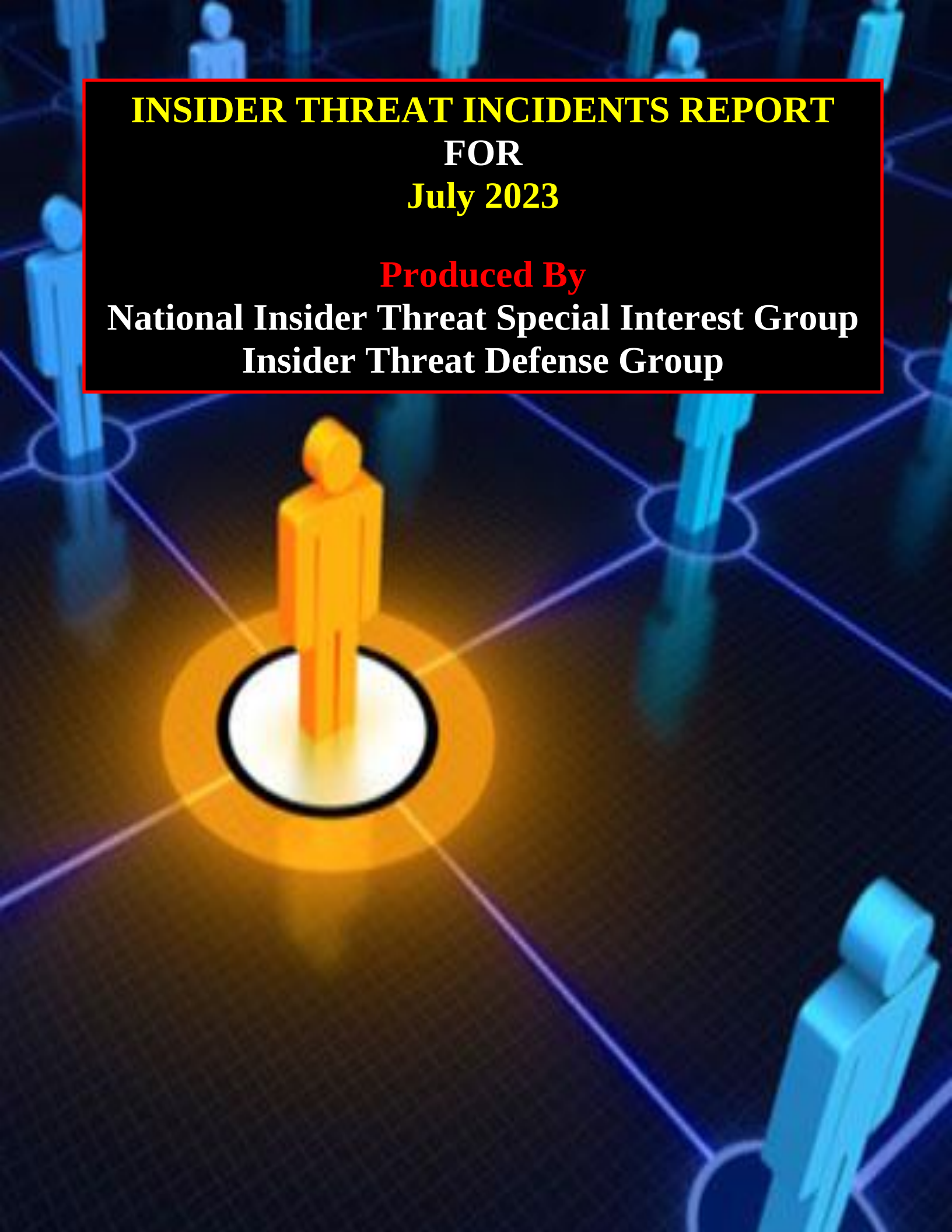


INSIDER THREAT INCIDENTS REPORT
FOR
July 2023

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

INSIDER THREAT INCIDENTS

A Very Costly And Damaging Problem

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

The National Insider Threat Special Interest Group (NITSIG) in conjunction with the Insider Threat Defense Group (ITDG) have conducted extensive research on the Insider Threat problem for 10+ years. This research has evaluated and analyzed over **4,600+** 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.

Surveys and reports that simply cite percentages of Insider Threats increasing, do not give the reader a comprehensive view of the **Actual Malicious Actions** employees' are taking against their employers. Some employees' may not be disgruntled / malicious, but have other opportunist motives such as financial gain to live a better lifestyle, etc.

Some organizations invest thousands of dollars in securing their data, computers and networks against Insider Threats, from primarily a technical perspective, using Network Security Tools or Insider Threat Detection Tools. But the Insider Threat problem is not just a technical problem. If you read any of the Insider Threat Incidents Reports published monthly by the NITSIG, you might have a different perspective on Insider Threats.

The Human Operating System (Brain) is very sophisticated and underestimating the capabilities of a **Negligent, Disgruntled**, **Malicious** or **Opportunist** employee can have severe impacts for organizations.

Some organizations need to re-evaluate their approach to detecting and mitigating Insider Threats, from a holistic approach. Successful Insider Threat Mitigation requires Key Stakeholder Commitments and Business Process Improvements. (CSO, CISO, Human Resources, Supervisors, CIO - IT, Network Security, Counterintelligence Investigators, Legal Etc.)

If you are looking to gain support from your CEO, C-Suite and Supervisors for detecting and mitigating Insider Threats, and want to provide them with the education, justification, return on investment, and funding needed for developing, managing or optimizing an Insider Threat Program, the incidents listed on pages 7 to 19 of this report should help. These reports also serve as an excellent Insider Threat Awareness Tool, to educate employees' on the importance of reporting employees' who may pose a risk or threat to the organization.

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 Conforming Change 2 & Other Sources) and be expanded.

