of the assets of Local 98 in ways that did not benefit the membership of Local 98 as a whole, including embezzlement of labor union assets, wire fraud, and theft from a union employee benefit plan.

Michael Neill served as the Training Director of Local 98's Apprentice Training Fund. He pleaded guilty to four counts of embezzlement of labor union assets, one count of theft from a union employee benefit plan, and one count of making and subscribing to a false federal income tax return. He is scheduled to be sentenced on April 7, 2023.

Marita Crawford served as Local 98's Political Director. She pleaded guilty to four counts of wire fraud, the object of which was to obtain money and property from Local 98 by means of false and fraudulent pretenses, representations, and promises. She is scheduled to be sentenced on April 4, 2023.

Niko Rodriguez was employed by Local 98's Apprentice Training Fund and by Local 98. He pleaded guilty to six counts of embezzlement of labor union assets. He is scheduled to be sentenced on April 4, 2023.

Brian Fiocca was employed by Local 98 as an office employee. He pleaded guilty to six counts of embezzlement of labor union assets. He is scheduled to be sentenced on April 6, 2023. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Former Hytera Director Pleads Guilty To Conspiracy To Steal $600 Million+ Of Motorola DMR Trade Secrets - December 7, 2022

A key former Hytera Communications Director has entered a guilty plea to criminal charges of conspiring to steal trade secrets from Motorola Solutions that enabled Hytera to accelerate the development of its profitable DMR product line, allegedly at the behest of a top executive at the China based LMR manufacturer.

Gee Ko was the Hytera Communications' former Director of Research & Development, as well as a former member of the company's board of directors. Kok was one of 7 former employees of Hytera indicted individually who were identified in April.

In the criminal plea agreement, Kok confirms many allegations made by Motorola Solutions in the lengthy case that resulted in the March 2020 judgment that required Hytera to pay hundreds of millions of dollars for stealing DMR trade secrets from Motorola to develop a competing product set. Although the damage amount of $764.6 million award was lowered, Hytera still owes Motorola Solutions more than $600 million from the case, according to legal documents. (Source)

FibroGen Files Lawsuit Against Former Employees For Trade Secret Theft - December 5, 2022

FibroGen is cracking down on former employees accused of trade secret theft. The company filed a lawsuit in the U.S. District Court in the Northern District of California.

The company slapped former employees Dong Liu, Ph.D., and Shaojiang Deng, Ph.D., with the suit to ask that the defendants stop their use of the propriety information and correct their patents to list the true owner, which is FibroGen, the company alleges. The company is also seeking compensation and wants the former employees to give up profits made from the patents they "wrongfully" claim.

Liu and Deng worked as scientists at FibroGen for years, giving the two access to the confidential information. 2 years before Liu left the company in 2015, he founded Kind, a direct competitor of FibroGen. A few years later, in 2019, Deng left FibroGen to take on a leadership position at Kind. FibroGen is now accusing the two of using the company's intellectual property and proprietary information to get a head start with Kind.

Allegedly, Deng and Liu filed a series of patent applications claiming FibroGen compounds without knowledge or consent of their former employer.

These patents "list the incorrect inventors, omit the FibroGen scientists who invented the compounds and are wrongly assigned to Kind" as opposed to FibroGen, the lawsuit says. (Source)

Johnson & Johnson's Robotic Surgery Unit Has Accused Former Employees Of The Misappropriation Of Trade Secrets - December 19, 2022

In a lawsuit filed in U.S. District Court, three J&J subsidiaries claim executives and engineers at robotic surgery startup Noah Medical, including CEO and founder Jian Zhang, have documents from their time working at Auris Health. Auris and two other J&J subsidiaries, Verb Surgical and Cilag GmbH International, have asked the court to require the return of trade secrets and the payment of damages by Noah.

The lawsuit accuses Noah of engaging "in a systematic process of hiring other Auris employees that has maximized [its] ability to obtain Auris trade secrets." According to the plaintiffs, Zhang, Auris' second employee, still has documents from his time at the J&J company and runs a business that is built on the work of others.

