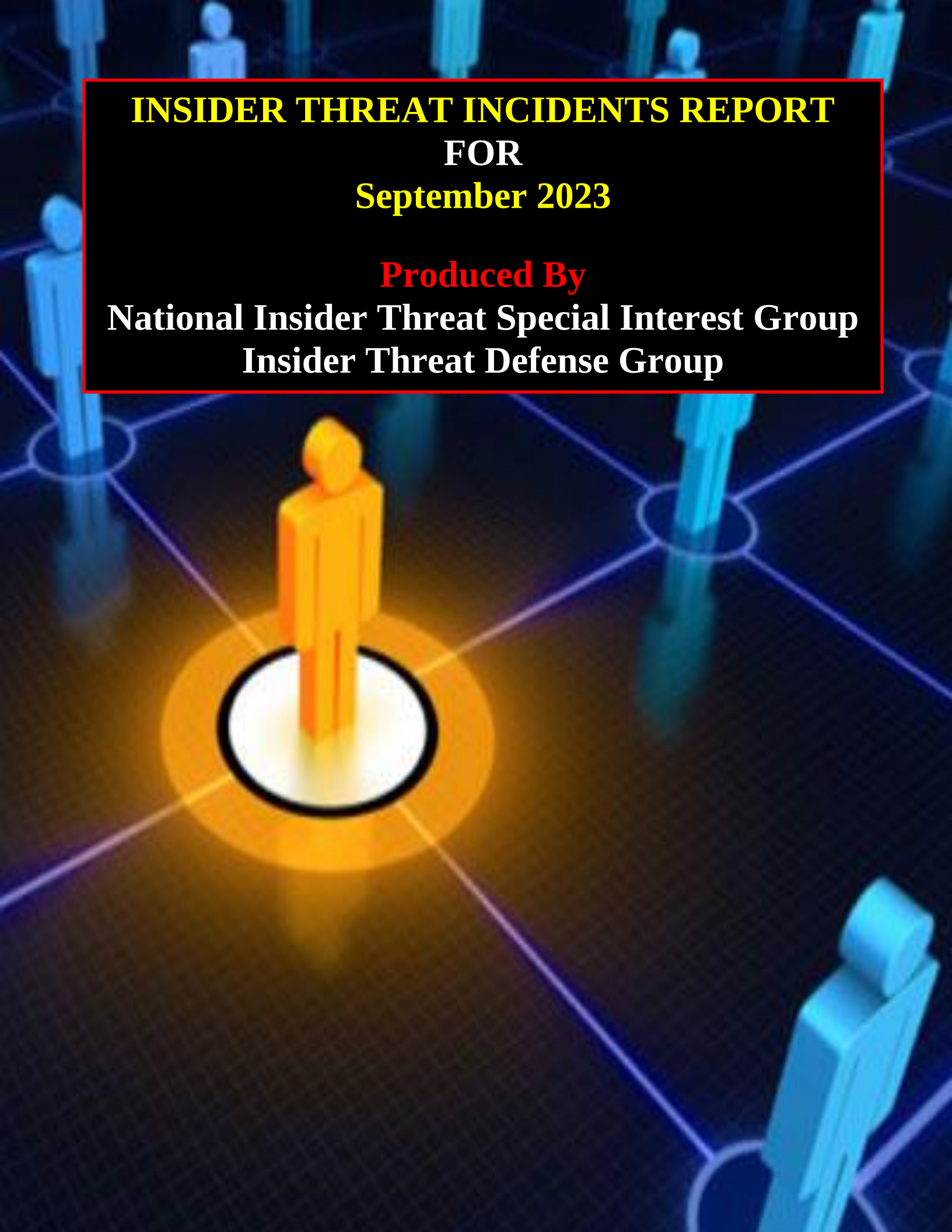


INSIDER THREAT INCIDENTS REPORT
FOR
September 2023

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 **4,700+** 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 must 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 using 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 22 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.

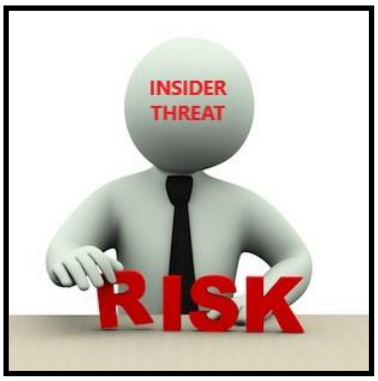
TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH