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

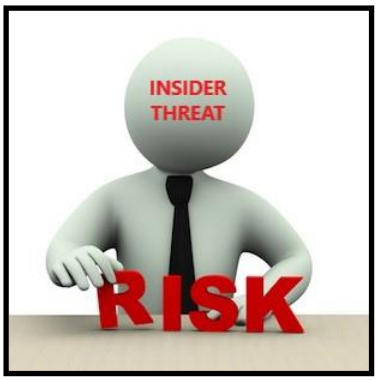
TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH

- ☐ Non-Malicious But Damaging Insiders (Un-Trained, Careless, Negligent, Opportunist, Job Jumpers, Etc.)
- ☐ Disgruntled Employees' Transforming To Insider Threats
- ☐ Damage Or 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 (Pilots, Flight Attendants, Etc.)
  - 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, Etc.)
- ☐ And Others



INSIDER THREAT DAMAGES / IMPACTS

The Damages From An Insider Threat Incident Can Many:

Financial Loss

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

Operational Impact / Ability Of The Business To Execute Its Mission

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

Reputation Impact

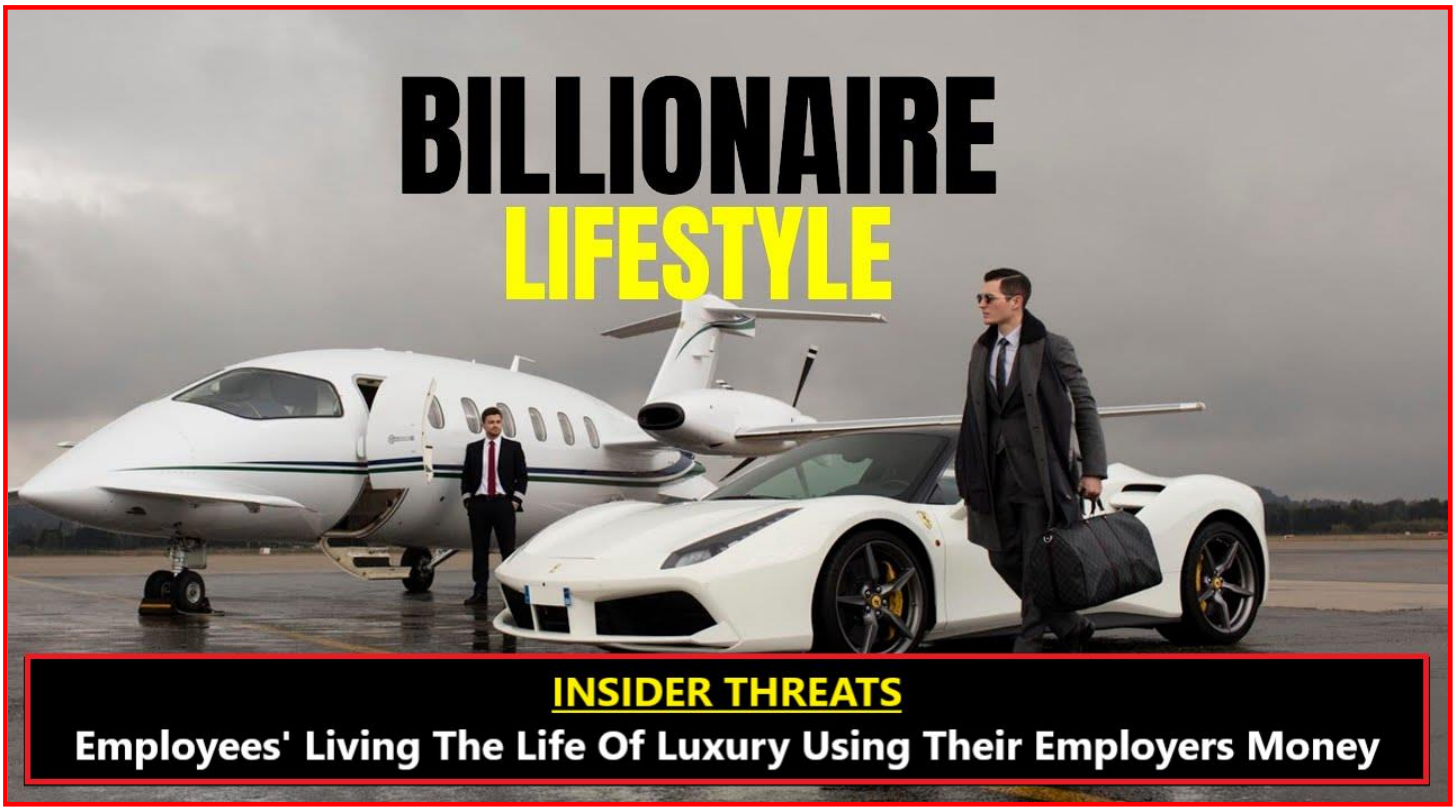
- ☐ Public Relations Expenditures
- ☐ Customer Relationship Loss
- ☐ Devaluation Of Trade Names
- ☐ Loss As A Leader In The Marketplace

Workplace Culture - Impact On Employees'

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

Legal & Liability Impacts (External Costs)

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



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

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

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

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

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

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

DISSATISFACTION, REVENGE, ANGER, GRIEVANCES (EMOTION BASED)

- ☐ Negative Performance Review, No Promotion, No Salary Increase, No Bonus
- ☐ Transferred To Another Department / Un-Happy
- ☐ Demotion, Sanctions, Reprimands Or Probation Imposed Because Of Security Violation Or Other Problems
- ☐ Not Recognized For Achievements
- ☐ Lack Of Training For Career Growth / Advancement
- ☐ Failure To Offer Severance Package / Extend Health Coverage During Separations – Terminations
- ☐ Reduction In Force, Merger / Acquisition (Fear Of Losing Job)
- ☐ Workplace Violence As A Result Of Being Terminated

MONEY / GREED / FINANCIAL HARDSHIPS / STRESS / OPPORTUNIST

- ☐ The Company Owes Me Attitude (Financial Theft, Embezzlement)
- ☐ Need Money To Support Gambling Problems / Payoff Debt, Personal Enrichment For Lavish Lifestyle