Much of the lawsuit centers on Enrique Romo, who became vice president of research and innovation at Noah after working on early-stage innovations for Auris' robotic platforms. Romo allegedly took "a treasure trove" of materials from Auris, including "a presentation depicting an endoscopic system developed by his team at Auris that bears a striking similarity to the subject of Noah's patent application." The lawsuit claims "a Noah patent application includes stolen Auris trade secrets." (Source)

Former Twitter Employee Sentenced To Prison For Acting As An Agent Of A Foreign Government & Unlawfully Sharing Twitter User Information / Taking Bribes – December 14, 2022

A former Twitter employee found guilty of spying on users on behalf of the Saudi royal family has been sentenced to three and a half years in prison.

Ahmad Abouammo, a dual U.S.-Lebanese citizen who helped oversee media partnerships for Twitter in the Middle East and North Africa, was part of a scheme to acquire the personal information of users, including phone numbers and birth dates, for a Saudi government agent.

The Justice Department has said it believes that another former Twitter employee accused of accessing user accounts and a man accused of helping the Saudi government with the scheme have fled to Saudi Arabia to evade American authorities.

According to testimony from an FBI agent presented to the Northern District of California, a Saudi government agent began courting Abouammo in 2014 by buying him gifts and depositing money in his cousin's bank account. Abouammo then began secretly accessing accounts of users who were critical of the Saudi government and sharing their email addresses and phone numbers with the government agent.

Even after Abouammo left Twitter in May 2015, he still helped the Saudi government by contacting former co-workers and encouraging them to verify particular Saudi accounts or remove posts that the Saudi agent highlighted as violating the site's terms of service, the FBI agent said in their testimony. He received hundreds of thousands of dollars and used some of that money to put a down payment on a home in Seattle, Wash. (Source)

New Electric Vehicle Company Claims Former Executives Joined Company To Steal Trade Secrets To Launch Rival Automaker - December 27, 2022

Electric vehicle upstart Canoo is alleging some of its former executives only joined the firm in order to steal its trade secrets and launch a rival auto company.

In a 58-page lawsuit filed December 22 in the United States Central District Court of California, Canoo alleges several former employees stole intellectual property, violated trade secrets policies, breached employee separation agreements, and more in order to benefit their own, new EV startup, Harbinger.

Harbinger, a Los Angeles-based EV-maker that launched in September, is led by a team of former Canoo, Faraday Future, and QuantumScape executives. They include CEO John Harris, CTO Phillip Weicker, COO Will Eberts, and VP of structures and chassis Alexi Charbonneau, all of whom are named in the suit, along with Harbinger itself. Harbinger is targeting a burgeoning commercial EV market and introduced its plan to go after the medium-duty, Class 4 through 7 segments this fall.

The suit also names Canoo's former vice president of corporate legal, securities, and global strategy, Michael Fielkow (now Harbinger general counsel, secretary, and head of corporate development), along with several investors. Its 17 claims also include breach of confidentiality and fraud. (Source)

Law Firm Suing Former Chief Operating Officer For Data Thef / Data Destruction - December 28, 2022

U.S. Law Firm Proskauer Rose is suing its former Chief Operating Officer, alleging he stole a trove of confidential information about the firm's finances, lawyer compensation and clients before leaving his job there this month.

The lawsuit filed claims Jonathan O'Brien copied sensitive internal documents to USB files and then wrongfully deleted thousands of emails before giving notice that he was leaving.

According to the complaint, O'Brien created a list of documents to steal, including each partner's client list, financial compensation and performance; software the firm developed to create proprietary reports; and confidential strategies for lateral partner recruiting. He then allegedly tricked a technology employee into letting him copy the data, saying it has been requested by an outside consultant.

O'Brien then copied the confidential files onto a USB drive, and on Dec. 16, the day his annual bonus posted, he "deleted every file on his personal network drive to try and cover up his theft," according to the complaint. (Source)

Former Construction Company Technology Manager Accused Of Stealing Proprietary Business Information - December 28, 2022

Williams Company Management Group initially sued Paul Comazzi in federal court. The case was settled recently, although a Nov. 30, 2022 court filing doesn't disclose the terms of the agreement, and the lawsuit was dismissed in December.

Williams Company accused its former construction technology manager of a data breach and taking the company's bank account statements and tax returns as well as 401(k) information with employees' names, Social Security numbers, birthdates and their compensation.

In a court filing, Williams said Comazzi "intentionally accessed Williams Co.'s server and other data information storage systems without authorization." Comazzi exceeded "the authority that he was granted when he used a colleague's username and password" to access, download and steal proprietary business information and then share it with others, the company argued.