- ☐ 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

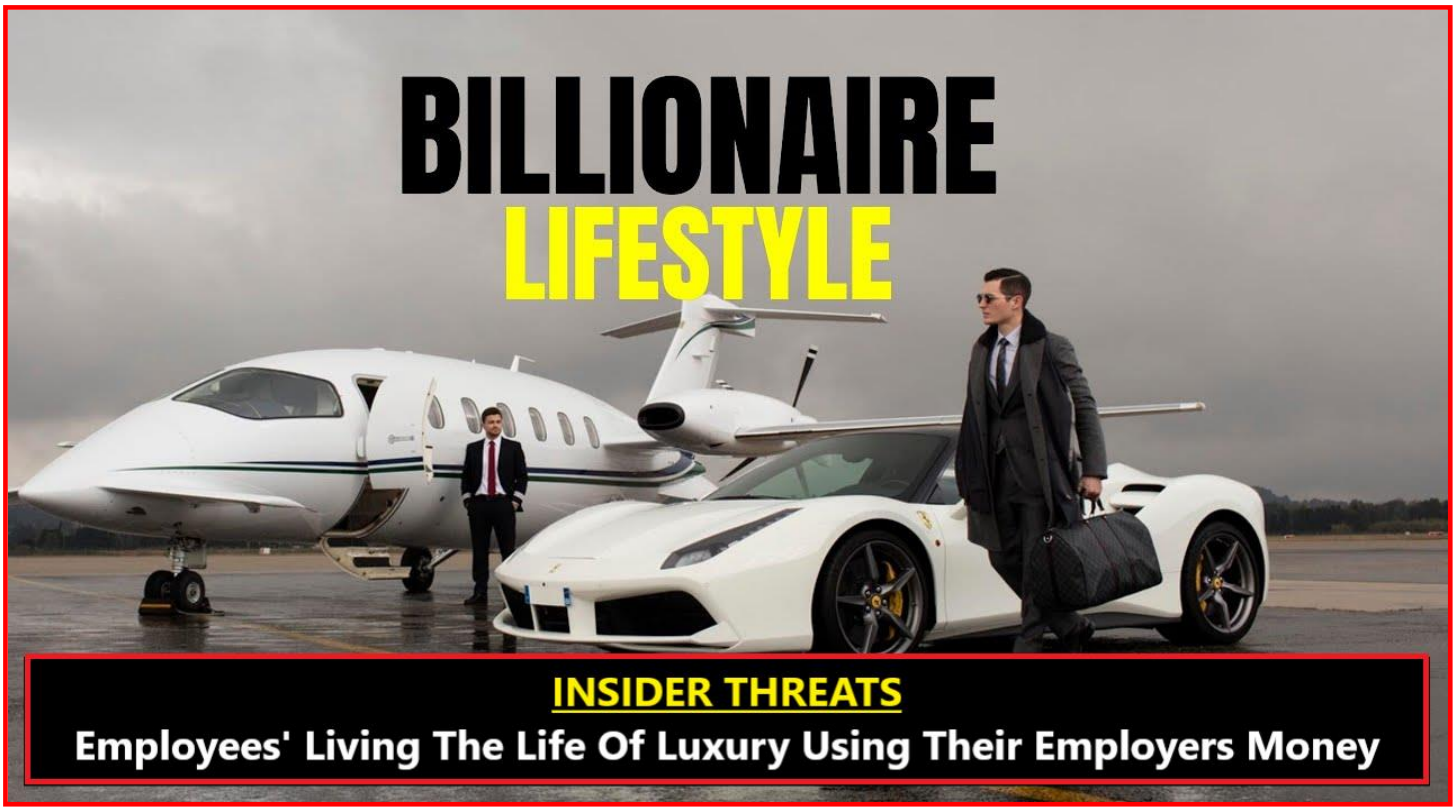
- ☐ Public Relations Expenditures
- ☐ Customer Relationship Loss
- ☐ Devaluation Of Trade Names
- ☐ Loss As A Leader In The Marketplace

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 SEPTEMBER 2023

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

Former German Intelligence Officer Charged With Treason For Spying For Russia - September 6, 2023

Germany's federal prosecutor reportedly filed charges against Carsten L., a former senior employee of Germany's Federal Intelligence Service (BND), before the Berlin Court of Appeal.

Police arrested him in December on suspicion of trading state secrets with Russian agents and sharing intelligence obtained through his work about the war in Ukraine, Reuters reported.

Another man, Arthur E., was also charged with treason as prosecutors believe he helped Carsten L. communicate with the Russia's Federal Security Service, the FSB.

Carsten L. was for many years the head of the BND department overseeing surveillance of phones, internet and satellite communication. Shortly before his arrest, he was promoted and put in charge of screening employees, according to German reports.

He reportedly met Arthur E., a Russian businessman, at a party in Bavaria in 2021. It is believed Carsten L. gave classified documents with information concerning the war in Ukraine and Russian mercenary group Wagner to Arthur E., who in turn traveled to Moscow and handed them over to the FSB. (Source)

U.S. GOVERNMENT

Former U.S. Postal Carrier & Husband Plead Guilty For $8.8+ Million Mail Theft Scheme - September 15, 2023

Kiara Padgett was employed by the U.S. Postal Service as a Mail Carrier with a postal route in West Charlotte, NC.

From August 2021 to November 2022, Padgett used her position as a Postal Carrier to steal incoming and outgoing checks of businesses and individuals. Padgett sold the stolen checks to Dominique Dunlap her husband, using Dunlap as her intermediary to other individuals, including to Terrell Alexander Hager, Jr. The total face value of the checks stolen by Padgett was over $8.8 Million.

Dunlap negotiated with Hager, Jr. about the sale of stolen checks over text messages, and sent Hager, Jr. photographs of stacks of stolen mail and of stolen checks of victim companies on Padgett's postal route.

In March 2023, Hager, Jr. pleaded guilty to conspiracy to commit bank fraud. Between August 2021 and November 2022, Hager, Jr. and other individuals obtained stolen checks from Padgett through Dunlap. Hager, Jr. and his co-conspirators deposited the stolen checks into bank accounts they controlled, and then made cash withdrawals before the financial institutions detected the fraud. Over the course of the scheme, Hager, Jr. and his co-conspirators deposited more than $66,000 in stolen checks and money orders. Hager, Jr. also posted online for sale more than 400 stolen checks totaling over $7.3 million. The checks posted by Hager, Jr. were stolen from Padgett's postal route in West Charlotte. At the time Hager, Jr. committed this fraud, he was on probation with the state of North Carolina for an unrelated offense. (Source)

Former U.S. Postal Worker Charged With Stealing $1.6 Million+ Of Checks From Mail - September 22, 2023

Between October 2021 and March 2023, Hachikosela Muchimba was an employee of the U.S. Postal Service.