IDEOLOGY

- ☐ Opinions, Beliefs Conflict With Employer, Employees', U.S. Government (Espionage, Terrorism)

COERCION / MANIPULATION BY OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

- ☐ Bribery, Extortion, Blackmail

COLLUSION WITH OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

- ☐ Persuading Employee To Contribute In Malicious Actions Against Employer (Insider Threat Collusion)

OTHER

- ☐ New Hire Unhappy With Position
- ☐ Supervisor / Co-Worker Conflicts
- ☐ Work / Project / Task Requirements (Hours Worked, Stress, Unrealistic Deadlines, Milestones)
- ☐ Or Whatever The Employee Feels The Employer Has Done Wrong To Them

INSIDER THREAT INCIDENTS
FOR JULY 2023

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

United Kingdom

Former IT Employee Sentenced To Prison For Impersonating Ransomware Gang To Extort Employer He Worked For - July 12, 2023

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

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

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

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

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

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

U.S. GOVERNMENT

Former Social Security Administration Employee Sentenced To Prison For Stealing $324,000+ - July 13, 2023

Beginning around August 2019 and continuing through September 2021, Justin Skiff used his position as a Claims Specialist with the Social Security Administration (SSA) to fraudulently obtain money from the SSA.

Skiff used his knowledge and access to establish Social Security Numbers for ten fictitious children. He then established fictitious records of entitlements for surviving child benefits which he connected to the record of a real deceased individual. These benefits were deposited into a bank account accessible to Skiff through debit cards he directed to be mailed to a P.O. Box to which he had access. Skiff withdrew money and made purchases from this account from October 2019 through September 2021 for a total amount of $324,201.44. (Source)

U.S. Postal Worker Charged For Role In Stealing $40,000+ In Checks / Money Laundering - July 24, 2023

From at least May 2021 Jakia McMorris was an employee of the U.S. Postal Service (USPS), working as a city carrier at the North Tryon Station in Charlotte, North Carolina.

Around September 13, 2021, McMorris reported that, while she was delivering mail, she lost a USPS universal key that could open many U.S. mailboxes. After that day, McMorris allegedly stopped reporting for work at the USPS.

Beginning in September 2021, McMorris and her co-conspirators executed a scheme to commit bank fraud by stealing more than $40,000 in checks, including from the U.S. mail. The indictment alleges that the co-conspirators used stolen universal USPS keys to open multi-unit outdoor mailboxes in Charlotte and steal mail. The stolen mail included business checks.

As part of the scheme, the indictment alleges that the co-conspirators deposited the stolen checks into bank accounts they controlled, including in bank accounts in McMorris's name. It is alleged that the co-conspirators then quickly withdrew the cash from the accounts before the banks detected the fraud. McMorris allegedly received a portion of the funds as payment for using her bank accounts to perpetuate the scheme. As part of the conspiracy, the indictment also alleges that the co-conspirators attempted to disguise the payments made to the defendant by using the fraudulent proceeds in McMorris's bank account to purchase money orders, which McMorris then deposited back into her bank accounts. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

U.S. Army Financial Counselor Charged With Defrauding Families Through Investment Scheme Which Earned Him $1.4 Million In Commissions - July 7, 2023

From November 2017 to January 2023, Craffy was a civilian employee of the U.S. Army, working as a financial counselor with the Casualty Assistance Office. He was also a Major in the U.S. Army Reserves, where he has been enlisted since 2003. Craffy was responsible for providing general financial education to the surviving beneficiaries. He was prohibited from offering any personal opinions regarding the surviving beneficiary's benefits decisions. Craffy was not permitted to participate personally in any government matter in which he had an outside financial interest. However, without telling the Army, Craffy simultaneously maintained outside employment with two separate financial investment firms.

Craffy used his position as an Army financial counselor to identify and target Gold Star families and other military families. He encouraged the Gold Star families to invest their survivor benefits in investment accounts that he managed in his outside, private employment. Based upon Craffy's false representations and omissions, the vast majority of the Gold Star families mistakenly believed that Craffy's management of their money was done on behalf of and with the Army's authorization.

From May 2018 to November 2022, Craffy obtained more than $9.9 million from Gold Star families to invest in accounts managed by Craffy in his private capacity. Once in control of this money, Craffy repeatedly executed trades, often without the family's authorization. These unauthorized trades earned Craffy high commissions. During the timeframe of the alleged scheme, the Gold Star family accounts had lost more than $3.4 million, while Craffy personally earned more than $1.4 million in commissions, drawn from the family accounts. (Source)

CRITICAL INFRASTRUCTURE

Wastewater Treatment Plant Facility Employee Sabotages Network Remotely After Resigning - July, 7, 2023

Prior to the attack on the Discovery Bay Water Treatment facility, Rambler Gallo was a full-time employee of a private Massachusetts-based company identified in the indictment as Company A. Company A contracted with Discovery Bay to operate the town's wastewater treatment facility; the facility provides treatment for the water and wastewater systems for the town's 15,000 residents.

During his employment with Company A, from July of 2016 until December of 2020, Gallo was the company's "Instrumentation and Control Tech," with responsibility for maintaining the instrumentation and the computer systems used to control the electromechanical processes of the facility in Discovery Bay.

While Gallo was employed with Company A, he installed software on his own personal computer and on Company A's private internal network that allowed him to gain remote access to Discovery Bay's Water Treatment facility computer network. Then, in January of 2021, after Gallo had resigned from Company A, he allegedly accessed the facility's computer system remotely and transmitted a command to uninstall software that was the main hub of the facility's computer network and that protected the entire water treatment system, including water pressure, filtration, and chemical levels. (Source)

United Airlines Pilot Removed From Service After Showing Up Drunk To Fly - July 28, 2023

A United Airlines pilot was removed from service after reportedly showing up drunk to work a flight from Paris to Washington, D.C., on Sunday afternoon.

French media reported that the pilot, identified as 63 year-old Henry W., received a six-month-long suspended prison sentence and was fined, in addition to having his license suspended for a year.