Comazzi resigned from the company Jan. 28, telling his employer it was for "unforeseen personal reasons," according to Williams.

But Comazzi told others the real reason he quit was because he wanted to sleep in until noon and play video games all day, according to Williams' lawsuit. (Source)

Former Construction Company Technology Manager Accused Of Stealing Proprietary Business Information - December 28, 2022

Williams Company Management Group initially sued Paul Comazzi in federal court. The case was settled recently, although a Nov. 30, 2022 court filing doesn't disclose the terms of the agreement, and the lawsuit was dismissed in December.

Williams Company accused its former construction technology manager of a data breach and taking the company's bank account statements and tax returns as well as 401(k) information with employees' names, Social Security numbers, birthdates and their compensation.

In a court filing, Williams said Comazzi "intentionally accessed Williams Co.'s server and other data information storage systems without authorization." Comazzi exceeded "the authority that he was granted when he used a colleague's username and password" to access, download and steal proprietary business information and then share it with others, the company argued.

Comazzi resigned from the company Jan. 28, telling his employer it was for "unforeseen personal reasons," according to Williams.

But Comazzi told others the real reason he quit was because he wanted to sleep in until noon and play video games all day, according to Williams' lawsuit. (Source)

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

No Incidents To Report

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

Surgeon Sentenced To Prison For Accepting $3.3 Million In Illicit Payments To Perform Spinal Surgeries At Corrupt Hospital - December 9, 2022

From 2010 to 2013, Lokesh Tantuwaya accepted money from Michael Drobot, who owned Pacific Hospital in Long Beach, in exchange for Tantuwaya performing spinal surgeries at that hospital. The bribe amount varied depending on the type of spinal surgery.

Pacific Hospital specialized in surgeries, especially spinal and orthopedic procedures. Drobot, who in 2018 was sentenced to 63 months in prison for his crimes in this scheme, conspired with doctors, chiropractors and marketers to pay kickbacks and bribes in return for the referral of thousands of patients to Pacific Hospital for spinal surgeries and other medical services paid for primarily through the California Workers' Compensation System. During its final five years, the scheme resulted in the submission of more than $500 million in medical bills for spine surgeries involving kickbacks.

Tantuwaya entered into contracts with Drobot and Drobot-owned companies. Tantuwaya knew or deliberately was ignorant that the payments were being given to him in exchange for bringing his patient surgeries to Pacific Hospital.

In furtherance of the scheme, Tantuwaya met with Drobot and Drobot's employees. Tantuwaya deposited bribe checks into his bank accounts.

He knew the receipt of money in exchange for the referral of medical service was illegal and that he owed a fiduciary duty to his patients to not accept money in exchange for taking their surgeries to Pacific Hospital.

In total, Tantuwaya received approximately $3.3 million in illegal payments. (Source)

Pharmacy Employee Admits Participating In $2.4 Million Kickback And Bribery Scheme - December 22, 2022

Srinivasa Raju had various responsibilities at the Morris County Pharmacy, including coordinating prescription deliveries and soliciting business.

From January 2019 through February 2021, Srinivasa Raju worked with other pharmacy personnel to pay kickbacks and bribes to medical employees in two different doctors' offices in Jersey City, New Jersey. In exchange, those employees steered numerous, high-value prescriptions to the pharmacy where Raju worked. Raju and his conspirators paid as much as $150 for each prescription and used various tactics to conceal many of those bribe payments. Overall, the pharmacy received over $2.4 million in Medicare reimbursement payments based on prescriptions derived from the kickback scheme. (Source)

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

Employee (Trader) At Financial Services Organization & Accomplice Charged In Multimillion Dollar Insider Trading Scheme - December 14, 2022

Lawrence Billimek was a trader at a major financial services organization (FSO) , and Alan Williams, a retired financial professional and active day-trader.

They were both charged with securities fraud and wire fraud in connection with an extensive insider trading scheme, in which they stole confidential information about the trade orders of the FSO, in order to conduct over a 1000 timely, profitable securities trades in the same stocks as the FSO. Billimek attempted to hide his conduct by using prepaid, unregistered burner phones, and Williams sent millions of dollars back to Billimek for sharing the confidential information.

Billimek has been employed at the FSO since approximately 2012. The FSO is a major financial services organization that provides asset management services with over $200 billion in assets. Williams spent years working as a trader in the financial services industry. Williams is currently retired, but is an active day-trader. (Source)

Former Credit Union President Admits To Embezzling $250,000+ - December 7, 2022

Tara Kewalis was the President and Chief Executive Officer of Skyline Financial Federal Credit Union located in Waterbury., Connecticut.