Muchimba executed a scheme to steal checks from the U.S. mail and direct those funds into a bank account under his control. Muchimba would remove the name of the proper payee and replace it with his own name. Many of these misappropriated checks were U.S. Treasury checks. He is seen on bank surveillance removing the proceeds from ATM machines. The total amount of the checks that were fraudulently deposited into Muchimba's accounts was $1,697,909.52. Law enforcement executed a search warrant at Muchimba's personal residence on March 29, 2023. In the course of that search, law enforcement recovered an ATM receipt that reflected a deposit of a U.S. Treasury Check in the amount of $415,173.53. (Source)

Former U.S. Postal Employee Pleads Guilty To Stealing $2,400+ Of Money Orders - September 11, 2023

Stephen Perrine admitted that while working for the United States Postal Service (USPS) in Ithaca, New York, he stole ten money orders totaling $2,480, by issuing them to himself and entering fraudulent justifications in an USPS accounting system.

Perrine admitted that he stole and cashed a $400 money order on or about September 13, 2022, and that he documented the money order as having been issued as payment for "local transport."

Perrine admitted that on November 15, 2022, he stole and cashed a $200 money order, which he fraudulently documented as having been issued as payment for "office supplies."

Perrine resigned his position with the USPS after he was charged criminally in this case. As part of his plea agreement, Perrine agreed to pay full restitution of $2,480 to the USPS. (Source)

Former U.S. Postal Service Employee Admits To Stealing Stimulus Checks From The Mail - September 18, 2023

Olivia Bryant admitted in a plea agreement that in 2020 and 2021 she stole hundreds of pieces of mail from her route in Chicago's Logan Square neighborhood.

Some of the stolen mail contained government stimulus checks that were issued by the U.S. Treasury during the Covid-19 pandemic. Bryant admitted that five of the stimulus-check thefts occurred on St. Patrick's Day 2021 when she removed the checks from her postal satchel and transferred them to her purse. (Source)

U.S. State Department Government Contractor Arrested On Espionage Charges To Aid Foreign Government - September 21, 2023

Between Dec. 19, 2022, and Aug. 7, 2023, Abraham Lemma copied classified information from intelligence reports and deleted the classification markings from them. Lemma then removed the information, which was classified as SECRET and TOP SECRET, from secure facilities at the Department of State.

Lemma used an encrypted application to transmit classified national defense information to a foreign government official associated with a foreign country's intelligence service. In these communications, Lemma expressed an interest and willingness to assist the foreign government official by providing information. In one communication, the foreign official stated, "It's time to continue your support." Lemma responded, "Roger that!"

In other chats, the foreign official tasked Lemma to focus on information related to particular subjects, and Lemma responded "absolutely, I have been focusing on that all this week." As alleged in the criminal complaint, the classified national defense information Lemma transferred to the foreign official included satellite imagery and other information regarding military activities in the foreign country and region. (Source)

IRS Consultant Charged With Disclosing Tax Return Information On Nation's Wealthiest Individuals & Disclosing Information To News Organization - September 29, 2023

Charles Littlejohn while working at the IRS as a government contractor, stole tax return information associated with a high-ranking government official (Public Official A) and disclosed it to a news organization (News Organization 1). Littlejohn also stole tax return information for thousands of the nation's wealthiest individuals, and disclosed this tax return information to another news organization (News Organization 2). (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

No Incidents To Report

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

FBI Special Agent Pleads Guilty To Concealing Receiving $225,000 From Foreign Security Officer - September 22, 2023

Charles McGonigal is a former FBI Special Agent in Charge of the New York Field Office.

From August 2017, and continuing through his retirement from the FBI in September 2018, McGonigal concealed from the FBI the nature of his relationship with a former foreign security officer and businessperson who had ongoing business interests in foreign countries and before foreign governments. McGonigal received at least $225,000 in cash from the individual and traveled abroad with the individual and met with foreign nationals. The individual later served as an FBI source in a criminal investigation involving foreign political lobbying over which McGonigal had official supervisory responsibility. (Source)

Former Police Chief Sentenced To Prison For Stealing $25,000+ From Evidence Room - September 15, 2023

Between February 2020 and February 2021, Jason Cross of the Columbia Chief of Police, stole over $25,000 from the Columbia Police Department evidence room and drug purchase fund. (Source)

Former District Of Columbia Fire / EMS Employee Sentenced To Prison For Accepting $42,000+ In Bribes From Contractor - September 29, 2023

Charity Keys was sentenced to prison for engaging in a scheme, with a co-worker, to defraud the District of Columbia Fire and Emergency Medical Services Department (FEMS). Keys accepted more than $42,500 in kickbacks from a contractor in exchange for directing purchase agreements and orders to the contractor and then falsely certifying that goods that FEMS had paid for had been delivered when, in fact, they had not. (Source)

STATE / CITY GOVERNMENTS / MAYORS

Former Social Worker Sentenced To Prison For Role In $973,000 Fraud Scheme By Using Clients' Stolen Identities - September 18, 2023

From August 2010 to June 2019, John Tran and his co-conspirators used the stolen information to fraudulently obtain money from the federal government, the State of California, the County of Orange and financial institutions.

The Orange County Social Services Administration employed Tran from July 1994 until October 2018. Tran abused his position of public trust to steal PII belonging to agency clients as well as other individuals, many of whom were recent immigrants to the United States.