Le Parisien reported Wednesday that the pilot had a blood alcohol concentration of more than three times the legal limit set by the Federal Aviation Administration (FAA).

The FAA said violations of its drug and alcohol testing regulation include those who used alcohol while on duty, those who used alcohol eight hours prior to duty for pilots, those who used alcohol within eight hours following an accident and an alcohol test resulting in a concentration of 0.04% or greater. (Source)

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

Las Vegas Police Officer Convicted Of Committing 3 Casino Robberies Taking $164,000+ - July 14, 2023

Caleb Rogers stole approximately $73,810 from a casino in the western part of Las Vegas on November 12, 2021. A few months later, on January 6, 2022, he robbed a casino in North Las Vegas of approximately $11,500. In both robberies, he walked directly to the casino's cashier cage and demanded money from the cashiers.

The third robbery occurred on February 27, 2022, in which Rogers ran toward two casino employees in the sportsbook area and yelled: "Get away from the money. I've got a gun. I will shoot you!" Rogers climbed over the counter and shoved one of the employees to the floor, before grabbing approximately $78,898 and placing it into a bag. Rogers fled when the employees triggered an alarm. As Rogers ran toward the parking garage, a casino security officer tackled him.

Rogers drew a .357 caliber revolver and, with his finger on the trigger, threatened: "I'm going to shoot you!" Security officers were able to disarm Rogers and restrain him until LVMPD officers arrived. The officers arrested Rogers and seized his firearm. Checking the revolver's serial number, officers learned that it belonged to the LVMPD. (Source)

Correctional Officer Sentenced To Prison For Accepting $77,000+ In Bribes From Inmates And Assaulting Inmate He Suspected Of Cooperating With The Government - July 25, 2023

From at least October 2019 through February 2020, Perry Joyner was a Correctional Officer at the Metropolitan Correctional Center (MCC), New York.

Joyner received approximately $77,894 in bribe payments from MCC inmates or their associates in exchange for Joyner smuggling to inmates drugs (including, but not limited to, oxycodone, alprazolam, Suboxone, marijuana, and K2), cellphones, cigarettes, and alcohol. MCC inmates then used, sold, or exchanged that contraband amongst themselves and resold it to other inmates.

In or about February 2020, Joyner believed a particular inmate (Inmate-1), who had previously bribed Joyner, was cooperating with the Government. In response, Joyner requested other inmates slash or otherwise assault Inmate-1 as retribution and intimidation. Before any inmate followed through on Joyner request, Inmate-1 was moved out of the MCC. (Source)

Detention Officer For Immigration & Customs Enforcement Charged For Role In $100,000 Scheme COVID-19 Relief Fraud - July 12, 2023

Anthony Faustin submitted fraudulent Paycheck Protection Program loan applications on behalf of six individuals in 2021. In the loan paperwork, Faustin made the applicants appear eligible for pandemic relief by misrepresenting them as sole proprietors or lying about their prior years' income (or both). Lenders disbursed over $100,000 to bank accounts controlled by the individuals, who would then withdraw the money and gave Faustin his cut.

At the time of the alleged crimes, Faustin was a contractor with Immigration and Customs Enforcement working as a Detention Officer at Krome North Service Processing Center in Miami. (Source)

Former Miami-Dade Police Officer Pleads Guilty To $125,000+ Of COVID-19 Relief Fraud - July 5, 2023

Samuel Harris, who was a full-time Miami-Dade Police Department Police Officer, also was the Owner and President of Oregen Digital, Inc. (Oregen). Working with an associate, on June 29, 2020, Harris submitted and caused to be submitted a false and fraudulent PPP loan application falsely claiming that Oregen had 10 employees and a monthly payroll of over $50,000 per month.

In support of this application, Harris submitted a fraudulent IRS Form W-3 falsely claiming that Oregen had paid 10 employees over $602,000 in wages during 2019. As a result of this false and fraudulent application, Harris obtained a $125,579 PPP loan from a Georgia-based SBA-approved PPP lender.

Harris also admitted that on June 30, 2020, he caused to be submitted to the SBA a false and fraudulent EIDL application in the name of Oregen, seeking both an EIDL and an EIDL advance.

In this fraudulent application, Harris falsely claimed that for the twelve-month period prior to January 31, 2020, Oregen had gross revenues of over $859,000 and 10 employees.

As a result of this fraudulent application, Oregen obtained from the SBA a $10,000 EIDL advance that did not need to be repaid and $149,900 in EIDL loan proceeds. (Source)

Former D.C. Police Union Vice Chairman Sentenced To Prison For $33,000+ Time & Attendance Fraud Scheme - July 26, 2023

Medgar Webster is a former Metropolitan Police Department (MPD) Officer, Washington, and Vice Chairman of the D.C. Police Union.

Webster engaged in unauthorized outside employment at three Whole Foods Market locations in Washington, D.C. between January 2021 and April 2022, while concurrently employed by MPD. Although employment outside of MPD may be permitted in certain circumstances, Webster never submitted the necessary administrative forms or received the proper authorizations, which are required by MPD, in part, to maintain records of an MPD member's hours worked throughout the year.

Acting unchecked during this period, Webster stole more than $33,845 from MPD after billing MPD for regular, overtime and holiday hours that he never worked. In total, Webster worked more than 1,400 hours of outside employment at Whole Foods, of which 514 hours were worked simultaneously with time he fraudulently reported working for MPD. This double-billed time included submissions by Webster for 246.5 hours in overtime pay, at an adjustable hourly rate of $79.67 per hour. (Source)

Customs & Border Protection Officer Charged For Receiving Bribes, Allowing Drug-Laden Vehicles To Enter U.S. - July 5, 2023

U.S. Customs and Border Protection Officer Leonard Darnell George was charged with accepting bribes to allow vehicles containing drugs such as fentanyl and methamphetamine to pass through the border into the U.S.