From approximately September 2016 until her employment was terminated in March 2021, Kewalis used her position to access the credit union's accounting system to create fraudulent accounts and make fraudulent entries, and steal $254,532 in credit union funds. (Source)

Former Chief Financial Officer Embezzled $130,000+ - December 14, 2022

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

From April 2014 through January 2016, Bowker withheld the funds but failed to pay over to the IRS more than $3.6 million worth of income and FICA taxes.

Bowker was entrusted with a company credit card and was responsible for paying the monthly credit card bill by authorizing the electronic transfer of funds from the company's checking account to the company's Visa account. From January 2014 through December 2015, Bowker is alleged to have fraudulently used the Visa credit card to make $130,000 worth of purchases for his own benefit then paying for those charges with funds from the company's checking account. (Source)

Part Time Target Employee Stole $10,000 Stole Cash / Gift Cards - November 30, 2022

After reviewing the store's security camera footage, it was determined that 55-year-old Denise Tilson, a part-time cashier, had been stealing cash from registers, as well as stealing gift cards and merchandize.

According to the Fairfax County Police Department, a security guard at the Target on Chantilly Crossing Lane in Virginia called the police after noticing that money was missing. (Source)

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

Former Company Bookkeeper Pleads Guilty To Embezzling Over $29 Million To Fund Her Own Contruction Business - December 29, 2022

Barbara Chalmers pleaded guilty to a scheme to embezzle at least $29 million from her employer, a charitable foundation and several other companies run by a Dallas family.

Chalmers admitted that starting in at least 2012, she abused her position as bookkeeper for the family's companies and her signatory authority over the companies' bank accounts to fraudulently write herself at least 175 checks, which she deposited into her personal accounts. In order to conceal her fraudulent conduct, she provided false paperwork to tax preparers misstating the year-end cash-on-hand numbers for the various accounts from which she was embezzling. She used more than $25 million of the stolen money to fund a construction business for which she was the president. (Source)

Former Assistant City Attorney & Police Officer Charged In $7 Million+ Paycheck Protection Program Scheme / Used Funds For Rolls Royce, Motorcycle, Jewelry - December 6, 2022

Shelitha Robertson, who formerly served as an Assistant City Attorney and a Police Officer for the City of Atlanta, has been indicted for an alleged scheme to defraud the Paycheck Protection Program (PPP), a federal stimulus program authorized as part of the Coronavirus Aid, Relief, and Economic Security (CARES) Act.

Robertson and other co-conspirators allegedly submitted fraudulent PPP loan applications on behalf of various companies they owned and controlled. Robertson fraudulently obtained over $7 million in PPP loan funds, which was not used for payroll or other permitted business expenses.

Robertson allegedly used loan proceeds to purchase luxury items, including a Rolls-Royce, a motorcycle, and jewelry, and to transfer funds to family members and co-conspirators. (Source)

Former Dermatologist Office Manager & Son Charged With Embezzling $490,000 / Used Funds For Rent, Tutition, Travel, Etc. - December 15, 2022

Tianna Keller used her position as the Dermatologist Office Manager, and her authority to sign office documents, and her position as benefits manager to orchestrate schemes to enrich herself, her son, and a friend.

Keller defrauded the practice of approximately $490,000. She allegedly did this by giving herself unauthorized salary increases totaling approximately $185,061; adding family members and a friend to the payroll and providing them with unauthorized gross wages totaling approximately $46,703; failing to deposit nearly $108,000 in patient cash payments; issuing dozens of checks payable to herself and others, signing the name of the medical practice's owner without his permission; and using company funds and credit cards as payment for her rent, a daughter's tuition, restaurant, grocery, retail and other personal and travel expenses; and personal services.

Keller authorized continued enrollment and payment for family medical insurance coverage for her son, Brandyn Coffman and his family, even after his self-termination as a data clerk at the medical practice, authorizing payment of nearly $40,000 for this coverage. Blue Cross Blue Shield paid more than $14,000 in claims submitted by Coffman and his family. (Source)

Chief Financial Officer Embezzled $2.1 Million To Fund Shopping Addiction - December 1, 2022

Michele Sharar worked for Emerald City Athletics and Emerald City Health Properties for more than 25 years, rising to the role of Chief Financial Officer (CFO).