Tran and his co-conspirators used the stolen PII to file false federal and state tax returns in the names of identity theft victims, fraudulently obtaining welfare benefits, underreporting income, and falsely claiming deductions on their personal tax returns, and opening credit cards and other lines of credit in the names of the identity theft victims. Proceeds from the schemes were laundered and structured to avoid detection by law enforcement and banks.

Tran also used the stolen identities of two victims to open fraudulent bank accounts, open credit cards, and open social services cases. For example, in September 2014, Tran opened a credit card account in another person's name and used that card for personal expenses, including for items such as skin care products, Costco purchases, and sports gambling.

Tran in 2007 charged approximately $14,000 to a credit card in the name of one victim after he convinced the victim to allow him to use the victim's credit card. The victim, who was a recent immigrant to the United States and one of Tran's SSA clients, believed that he had to let Tran use the credit card because Tran was a powerful government official who had control over the victim's families' SSA benefits.

In addition to opening at least 12 fraudulent bank and credit card accounts, Tran fraudulently created and managed SSA benefits cases for family, friends, and for himself, obtaining state benefits for which he and others were not entitled.

In total, along with the $973,153 in fraudulently obtained tax refunds, Tran defrauded two victims out of approximately $44,604, and defrauded the Orange County Social Services Administration out of approximately $92,531. (Source)

Former Chairperson For Michigan Medical Marijuana Licensing Board Sentenced To Prison For Accepting 110,000+ In Bribes - September 28, 2023

Rick Johnson was a member and the Chairperson of the Michigan Medical Marijuana Licensing Board (MMLB) between May 2017 and April 2019. Prior to his appointment to that Board, Johnson worked as a lobbyist in Lansing, Michigan, and served as Speaker of the Michigan House of Representatives between 2001 and 2004.

Johnson received at least $110,200 in bribes while he was MMLB Chair, including cash payments, flights to Canada on private aircraft, and commercial sex paid for by others. Co-defendant John Dalaly paid Johnson $68,200 in bribes. Co-defendants Brian Pierce and Vincent Brown paid Johnson $42,000 in bribes.

Johnson took several steps to conceal the bribes, such as using a second burner phone and laundering bribes through various limited liability companies he controlled to hide their purpose.

In return for the bribe payments, Johnson provided an unfair advantage to bribe payers in the form of his favorable vote on license applications, his help and support throughout the licensing process, and confidential inside information pertaining to the MMLB's work and other applicants. (Source)

Former Montana Department Of Public Health & Human Services Employee Admits To Stealing $89,000+ From Federal Aid Programs - September 21, 2023

Heather Bugni was employed by the Montana Department of Public Health and Human Services as a Client Services Coordinator from October 2015 to July 2021. Bugni processed applications, conducted interviews and approved benefits for multiple public assistance programs, including the federal programs Medicaid, which is medical assistance for low-income persons, and the Supplemental Nutrition Assistance Program (SNAP), which is a nutrition assistance program for low-income individuals and families.

Bugni approved applications, entered false information and incorrect wage information that resulted in her boyfriend's mother receiving $13,869 in Medicaid benefits and $848 in SNAP benefits and her boyfriend's father receiving $63,303 in Medicaid benefits. Bugni also applied for SNAP benefits on behalf of her daughter and filled out the application posing as her boyfriend. Bugni intentionally provided an incorrect address for them and later called DPHHS, posing as the boyfriend's mother, and verified the incorrect address.

Bugni knew that if she had provided the correct address, her own income would have made her daughter and boyfriend ineligible for SNAP benefits. Bugni received $11,309 in SNAP benefits from this conduct. (Source)
https://www.justice.gov/usao-mt/pr/former-montana-department-public-health-and-human-services-employee-admits-stealing

3 City Council Members Sentenced To Prison For Accepting Bribe Payment In Exchange For Votes - September 6, 2023

3 former Toledo City, Ohio Council members were sentenced to prison for their roles in accepting bribery payments during their time in office in return for support and votes on legislative matters. (Tyrone Riley, Yvonne Harper, Larry Sykes)

On multiple occasions from May 2018 through February 2020, Riley, Harper, and Sykes accepted bribery payments in return for their official support and votes on legislative matters as members of the Toledo City Council.

Court documents also state that Riley, Harper, and Sykes each accepted cash payments in return for their support and votes on zoning changes and "special use permits" (SUPs) for local businesses. Riley accepted more than $10,000 in payments and meals in return for his support on five separate city council matters. Harper accepted more than $5,000 in return for her support on two matters, and Sykes accepted $1,500 for his support on three matters. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

School Police Officer Facing Federal Charges For $215,00+ Overtime Fraud Scheme - September 8, 2023

Lawrence Smith began working as a Baltimore City School Police Officer in 2005 and in 2016 was promoted to detective and put in charge of the School Police Overtime Unit. In this role, Smith managed the Overtime Unit and was responsible for the coordination and scheduling of School Police Officer overtime, including his own.

During the COVID-19 pandemic, Smith was authorized to receive overtime pay to provide security for COVID testing sites and food sites set up at various Baltimore City Public School System schools and at Baltimore City Recreation and Parks community centers, as well as the COVID-19 hospital and homeless shelter.

From January 2019 through August 2022, Smith fraudulently received overtime pay for hours for which he had not worked. The indictment alleges that Smith used his position as the Detective in charge of the Overtime Unit for School Police to assign himself to overtime shifts.