In addition, George is charged along with Mario Angel Gutierrez, Esteban Galvan and four other unnamed defendants with conspiracy to import and conspiracy to distribute controlled substances in the Southern District of California and elsewhere. The defendants allegedly coordinated the smuggling of methamphetamine, fentanyl, cocaine, and heroin from Mexico with an ultimate destination of the United States.

Officer George is charged separately with receiving bribes. The indictment alleges that he did directly and indirectly corruptly demand, seek, receive, accept, and agree to receive items of value in return for being induced to permit narcotics laden vehicles entry into the United States in violation of his official duties, that is failing to enforce controlled substances and customs laws of the United States. (Source)

3 Miami TSA Officers Arrested For Stealing From Flyers During Airport Screening - July 12, 2023

3 TSA officers at Miami International Airport were arrested for allegedly stealing from airline passengers, including swiping hundreds of dollars in cash from a man's wallet.

Josue Gonzalez, Elizabeth Fuster and Labarrius Williams were charged with organized scheme to defraud. Gonzalez, Fuster and Williams were captured on surveillance footage working together to steal from passengers as they went through routine TSA screening checks

Miami International Airport authorities began investigating several reports of theft at Security Checkpoint E, where the officers were stationed. Security footage at the checkpoint reportedly showed that while some of the officers attempted to distract passengers as they went through screenings, the others would rifle through passengers' belongings in search of money.

In one instance, the 3 officers managed to steal $600 from a single passenger's wallet. Cameras reportedly caught them engaging in multiple other instances of theft.

After a formal interview process at the TSA Command Center, according to the reports, Gonzalez and Fuster waived their rights and provided written confessions. Williams, however, did not waive his rights and provided no communication. (Source)

STATE / CITY GOVERNMENTS / MAYORS

Former Contractor For Michigan Unemployment Insurance Agency Sentenced To Prison For Role In $300,000+ COVID-19 Fraud Scheme - July 18, 2023

Semaje Reffigee began working as an Unemployment Insurance Examiner (UIE) with the MUIA in October 2020, and as such, had electronic access to the MUIA claims database.

Reffigee used her credentials to access and approve specific UI claims submitted to the agency. Between October 2020 and June 2021, Reffigee conspired with others to obtain benefits through the submission of false UI claims. Reffigee's co-conspirators electronically submitted fraudulent claims to MUIA. Reffigee then abused her position as a UIE to (1) re-activate claims that had previously been flagged for fraud, and (2) go outside her assigned workflow to approve fraudulent claims in the first instance. In total, Reffigee re-activated or approved over 35 fraudulent claims valued at more than $300,000. In exchange, Reffigee received kickback payments from her co-conspirators. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

School Bookkeeper Sentenced To Prison For Stealing $130,000+ From 2 School Districts - July 12, 2023

Amy Burley was employed as a Bookkeeper for Barnstead School District and then Hampton School District (New Hampshire). In her role, Burley processed payroll and handled the payment of invoices.

Burley used her access at Barnstead School District to alter her payroll information, make personal student loan payments and payments to personal creditors, and pay for an Amazon account charged to Barnstead but controlled by Burley, totaling $110,295.26. Following her termination from Barnstead, Burley was hired as a bookkeeper at Hampton School District, where she used again her position to use district funds to pay student loans and credit cards belonging to her or her family members, totaling $20,966.52. Burley was also ordered to pay $131,261.81 in restitution. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

Executive Pastor Sentenced To Prison For Stealing Approximately $130,000 From Church To Pay Off Gambling Debts - July 19, 2023

Between January 2017 to March 2020, as the Executive Pastor of the Journey Baptist Church, Gregory Neal made unauthorized withdrawals of the church's funds to pay off his gambling debts. He also made unauthorized purchases with the church's credit cards for his own benefit, including items from various vendors and retail stores. These unauthorized transactions amounted to $129,960.13. (Source)

LABOR UNIONS

No Incidents To Report

BANKING / FINANCIAL INSTITUTIONS

Bank Director Convicted For $1.4 Million Of Bank Fraud Causing Bank To Collapse

In or about 2009, Mendel Zilberberg (Bank Director) conspired with Aron Fried and others to obtain a fraudulent loan from Park Avenue Bank. Knowing that the conspirators would not be able to obtain the loan directly, the conspirators recruited a straw borrower (Straw Borrower") to make the loan application. The Straw Borrower applied for a $1.4 Million loan from the Bank on the basis of numerous lies directed by Zilberberg and his coconspirators.

Zilberberg used his privileged position at the bank to ensure that the loan was processed promptly. Based on the false representations made to the Bank and Zilberberg's involvement in the loan approval process, the Bank issued a $1.4 Million loan to the Straw Borrower, which was quickly disbursed to the defendants through multiple bank accounts and transfers. In total, Zilberberg received more than approximately $500,000 of the loan proceeds. The remainder of the loan was split between Fried and another conspirator.

The Straw Borrower received nothing from the loan. The loan ultimately defaulted, resulting in a loss of over $1 million. (Source)

Former Bank Vice President Pleads Guilty To Embezzling $550,000 Over 7 Years - July 6, 2023

Angela Flippin was the Vice President and Chief Operating Officer at the People's Bank of Moniteau County, in Missouri. She was also the board secretary for many years and held that position when she was terminated.

Flippin admitted that she embezzled at least $550,000 from 2010 to Jan. 30, 2017. The government believes she embezzled $645,638 and will present evidence for that amount at the sentencing hearing.

In January 2017, the Missouri Division of Finance discovered improper transactions involving Flippin.

From 2010 through 2017, three areas of improper activity were identified; improper disbursements; improper expense reimbursements; and improper insurance premiums. Through their analysis, auditors determined Flippin received more than $550,000 in improper comp time disbursements and more than $8,000 in improper expense reimbursements.