During a time period when the owner of the company had medical issues, Sharar began stealing money from the company to feed a shopping addiction.

Over a period of three years, she stole $2,144,551 by depositing third party checks to her own account, transferring money from company accounts to her own accounts, and writing checks on company accounts and depositing them to her own accounts. Sharar then falsified the company financial reports to hide the fact that she had embezzled the money.

Sharar told her employer about the theft in 2018 and agreed to attempt to pay the money back. The judge ordered Sharar to pay $2,144,551 in restitution, and ordered three years of supervised release to follow prison. (Source)

Former Company IT Director Charged With Embezzling $1 Million+ For 10 Years / Used Funds For Himself, Family, Friends - December 7, 2022

Juan Hicks who was employed at the time as IT Director for the AT Wall Companies. He, used his access to the company's computer network; his purchasing authority for computer hardware, software, and other equipment; his management authority over the company phone systems and internet services; and his access to company credit cards to orchestrate schemes in which he obtained goods and services for himself, family members, and friends, and paid personal expenses for Hicks and his family.

During a cyber-attack which took place in March 2022, AT Wall Companies hired forensic analysts to determine the source of the attack and to identify vulnerabilities. According to company officials, during that inquiry, Hicks refused to provide his computer and passwords, as per company policy. An internal investigation provided by the company to the Warwick Police Department, Homeland Security Investigations, and the United States Attorney's Office subsequently revealed that Hicks had allegedly embezzled over $ 1 Million from the company since 2012.

Hicks' alleged fraud included getting reimbursement for false expense reports and fraudulent invoices he created; enrolling family members on the company's wireless phone service plan and issuing company phones to himself and six family members; purchasing airline and entertainment tickets for himself and family members; and using a company credit card to make purchases at retail stores and payments for auto repairs. (Source)

Call Center Employee Charged For Role In Theft Of USAA Customers Bank Account Information Resulting In $1 Million+ Of Damages / Used Money To Buy Cars, House - November 23, 2022

ZarRajah Watkins was arrested for using her job at the Teleperformance Customer Call Center to gain access to bank account information of USAA customers.

Destane Glass and ZarRajah Watkins remain in a correctional center. Glass is charged with 65 counts of identity theft, Watkins with 175. Glass has been arrested previously.

Watkins sold that information to Glass and others, who used a number of tactics to defraud account holders of more than one million dollars.

Glass used the money to buy cars, lavish items and even purchase a home. Glass paid cash for the home, which last listed for $639,000. (Source)

Former Office Manager For 27 Years - Sentenced To Prison For Embezzling $700,000 / Used Funds To Purchase Cars, Renovate Home, Etc.- December 15, 2022

Pamela Smith was employed as an Office Manager for a family-owned construction company for 27 years. As part of her duties, Smith was responsible for handling the company's payroll and had access to the company's business accounts.

Dating back to at least 2008, Smith made payments on multiple personal credit cards directly from the company's business bank accounts without her employer's permission. Beginning in 2013, Smith altered her payroll to increase her weekly salary without her employer's permission. She began with a $1,000 per week increase, and, by the time her employer discovered the fraud, she was embezzling $2,000 per week. In total, Smith stole at least $700,000 from her employer.

She used the funds to purchase cars, renovate her home, and otherwise live above her means. Smith took numerous steps to conceal her criminal activity, including transferring money between business bank accounts, limiting access to the company's monthly banking statements, and altering the company's general ledger.

As part of her sentence, the court also entered an order of forfeiture in the amount of $500,000, the proceeds of the offense. The court also entered an order of forfeiture for Smith's residence, which was substantially remodeled using stolen funds, as a substitute asset. (Source)

Chief Financial Officer Sentenced To Prison For Embezzling $433,000 To Pay Off Personal Credit Cards - December 2, 2022

David McManus was the Chief Financial Officer for a Hartford-based company for nearly 14 years.

Between 2012 and 2018, McManus embezzled approximately $433,584 from the company by using company funds to pay off his personal credit card expenses, and by issuing reimbursements to himself for personal expenses unrelated to the company. (Source)

Former Bookkeeper Sentenced To Prison For $374,000 Of Wire Fraud / Used Funds For Personal Use - December 16, 202

Deonne Drawdy was employed at the architectural firm of Barron, Heinberg, and Brocato (BH&B), from approximately 2007 to 2020, as the Bookkeeper and Financial Director. Some of her duties as an employee there included issuing checks to vendors.