Smith allegedly falsely claimed that he was working overtime as a School Police Officer for overtime shifts that required his physical presence when he was at home, running personal errands, at other locations socializing, coaching football, and out of state on vacation. The indictment seeks a money judgment of $215,352, alleged to be the proceeds of the fraud scheme. (Source)

Former Head Of Mission School Pleads Guilty To Misusing Nearly $40,000 in School Funds / Used Funds To Pay For Vacations For Herself / Friends - September 6, 2023

Naia Wilson is the former Head of School for New Mission School in Hyde Park, Massachusetts. Wilson was employed as Head of School for New Mission School from 2006 until about June of 2019.

She pleaded guilty to engaging in a scheme to defraud Boston Public Schools of approximately $38,806 by misusing school funds for her own personal use.

Beginning in September 2016 and continuing until May of 2019, Wilson requested checks from the external fiscal agent school account to be issued in the name of other individuals, fraudulently endorsed those checks to herself and then deposited them into her own bank account without the nominee ever knowing or authorizing her to do so.

Additionally, Wilson requested checks from the external fiscal agent that were used to pay for two all-inclusive personal vacations to Barbados for herself and her friends in 2016 and 2018. For both the 2016 and 2018 Barbados trips, Wilson requested that the external fiscal agent issue checks payable to other people who went on the trips and then converted that money to pay for the all-inclusive hotel and airfare. Wilson also fraudulently endorsed the checks used to pay for the 2018 trip. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

Bookkeeper Sentenced To Prison For Embezzling $300,000+ From Labor Union - September 27, 2023

Denise Kovacs was the Bookkeeper at Plumbers AFL-CIO Local 803, a labor union that represents plumbers and pipefitters in central Florida.

During a nearly five-year period of employment, Kovacs stole $43,777 in cash from union dues and charged $261,126 in expenses on the union's credit card. To conceal her theft, Kovacs altered internal business records which kept union officials in the dark about her ongoing embezzlement of funds. Kovacs was also ordered to pay $304,903.27 in restitution. (Source)

Former Union President Sentenced To Prison For Embezzling $36,000 / Used Funds For Shopping, Travel, Dining, Etc. - September 27, 2023

Felix Luciano, former President of Local 2805 chapter of the American Federation of Government Employees and former Department of Homeland Security Officer, was sentenced in federal court today to four months in custody for filing a false report to conceal his embezzlement of thousands of dollars in union dues

According to court records, from January of 2016 to December of 2018, Luciano used some of Local 2805's money for a variety of personal expenses, including shopping, travel reimbursements, groceries, dining, dry cleaning, and paying for non-union accounts.

He did this by writing checks from Local 2805's checking account and using Local 2805's debit and credit cards to directly pay personal expenses. As a result of Luciano's actions, he caused a total loss of $36,000 to Local 2805. (Source)

BANKING / FINANCIAL INSTITUTIONS

Former Bank President Sentenced To Prison For Role In $1 BILLION Fraud Scheme, Resulting In 500 Lost Jobs & Causing Bank To Cease Operations - September 6, 2023

Ashton Ryan was the President, CEO, and Chairman of the Board at First NBC Bank.

According to court documents and evidence presented at trial, Ryan and others conspired to defraud the Bank through a variety of schemes, including by disguising the true financial status of certain borrowers and their troubled loans, and concealing the true financial condition of the Bank from the Bank's Board, external auditors, and federal examiners.

As Ryan's fraud grew, it included several other bank employees and businesspeople. Several of the borrowers who conspired with Ryan, used the banks money to pay Ryani ndividually or fund Ryan's own businesses. Using bank money this way helped Ryanconceal his use of such money for his own benefit.

When the Bank's Board, external auditors, and FDIC examiners asked about loans to these borrowers, Ryan and his fellow fraudsters lied about the borrowers and their loans, hiding the truth about the deadbeat borrowers' inability to pay their debts without receiving new loans. As a result, the balance on the borrowers' fraudulent loans continued to grow, resulting, ultimately, in the failure of the Bank in April 2017. This failure caused approximately $1 billion in loss to the FDIC and the loss of approximately 500 jobs.

Ryan was ordered to pay restitution totaling over $214 Million to the FDIC. (Source)

Capital One Financial Corporation Data Analyst Pleads Guilty To $3 Million+ Insider Trading Scheme - September 28, 2023

Nan Huang conspired with his a co-worker to commit insider trading. From 2008 to 2015, Huang worked as a senior data analyst for a subsidiary of Capital One Financial Corporation. As a senior data analyst, Huang had access to a Capital One database that collected transaction data from Capital One credit card and debit card customers.

In violation of his fiduciary duties to Capital One, Huang searched this database thousands of times and compiled on his work computer material, nonpublic information about publicly traded companies. Because this information was highly correlated with the not-yet-public actual revenue of these companies, Huang was able to predict whether these companies would meet their revenue expectations.

Huang then executed hundreds of trades using this non-public information and reaped extraordinary profits. Huang personally made over $1.4 million in profits and the conspiracy made over $3.1 million.

Capital One fired Huang in 2015 after it discovered his activity. Days later, Huang fled the country to China where he remained until his arrest at San Francisco International Airport earlier this year. (Source)

Former Bank Branch Manager Sentenced To Prison For Stealing $120,000+ From Customer Accounts - September 29, 2023

From June 2020 through November 2021, Nathan Wadsworth was employed as a Branch Manager for PNC Bank in Boston.