Flippin personally held three separate bank accounts. Analysis of these bank accounts by federal investigators found Flippin made payroll deposits in the amount of $105,750. In addition to Flippin's payroll deposits there were other deposits which totaled $892,782. Analysis of expenditures from Flippin's bank accounts found $338,569 in PayPal online shopping transactions and other general debit card transactions. (Source)

Bank Teller Supervisor Pleads Guilty To Stealing $375,000 From Bank Vault - July 21, 2022

Between July 2022 and December 2022, Pablo Rocha worked as a Bank Teller Supervisor at a federally insured bank in Massachusetts. Rocha used his access to the bank's vault to steal cash. Rocha then covered his tracks by writing false entries in the bank's records and by processing fake transactions in the bank's electronic records system to make it appear that the cash had been shipped to the Federal Reserve Bank of Boston. In total, Rocha stole approximately $375,000. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

No Incidents To Report

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

No Incidents To Report

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

Doctors Office Receptionist Arrested For Stealing $40,000+ From Patients - July 26, 2023

Angelina Mena was a Receptionist at MacDonald Family EyeCare.

Mena was allegedly illegally using patients' credit card information to commit credit card fraud, according to the police. Police found that Mena used her own Square account to steal approximately $44,000 from 76 patients. (Source)

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

Former Bookkeeper Sentenced To Prison For Embezzling $55,000+ - July 7, 2023

Melanie Titus was employed as the Bookkeeper for the Minto Village Council, which is the federally recognized native governing body for the Native Village of Minto.

Starting in January 2015, the defendant began embezzling funds from the Minto Village Council's accounts by issuing herself multiple payroll checks for the same pay periods, tendering duplicative deposits, and falsifying reimbursements for work expenses over the years for personal enrichment. She never returned the money. In May 2019, the defendant confessed her theft to the Minto Village Council, and a federal investigation ensued, revealing that her scheme resulted in an actual loss of $55,753.99. (Source)

EMPLOYEES' WHO EMBEZZLE / STEAL MONEY FOR PERSONAL ENRICHMET AND TO LIVE ENHANCED LIFESTYLE OR TO SUPPORT GAMBLING OR DEBIT PROBLEMS

NASA - JPL Employee Pleads Guilty To COVID-19 Economic Relief Program Fraud ($151,000) / Used Some Proceeds To Grow Marijuana - July 24, 2023

A NASA-Jet Propulsion Laboratory (JPL) employee has agreed to plead guilty to defrauding a government-sponsored loan program designed to help people and businesses survive the COVID-19 pandemic's economic impact and has admitted that he used part of the proceeds to fund illegal marijuana cultivation, the Justice Department announced today.

Armen Hovanesian was a Cost Control And Budget Planning Resource Analyst for the NASA-Jet Propulsion Laboratory (JPL).

From June 2020 to October 2020, Hovanesian submitted three loan applications in the names of business entities under his control to the Economic Injury Disaster Loan Program (EIDL), a program administered by the Small Business Administration (SBA) that provided low-interest financing to small businesses, renters, and homeowners in regions affected by declared disasters, including businesses impacted by the COVID-19 pandemic.

Hovanesian admitted to making false and fraudulent statements in the loan applications concerning the gross revenues each of the businesses had generated in the preceding year as well as false and fraudulent statements concerning his intended use of loan proceeds.

Hovanesian certified to the SBA under penalty of perjury that he would "use all the proceeds" of the loans for which he applied and caused others to apply for "solely as working capital to alleviate economic injury caused by disaster" consistent with the terms and limitations of the EIDL program. But Hovanesian instead applied those proceeds toward his own prohibited personal benefit to repay a personal real-estate debt and fund his illegal marijuana cultivation. Hovanesian fraudulently caused the SBA to transfer via interstate wire EIDL proceeds totaling $151,900. (Source)

Former Private School Business Manager Sentenced To Prison For $684,000 Of Wire Fraud / Spent Funds On Travel, Jewelry - July 17, 2023

James Melis was involved a fraud schemes. Melis abused his position as Business Manager at a private school in Hillsborough County, Florida by fraudulently attaching his personal bank account to one of the school's financial accounts. When parents made tuition payments, Melis initiated fraudulent electronic funds transfers to his personal account. He then spent the stolen funds on travel and luxury items, including jewelry. (Source)

The court also ordered Melis to pay $684,000 in restitution. (Source)

Former Office Administrator Charged With Embezzling $500,000 Over 6 Years / Used Funds For Airline Tickets, TV, Hot Tub, Sports Tickets, Etc. - July 13, 2023

Stephanie Pratt was the Office Administrator for a company based in Hinsdale, New Hampshire. She had full access to the company's finances, including its bank accounts and credit cards.

Over the course of six-and-a-half years, Pratt stole more than $500,000 from the company. She cashed unauthorized checks to herself and entered them as payments to legitimate vendors in the company's accounting system.

Pratt also used the company's credit cards to make unauthorized personal purchases, including for items like plane tickets, a smart TV, a hot tub, Patriots tickets, and miscellaneous herbs and spices. (Source)

Former San Francisco Senior Building Inspector Sentenced To Prison For Accepting $260,000 Of Illegal Gratuities (Interest Free Loan) - July 17, 2023

Bernard Curran is a former San Francisco Senior Building Inspector.

Curran admitted that he received cash payments from a San Francisco developer "in connection with and as rewards for" the inspections that he conducted or for the approvals that Curran granted as an inspector. In addition, Curran admitted that he accepted what amounted to a $260,000 interest-free loan from the same developer, $30,000 of which was never paid back. Curran admitted that he understood the developer never required the outstanding $30,000 balance to be repaid, "in part due to our friendship, but also in connection with and as a reward for conducting past and future inspections," on the developer's projects.