In 2020, BH&B noticed suspicious activity in the firm's accounts and an audit was conducted. Law enforcement agents with the United States Secret Service joined in the investigation. Their investigation revealed that on or about January 7, 2019, Drawdy issued a check on the firm's bank account made payable to Meyer, Meyer, Lacroix & Hixson. Drawdy fraudulently endorsed the check and deposited it into her personal bank account on January 10, 2019 and converted those funds for her own personal use.

Drawdy was also ordered to pay restitution in the amount of $374,331.30. (Source)

2 Former Officers Of Non-Profit Plead Guilty To Stealing $155,000 For Personal Use (Auto Repairs, Travel, Etc.) - December 1, 2022

The former Executive Director and the former Director of Operations and Finance of the now-defunct non-profit organization DC Children and Youth Investment Trust Corporation (DC Trust) each pleaded guilty today to one felony charge relating to their personal use of the non-profit's funds, which were intended for youth scholarship programs.

From at least November 2015 to February 2016, Edward Davies and Earl Hamilton perpetrated a scheme in which they obtained and used for personal benefit, DC Trust credit cards and a check card, whose bills were paid for by DC Trust funds. Davies was the Executive Director and Hamilton was the Director of Operations and Finance. The organization was dissolved in late 2016.

Davies and Hamilton used DC Trust credit cards and a check card to make hundreds of personal purchases, for expenses such as meals, automobile repairs, and personal travel for themselves, their family members, and their friends. In total, Davies admitted to stealing at least $111,000 and Hamilton admitted to stealing at least $44,000 by using DC Trust credit cards and a check card for personal expenses. (Source)

Former Bookkeeper Pleads Guilty To Using Company Credit Cards For $121,000+ Of Unauthorized Online Purchases, Even After She Was Fired - December 12, 2022

From August 1, 2019, through March 9, 2021, Tiffani Meeks was the company's bookkeeper and had duties that included paying bills, monitoring credit and bank statements, maintaining accurate accounting records, and providing those records to the company's owners upon request.

Meeks pleaded guilty to using company credit cards not issued to her to make three unauthorized personal online purchases totaling $7,329.39 between February 19, 2020, and November 3, 2020. Those purchases included $3,179.99 for an inflatable bouncy house.

Meeks further admitted that her unauthorized personal online purchases with company credit cards totaled at least $121,841.60 between February 12, 2020, and June 18, 2021. Meeks made at least $6,862.83 of the unauthorized online purchases after she was fired by the company on March 19, 2021. To hide her fraud, Meeks had the unauthorized purchases shipped to her residence, mislabeled them as legitimate payments in company records, and withheld pages listing them before providing those records to the owners. (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

2 Former Amazon Employees Pleads Guilty To Stealing $10 Million By Creating Fictitious Invoices For Fake Vendors - December 1, 2022

Kayricka Wortham and Demetrius Hines used their positions at Amazon.com, Inc., to submit more than $10 million in fictitious invoices for fake vendors, causing Amazon to pay approximately $9.4 million to Wortham, Hines, and their co-conspirators.

From about August 2020 to March 2022, Wortham worked as an Operations Manager at Amazon. She was employed at the company's warehouse in Smyrna, Georgia. In her position, Wortham supervised others and acted with authority to approve new vendors and the payment of vendor invoices.

Hines was a Loss Prevention Multi-Site Lead at Amazon. He also worked at the Smyrna warehouse and at other company sites. In his position, Hines was responsible for preventing loss, monitoring security risks, and protecting people, products, and information at Amazon.

Wortham, who was the leader of the scheme, provided fake vendor information to unknowing subordinates and asked them to input the information into Amazon's vendor system. Once the information was entered, Wortham approved the fake vendors, thereby enabling those vendor accounts to submit invoices to Amazon. Wortham and her co-conspirators, including Hines, then submitted fictitious invoices for payment. These invoices falsely represented that the fake vendors had provided goods and services to Amazon. The payments for these invoices, typically approved by Wortham, went to bank accounts controlled by Wortham and her co-conspirators. (Source)

THEFT OF COMPANY PROPERTY

No Incidents To Report

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

Former Software Engineer Steals $300,000+ From Employer By Modifying Software Code / Was Inspired By Office Space Movie - December 30. 2022

A man allegedly transferred thousands of dollars from his employer into a personal account after being inspired by the 1999 cult movie "Office Space," according to an arrest report by the Seattle Police Department.