Beginning in or around March 2021, Wadsworth used his position to identify dormant accounts of foreign account holders, transferred the funds in those dormant accounts to a new account he opened in the customers' names and then moved the funds to his own accounts for personal use. In total, Wadsworth stole approximately $121,000 in customer funds. All the funds have since been repaid by PNC to the affected customers. (Source)

Former Credit Union Employee Charged For Stealing $40,000+ - September 12, 2023

From June 2021 through September 2022, Heidi Metz, Metz stole more than $40,000 from Cal-Ed Federal Credit Union. (Source)

Former Manager Of Credit Union Charged For Embezzling Money From Credit Union For 10 Years - September 11, 2023

Rita Hartman was the Manager of Muddy River Credit Union from the early 1990s through January 2021. Muddy River served the employees of the Bradken foundry located in Atchison, Kansas. In 2013, the Governor of the State of Kansas appointed Hartman to the Kansas Credit Union Council, which advises the Kansas Department of Credit Unions on issues and needs of credit unions.

As Manager, Hartman had responsibility for and control over all aspects of Muddy River's finances and books and records.

From at least 2010 through December 2020, Hartman is accused of using her position to steal money from Muddy River. Hartman allegedly did so by crediting fraudulent deposits and loan payments to her or her relatives' accounts or by stealing cash deposits, then concealing her conduct by altering Muddy River's books and records, and falsifying information submitted to Muddy River's regulators. (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

Hospice Medical Director Sentenced To Prison For Role In $150 Million Fraud Scheme - September 27, 2023

From 2009 to 2018, Jesus Virlar-Cadena served as the Medical Director of the Merida Group, a large health care company that operated dozens of locations throughout Texas. He was a physician but the Texas Medical Board later suspended his medical license.

A federal jury convicted co-conspirators Rodney Mesquias, Henry McInnis and Francisco Pena in October 2019.

Evidence at the trial showed that the Merida Group marketed their hospice programs through a group of companies. They enrolled patients with long-term incurable diseases such as Alzheimers and dementia as well as patients with limited mental capacity who lived at group homes, nursing homes and in housing projects. In some instances, Merida Group marketers falsely told patients they had less than six months to live. They also sent chaplains to the patients based on the false pretense they were near death.

In order to bill Medicare for these services, the Merida Group hired Virlar and other medical directors but made payment of their medical director fees contingent upon an agreement to certify unqualified patients for hospice. In addition to regular medical director payments,

Virlar received luxury trips, bottle service at exclusive nightclubs and other perks in exchange for his certification of unnecessary hospice patients. In exchange for these illegal kickbacks, Virlar himself certified over $18 million in unnecessary hospice services as part of the over $150 million conspiracy. (Source)

Manager For Radiologist Staffing And Recruiting Company Pleads Guilty To Stealing $100,000+ - September 7, 2023

Scott Dulac worked as the Manager of Confluence Medical, a radiologist staffing and recruiting company. He had access to and signatory authority on the company's bank accounts in order to manage payroll, pay company bills, and arrange for payments to contracted radiologists.

On numerous occasions, between early 2019 and early 2020, Dulac made unauthorized fund transfers and cash withdrawals for his own personal benefit in excess of $100,000. (Source)

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

Former CEO Of International Investment Advisory Firm Pleads Guilty To Role In $155+ Million Investment Fraud Scheme - September 12, 2023

Roberto Gustavo Cortes Ripalda (Cortes) pleaded guilty to participating in a years' long conspiracy to defraud clients of Biscayne Capital, an international investment advisory firm that operated in the United States, South America, and the Caribbean. Today's plea took place before United States District Judge Carol Bagley Amon. When sentenced, Cortes faces up to 20 years in prison and as part of his plea agreement will pay forfeiture in the amount of $3.4 million.

Between approximately 2013 and 2018, Cortes, together with others at Biscayne Capital, orchestrated a scheme to defraud Biscayne Capital clients through a series of material misrepresentations and omissions about how Biscayne Capital client funds would be used, including falsely claiming that their funds would be used to develop luxury real estate in Florida. As part of the scheme, Cortes and his co-conspirators used client money to pay promised investment returns to other Biscayne Capital clients.

According to the indictment, by September 2018, the scheme collapsed and Biscayne Capital went into liquidation, causing more than $155 million in losses to Biscayne Capital clients.

Co-conspirators Ernesto Heraclito Weisson Pazmino pleaded guilty to conspiracy to commit wire fraud in April 2022; Gustavo Trujillo pleaded guilty to conspiracy to commit wire fraud and conspiracy to commit money laundering in April 2019; Juan Carlos Cortes pleaded guilty to conspiracy to commit wire fraud and conspiracy to commit money laundering in July 2022; Fernando Martinez Gomez pleaded guilty to conspiracy to commit wire fraud and conspiracy to commit money laundering in March 2022. (Source)

Computer System Administrator & Spouse Plead Guilty To $88 Million Fraud Scheme To Sell Pirated Business Telephone System Software Licenses - September 19. 2023

Brad Pearce and Dusti O. Pearce conspired with Jason Hines, Chad Johnson, and Justin Albaum to commit wire fraud in a scheme that involved generating and then selling unauthorized Avaya Direct International (ADI) software licenses. The ADI software licenses were then used to unlock features of a popular telephone system used by thousands of companies around the globe. The ADI software licensing system has since been decommissioned.

Brad Pearce, a long-time customer service employee at Avaya, used his system administrator privileges to generate tens of thousands of ADI software license keys that he sold to Hines and other customers, who in turn sold them to resellers and end users around the globe. The retail value of each Avaya software license ranged from under $100 to thousands of dollars.

Dusti Pearce handled accounting for the illegal business. Hines was by far the Pearces' largest customer, buying over 55% of the stolen licenses, and significantly influenced how the scheme operated. Hines operated Direct Business Services International (DBSI), a de-authorized Avaya reseller, in New Jersey.