Further, Curran admitted that in 2021, the San Francisco City Attorney's Office investigated potential conflicts of interest related to his employment and, in response, Curran falsely certified that the loan he received was not from the developer, but rather was from a relative and had been issued at a 6% interest rate. Curran admitted that he submitted this false statement in an effort to deceive the City officials. (Source)

Company Accounting Clerk Steals $28,000+ From Employer Using Credit Card For Personal Expenses - July 20, 2023

Between June 2017 and April 2021, Angelia Holt stole more than $28,000 from her employer by using a credit card issued to another employee for unauthorized personal expenses and then altering the invoices to conceal the theft. Holt was employed as an accounting clerk for the organization. (Source)

Bookkeeper Admits To Embezzling $8,500+ From 2 Businesses To Pay For Personal Debt - July 13, 2023

Between 1997 and 2019, Tara Durnell worked as a Bookkeeper for Kronebusch Electric, Inc., (KEI) a small company in Conrad, Montana.

Durnell used her access to pre-signed company checks to make payments to cover personal expenses and then miscoded the payments in the accounting system to make them look like legitimate business expenses. As part of the scheme, Durnell used a pre-signed KEI check to make an unauthorized payment of $5,175 to the TNT Tavern for a personal debt. KEI eventually discovered the embezzlement when it sought to sell the company, and due diligence uncovered several hundred thousand dollars in miscoded transactions.

Durnell left employment with KEI and found a job as a Bookkeeper with Mitchell's Crash Repair in Great Falls. In January 2022, Durnell used her access to the business's pre-signed checks and mailed an unauthorized payment of $3,564 to the Pondera County Treasurer to cover a personal debt. (Source)

Former San Francisco Public Utilities Commission General Manager Convicted Of Accepting Bribes (Luxury Vacations) For City Contracts - July 17, 2023

Harlan Kelly is the former General Manager of the San Francisco Public Utilities Commission (PUC).

He was convicted of charges that he accepted bribes and gifts from a local businessman in a scheme to provide confidential information about the city public bidding process and steer city contracts to that person's businesses.

Kelly was appointed in 2012 as General Manager of the San Francisco PUC, had access to confidential information about city contract bidding processes, and the ability to influence the awarding of some city contracts.

Documents and testimony showed that Kelly had a close personal and professional relationship with San Francisco business owner and contractor Walter Wong, and that during the time Wong both conducted business with the city and sought additional lucrative contracts to supply the PUC with LED streetlights.

While he was doing business with the city and seeking contracts, Wong provided numerous gifts, benefits, and bribes to Kelly. These bribes including discounted construction work on Kelly's personal residence and a lavish international trip hosted by and in part paid for by Wong. Evidence showed that Wong paid travel and personal expenses for Kelly and his family during a March 2016 Kelly family vacation to Hong Kong, Macau, and China, and that Wong paid for hotel expenses and incidentals such as meals and luxury excursions.

Wong has previously pleaded guilty to charges that he engaged in an honest services fraud conspiracy in connection with his interactions with Kelly and others. (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

Former Amazon Manager Sentenced To Prison As Mastermind In $10 Million Fake Invoice Fraud Scheme - July 5, 2023

Kayricka Wortham abused her position at Amazon to submit more than $10 Million in fictitious invoices for fake vendors, causing Amazon to pay approximately $9.4 million to Wortham and her other 6 co-conspirators.

From about August 2020 to March 2022, Wortham worked as an Operations Manager at the Amazon Warehouse in Smyrna, Georgia. In her position, Wortham supervised others and acted with the authority to approve both new vendors and the payment of vendor invoices for 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, enabling them to submit invoices. Wortham and co-conspirators then submitted fictitious invoices to Amazon, falsely representing that the vendors had provided goods and services to Amazon. Wortham approved the invoices, causing Amazon to transfer millions in fraudulent proceeds to bank accounts controlled by her and her co-conspirators.

Wortham conspired with others, including Brittany Hudson, in the scheme. Hudson was in a relationship with Wortham and owned a business. Hudson allegedly worked with Wortham to submit millions in fictitious invoices for fake vendors to Amazon.

Wortham and Hudson purchased expensive real estate and luxury cars, including a nearly $1 Million home in Smyrna, Georgia, a 2019 Lamborghini Urus, a 2021 Dodge Durango, a 2022 Tesla Model X, a 2018 Porsche Panamera, and a Kawasaki ZX636 motorcycle, all with fraudulent proceeds from the scheme.

Wortham also recruited co-conspirators Demetrius Hines, who was in Loss Prevention at Amazon, and Laquettia Blanchard, who worked as a Senior Human Resources Assistant at the company.

Hines also recruited Jamar L. James, Sr., another Operations Manager at Amazon's location in Duluth, Georgia, into the scheme. Like Wortham, James allegedly approved fake vendors and fictitious invoices, including after Wortham left Amazon in March 2022. (Source)

Former State County Employee Pleads Guilty To Stealing $1.7+ Million In County Funds By Falsifying Invoices - July 19, 2023

John Gibson pleaded guilty to defrauding Wayne County in Detroit) out of nearly $2 Million in taxpayer funds.

Gibson and his supervisor, fellow Wayne County employee Kevin Gunn engaged in a scheme to use taxpayer dollars to make unauthorized purchases of generators and other power equipment from retailers in southeast Michigan which they sold for personal profit. Gunn pleaded guilty to these charges in January and is awaiting sentence.

The investigation determined that between January 2019 and August 2021, Gunn and Gibson solicited vendors to purchase generators and other power equipment from local retailers on behalf of Wayne County. The vendors then submitted invoices for these items to Wayne County.

To conceal the scheme to defraud, Gunn instructed the vendors to falsify the invoices they submitted to the Roads Division by listing items the vendors were authorized to sell to the county under their contracts, rather than the generators and power equipment they were unlawfully acquiring at Gunn's and Gibson's direction. Roads Division employees then approved and paid each vendor's invoice with taxpayer funds.

Next, Gibson took possession of the equipment, paid Gunn for the items, and resold the generators and other items for personal profit.

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

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

No Incidents To Report

THEFT OF ORGANIZATIONS ASSESTS

No Incidents To Report

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

No Incidents To Report

EMPLOYEE DRUG RELATED INCIDENTS

No Incidents To Report

OTHER FORMS OF INSIDER THREATS

Former ATM Technician Sentenced To Prison For Tampering With ATM's - Then Robbed ATM Technicians Sent To Repairs ATM's - July 18, 2023

Johnson Saint-Louis was a former ATM technician who traveled around the southeast Florida tampering with ATMs serviced by his former employer. Over a two-year period, Saint-Louis robbed four ATM technicians sent out to fix problems Saint-Louis had caused.