Ermenildo Castro worked for the online retailer Zulily as a Software Engineer from December 2018 until he was fired in June

Starting in the spring of 2022, Castro began editing Zulily's software code in ways that allowed him to steal from the company, the police report said.

Police said Castro inserted three types of malicious code in the checkout process at Zulily and by using those methods, "stole a combined $302,278.52 before he was terminated in June 2022."

Zulily's fraud team was able to discover a pattern of price adjustments on several products that were sold by the company, which police said were ordered by Castro and shipped to his residence, the report said.

A OneNote document on Castro's work laptop called "Office Space Project" was found through the investigation, and in it, a "scheme to steal shipping fees," was outlined, according to the report.

Castro also told authorities he placed orders for over 1,000 items that were shipped to his house, and that they were part of a "testing process that Zulily was aware about, but he claimed that there was a script that was to be run shortly thereafter that would essentially cancel the order and ensure the orders did not process," the report said.

"He said the test orders would have to be billed to a personal credit card, thus his changing of the items' prices, as to avoid incurring a large expense on his personal credit card. He said he forgot to run the script; therefore, the orders shipped. He admitted that he did not ever notify Zulily staff of the orders being delivered," the police report said. Castro also told police he threw many of the items away once he was fired. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

No Incidents To Report

EMPLOYEE DRUG RELATED INCIDENTS

Former Physician Working At Medical Practice Sentenced To Prison For Writing 1,600 Illegal Oxycodone Prescriptions Over 8 Years / 38 Co-Conspirators Involved - December 1, 2022

From 1996 to 2020, D'livro Beauchamp practiced medicine at a Montgomery medical practice named Obelisk Healthcare.

Around 2012, Beauchamp agreed to write illegitimate and unnecessary oxycodone prescriptions. For writing each prescription, Beauchamp received $350. From 2012 to 2020, various organizers of the scheme recruited individuals to fill these illegitimate prescriptions at assorted pharmacies. Beauchamp wrote prescriptions to these recruits that he knew served no legitimate medical purpose. Recruits were typically paid between $100 and $250 per prescription filled, and the organizers then collected the oxycodone pills to sell to other distributors. Beauchamp wrote nearly 1,600 illegal prescriptions as part of the scheme, causing the illegal distribution of approximately 4,000,000 milligrams of oxycodone. In total, 38 individuals were charged for their roles in this conspiracy. (Source)

Former TSA Officer Sentenced To Prison For Accepting $8000 In Bribes / Attempting To Smuggle Methamphetamine Through LAX Airport - December 9, 2022

Michael Williams is a former Transportation Security Administration (TSA) Officer was sentenced to 70 months in federal prison for smuggling what he believed was methamphetamine through Los Angeles International Airport (LAX) in exchange for a total of $8,000 in cash.

In 2020, authorities conducted undercover operations involving Williams, whom they suspected of helping smuggle narcotics past security checkpoints at LAX. During the operations, Williams met several times with a drug source to receive what he thought was methamphetamine.

Williams agreed to deliver the "methamphetamine" in a backpack to the drug source's accomplice in the men's restroom past the airport terminal's security checkpoint.

After taking possession of what he believed was real narcotics, Williams transported an unscreened package containing the fake methamphetamine beyond the TSA screening area and delivered the package to another individual. This individual, whom Williams did not know was a federal agent, on both occasions, exchanged $4,000 in cash in the stalls of the men's restroom in the airport's secure area. (Source)

Former Cancer Treatment Center Nurse Sentenced To Prison For Stealing Medications To Satisfy Her Addiction - December 13, 2022

Between February and June 2018, Kelsey Mulvey worked as a Registered Burse at Roswell Park Comprehensive Center in New York.

Mulvey tampered with and stole controlled medications, including Dilaudid, from various medication dispensing machines located throughout the hospital, which tracked and held controlled substances meant for Rowell Park patients. She did so to satisfy her addiction. Mulvey utilized the patient medical record database to search for patients specifically prescribed hydromorphone, because to access the dispensing machine, she had to first access patient profiles. At times, Mulvey would divert vials of controlled medications from the dispensing machine and not administer the medication to any patient.