Brad Pearce also employed his system administrator privileges to hijack the accounts of former Avaya employees to generate additional ADI software license keys. Furthermore, he used these privileges to alter information about the accounts to conceal the fact that he was generating ADI license keys, preventing Avaya from discovering the fraud scheme for many years. (Source)

Chief Operating Officer Sentenced To Prison For Role In Conspiring To Steal $1.8 Million+ From Business For Personal Use - September 8, 2023

Stephen Franklin was the Chief Operating Officer of Accurate Optical, a chain of optometric shops on the Eastern Shore of Maryland, and with the owners of Accurate Optical he also purchased East Coast Optometric, a chain of South Carolina optical shops. Franklin and co-defendant Duane G. Larmore met through the Salisbury Chamber of Commerce and became friendly.

Larmore was an employee at Shore Appliance Connection (Shore Appliance), located in Salisbury, Maryland, whose duties included maintaining the books and records for the company. The company was owned and operated by Owner #1 and Owner #2. From mid-September 2016 through about March 2020, Franklin conspired with others, including Larmore, to steal more than $1.8 Million from Shore Appliance.

Franklin and Larmore stole over $1 million from Shore Appliance to use for their own purposes, including to make investments and to pay business expenses for Franklin's businesses, without the knowledge and consent of the owners of Shore Appliance. Franklin convinced Larmore to invest $100,000 in an oil deal that promised quick and substantial returns. Those funds were ultimately returned to Shore Appliance because the name on the bank account did not match the named beneficiary on the wire transfer form completed by Franklin.

Prior to the funds being returned and at Franklin's urging, Larmore transferred another $100,000 to a purported attorney for the oil deal. Franklin also convinced Larmore to invest in other deals, including: in 2016, a $95,000 initial investment with a finance company in London, U.K., followed by another $300,000, plus funds for expenses and travel abroad; in 2018, an investment through W.S. of $35,000 and an investment through Gateway Capital of $50,000; and in 2019 - 2020, investments and expenses through I.P. and E. P.-S. to recover assets purportedly in the custody of U.S. Customs, part of the Department of Homeland Security. No investment paid any return to the schemers. (Source)

Former CEO And Former CFO Of Telecommunications Company Charged In Connection With $40 Million+ Accounting Fraud Scheme - September 28, 2023

Victor Bozzo, the former CEO of Pareteum, and Edward O'Donnell, the former CFO, and their co-conspirators allegedly schemed to inflate the company's revenue, thereby making the company appear more profitable than it was and allowing Bozzo and O'Donnell to obtain performance bonuses they had not earned. To conceal their alleged fraud, Bozzo and O'Donnell then took steps to mislead the independent certified public accountants engaged to audit Pareteum's financial statements.

As a result of this fraudulent revenue recognition practice, from at least in or about 2018 through the first half of 2019, Pareteum improperly recognized and reported to the investing public more than $40 million of revenue that it should not have. (Source)

Former Secretary Sentenced To Prison For $1.2 Million+ Of Wire Fraud - September 11, 2023

While working as a secretary for Bridges Equipment, LTD, Tamara Allen fraudulently cashed her employer's checks using the owner's signature stamp and made electronic payments to her personal bank accounts from company accounts. The scheme amounted to a total loss of at least $868,770.60. Additionally, Allen underreported her income on her taxes over a four-year span, for a total amount of $553,390.00. (Source)

Former Accounting Manager Pleads Guilty To Insider Trading that Led To Nearly $500,000 in Profits - September 27, 2023

A former employee (Marco Antonio Perez) at a publicly traded company has agreed to plead guilty to buying more than 66,000 company shares based on non-public information that the company was about to be acquired at a higher per-share price, and then selling the shares after news of the acquisition became public, resulting in nearly $500,000 in ill-gotten gains.

General Finance Corp., a storage and modular space company, employed Perez as an accounting manager who reported to the company's Chief Financial Officer. He also performed assignments for the company's chairman, including printing out the chairman's emails. As a result, Perez had access to material information belonging to General Finance, including offers to buy the company, before the information was released to the investing public. (Source)

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

Former Finance Director At 2 Non-Profit Organizations Sentenced To Prison For Embezzling $3 Million+ Over 11 Years / Used Funds To Pay For Credit Cars Bills, Gambling, Vacations, Etc. - September 5, 2023

In 1999 Susana Tantico began working for a non-profit that provides healthcare to underserved populations. Ultimately, Tantico became the non-profit's Finance Director.

Between 2011 and June 2020, Tantico secretly embezzled millions of dollars from the healthcare organization. Bank records are available only for the period beginning in December 2016. Between December 2016 and 2020, Tantico stole nearly $2.3 million from the healthcare non-profit.

She used the non-profit's debit and credit cards to withdraw $1.6 million at casinos for gambling. She also used the debit and credit cards to pay for personal vacations, such as a $26,000 family trip to Florida, and trips to Las Vegas and San Diego. Tantico also used the healthcare non-profit's debit and credit cards for more than $83,000 worth of purchases at Nordstrom, and $40,000 worth of purchases at Apple stores.

After running up these expenses, Tantico used the non-profit's funds to pay the credit card bills and disguised the payments as legitimate expenses. For example, she categorized expenses for one vacation as "pharmacy supplies" in the accounting system.

In 2020, Tantico went to work as Finance Director for a different non-profit, one with a focus on criminal justice issues. Tantico used more than $485,000 of the non-profit's funds for gambling at casinos.

She transferred $21,000 from the non-profit to her mortgage servicer to pay her home mortgage. She also transferred money to her personal bank account. Tantico then altered the bank records to hide the embezzlement.