The FBI's financial investigation revealed that Saint-Louis, who had been unemployed since mid-2019, was making large cash deposits into his bank accounts (e.g., $89,939 in 2021) and gambling large amounts of money (e.g., losing $189,814 in 2021). Saint-Louis was ordered to pay $104,840.00 in restitution. (Source)

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'

Employee Who Lost Job Killed After Shooting / Killing 2 Co-Workers - July 17, 2023

A manhunt for the former employee who opened fire on co-workers at a Louisiana shipyard ended in a deputy-involved shooting.

Two men were killed when the former employee opened fire at FMT Shipyard and Repair in Harvey, Louisiana.

Authorities say that the two men were targeted by the suspect, who was recently fired from the business.

The former employee opened fire on the deputies. The officers returned fire, killing him. (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

EMPLOYEE EXTORTION

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

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

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

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

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

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

EMPLOYEES' WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

DATA / COMPUTER - NETWORK SABOTAGE & MISUSE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

UNDERAPPRECIATED / OVERWORKED / NO OVERSIGHT

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

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

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

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

WORKPLACE VIOLENCE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

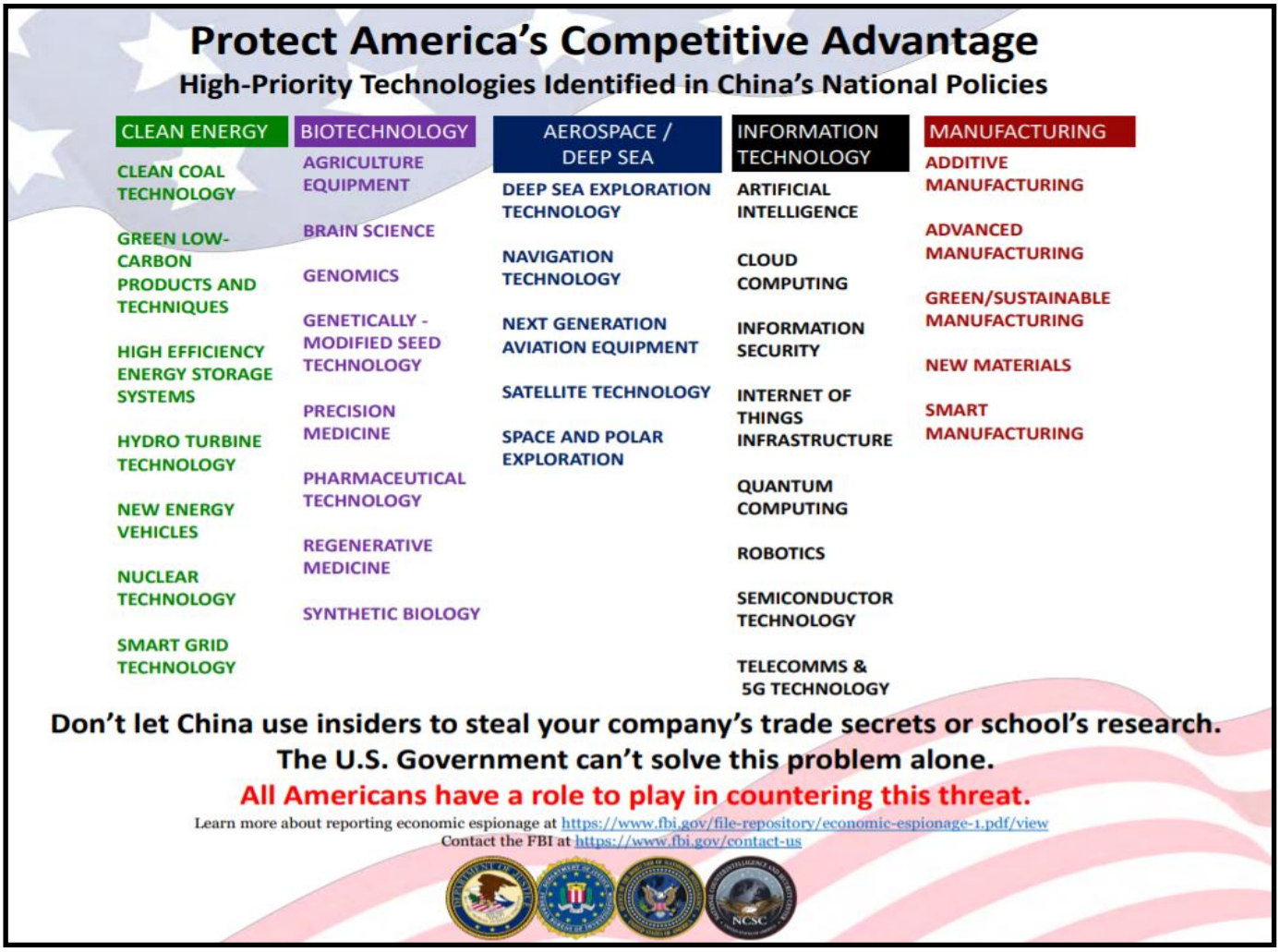
WORKPLACE VIOLENCE TODAY E-MAGAZINE
https://www.workplaceviolence911.com/node/994

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

CTTP = China Thousand Talents Plan

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

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



SOURCES FOR INSIDER THREAT INCIDENT POSTINGS

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

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

INSIDER THREAT INCIDENTS E-MAGAZINE

2014 To Present / Updated Daily

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**4,600+ 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

Updated Daily

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

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS

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

National Insider Threat Special Interest Group (NITSIG)

NITSIG Overview

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

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

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

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

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

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

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

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

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

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

Security Behind The Firewall Is Our Business

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

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

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

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

ITDG Training / Consulting Services Offered

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

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

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

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