On June 27, 2018, a scheduled vacation day, Mulvey was observed accessing a dispensing machine, carrying a backpack, and exiting a medication room in which she was not assigned.

It was later determined that Mulvey had accessed the drawer for hydromorphone. She was subsequently placed on administrative leave and resigned in lieu of termination.

From June to July 2018, there was a spate of waterborne infections at Roswell Park, during which six patients became ill. An investigation by the hospital concluded that tampering of compounded hydromorphone vials was the cause. (Source)

Former Police Chief Admits Stealing & Using Heroin Seized In 2 Federal Investigations - December 13, 2022

Timothy Butler is a former Elizabeth Borough Police Chief, in Pennsylvania.

From June 2017 until December 2018, Butler, the former Chief of Police, stole hundreds of bricks and bundles of heroin from the Elizabeth Borough Police Department for his own personal use. The heroin was evidence that had been seized in two federal drug trafficking investigations and stored in the evidence locker at the police station. (Source)

Former Outpatient Surgery Center Nurse Charged With Tampering / Stealing Fentanyl - December 16, 2022

Catherine Dunton was charged with tampering with vials of liquid fentanyl at an outpatient surgery center where she worked as a licensed registered nurse.

Medical providers use a liquid form of fentanyl, fentanyl citrate to keep patients from moving during surgery and relieve their pain. While working as a nurse at a Martin County Outpatient Surgery Center in Miami, Florida,, Dunton removed liquid fentanyl from vials, refilled them with saline, and returned the adulterated vials to their location for use during surgeries. (Source)

OTHER FORMS OF INSIDER THREATS

No Incidents To Report

MASS LAYOFF OF EMPLOYEES AND RESULTING INCIDENTS

No Incidents To Report

EMPLOYEES MALICIOUS ACTIONS CAUSING COMPANY TO CEASE OPERATIONS

No Incidents To Report

WORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES

FedEx Contract Driver Arrested For Kidnapping And Murdering Missing 7 Year Old Girl - December 3, 2022

A FedEx contract driver in Texas was arrested and charged in the kidnapping and murder of a 7-year-old girl (Athena Strand), who went missing two days earlier.

County Sheriff Lane Akin told reporters: “We do have a confession”.

Athena arrived home from school in the afternoon as she usually does, and at 6:40 p.m. her stepmother reported the child missing, Akin has said.

Horner delivered a package to the home around the time she was discovered missing. Investigators believe the girl died within about an hour of the abduction. (Source)

EMPLOYEES INVOLVED IN TERRORISM

No Incidents To Report

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

SEVERE IMPACTS FROM INSIDER THREATS INCIDENTS

EMPLOYEES WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

DATA / COMPUTER - NETWORK SABOTAGE & MISUSE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

WORKPLACE VIOLENCE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

WORKPLACE VIOLENCE (WPV) INSIDER THREAT INCIDENTS E-MAGAZINE

This e-magazine contains WPV incidents that have occurred at organizations of all different types and sizes.

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

https://flipboard.com/@cybercops911/insider-threat-workplace-violence-incidents-e-magazine-last-update-8-1-22-r8avhdlcz

WORKPLACE VIOLENCE TODAY E-MAGAZINE

https://www.workplaceviolence911.com/node/994

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

CTTP = China Thousand Talents Plan

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

- Former Broadcom Engineer Charged With Theft Of Trade Secrets - Provided Them To His New Employer A China Startup Company

SOURCES FOR INSIDER THREAT INCIDENT POSTINGS

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

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

INSIDER THREAT INCIDENTS E-MAGAZINE

2014 To Present

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**4,200+ Incidents**).

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

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

INSIDER THREAT INCIDENTS MONTHLY REPORTS

July 2021 To Present

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

INSIDER THREAT INCIDENTS POSTINGS WITH DETAILS

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

Incident Posting Notifications

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

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

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

INSIDER THREAT INCIDENTS POSTINGS ON TWITTER

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

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS

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

National Insider Threat Special Interest Group (NITSIG)

NITSIG Overview

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

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

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

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

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

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

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

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

The NITSIG had to suspend meetings and the ITS&E in 2020 due to the COVID outbreak. We are working on resuming meetings in the later part of 2021, and looking at holding the ITS&E in 2022.

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

Security Behind The Firewall Is Our Business

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

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

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

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

ITDG Training / Consulting Services Offered

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

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

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

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