At one point, Tantico was questioned by one of the organization's banks about the pattern of withdrawals at casinos.

She claimed that the non-profit held youth programs at the casinos, and that the withdrawals were for cash prize giveaways. In all, Tantico stole nearly $893,000 from the non-profit. The non-profit has incurred $132,000 in costs to forensically audit its books, fix its accounting procedures and records, and reply to vendors. (Source)

Company Accountant Charged With Embezzling $1.1+ Million From Employer / Used Funds For Mortgage, Car, Vacation, Etc. - September 21, 2023

From January 2019 to June 2022, Mandy Urban was employed as a Senior Staff Accountant for a company. Urban was responsible for maintaining the company's general ledger, preparing financial statements, and reconciling the company's accounts payable and receivable and bank statements.

Urban executed a scheme to defraud her employer by misusing her access to make multiple transfers from the company's bank accounts to accounts under Urban's control. Urban also allegedly falsified the company's books and records to conceal the scheme. Urban made more than 245 fraudulent transfers from the accounts of the company totaling $1,115,344.73.

Urban used the embezzled funds to pay for personal expenses, including tens of thousands of dollars for mortgage, car, education, and vacation expenses, and to buy cryptocurrency. It is alleged that Urban transferred significant amounts of embezzled funds to family members. (Source)

Former Finance Director For Non-Profit Trade Association Sentenced To Prison For $490,000 Embezzlement Scheme For Personal Use - September 12, 2023

From about December 2017 until her sudden resignation in August 2022, Donna Murray was employed as the Director of Finance for a non-profit financial services trade association located in Manhattan. The organization, which has more than 600 institutional members, works to promote industry thought leadership, participate in industry advocacy work, educate members and stakeholders, and establish industry standards and best practices.

As the director of finance, Murray was the sole finance department employee and was responsible for maintaining the organization's books, updating its general ledger, handling accounts receivable and payable, and providing the organization's financial statements to outside auditors. Out of the organization's 14-16 employees during the relevant period, Murray was also the only employee with access to the organization's online banking accounts and the only employee with the ability to make wire transfers for the organization.

From at least October 2019 through at least in or about March 2021, Murray embezzled $488,177.24 from one of the organization's bank accounts through 105 unauthorized wire transactions from the organization's bank account to her personal bank account in amounts that increased over time.

To conceal her fraud from her employer and its outside auditor, Murray leveraged her knowledge of the outside auditor's practices and the organization's vendors and vendor invoicing schemes to generate false, but plausible-sounding, entries in the general ledger. Murray also transferred money from her employer's bank account to her bank account in amounts less than $10,000, which would have triggered bank reporting requirements. Murray altered a bank statement submitted to the organization's deputy general counsel to falsely reflect that a wire transfer had gone to an employer-funded health plan instead of Muray.

After misappropriating hundreds of thousands of dollars from her employer's bank account to her own, Murray withdrew from her bank account over $400,000 in cash on more than 347 occasions — sometimes multiple times a day and used the remainder of the stolen funds for peer-to-peer online money transfers, personal loan payments, and consumer and luxury items, including Yves Saint Laurent and Michael Kors designer apparel; beauty, wellness, and skincare products and services; home furnishings and décor; online streaming and satellite radio purchases; over 180 Amazon orders; smoke shop purchases; and a $200 treadmill for cats. (Source)

Former Railroad Employee Sentenced To Prison For Fraudulently Obtaining $279,000+ In Disability Benefits - September 22, 2023

Scott Carlberh operated and managed a tanning salon in Wisconsin for 6 years, while simultaneously receiving occupational disability benefits from the U.S. Railroad Retirement Board. In his application for benefits, Carlberg asserted that he could no longer perform any type of work due to numerous daily limitations, including short-term-memory loss, poor concentration, irritability, frequent loss of temper, and information-processing difficulties. After the benefits were approved, Carlberg misrepresented the nature of his work at the salon and lied about the income he received from it.

The judge ordered Carlberg to immediately pay more than $279,000 in restitution to the Railroad Retirement Board. (Source)

Former Accounting Controller For Construction Company Charged For Stealing $260,000+ For Personal Use / Others - September 11, 2023

Between December 2019 and September 2021, Amy Hall was the Accounting Controller for a local design and construction company. She stole more than $260,000 from her employer. She used access to the company's credit card and bank account granted to her by virtue of her position as accountant to devise and execute a scheme to steal the company's funds for her own use and benefit and for the use and benefit of others. (Source)

Former Airline Gate Agent Sentenced To Prison For Cheating Airline Ticketing System For Friends & Family - September 28, 2023

As a gate agent, Tiffany Jenkins had access to the airline's computer reservation database and had the ability to use a special code, referred to as an involuntary exchange or INVOL, to change flights for customers at no additional cost. This code enables agents to change flights for customers who miss their flights or experience a death in the family.

During a 15-month period, from approximately July 1, 2016, through Sept. 27, 2017, Jenkins executed approximately 505 involuntary ticket exchanges for more than 100 different passengers. Many of those exchanges occurred after the passenger was first booked on domestic flights at one of the airline company's lowest available fares—often, roundtrip flights between Las Vegas, Nev., and Long Beach, Calif. A short time later, Jenkins exchanged those tickets for a completely different city pair, generally involving much more expensive international locations, for friends, family and acquaintances. (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

Former Executive & 3 Employees Charged With Defrauding Company Of $3 Million+ - September 22, 2023

Former employees of Mohawk Industries, Inc. Jana Kanyadan, Sivakumar Thiyagasamadram, Madhu Shivalingegowda, and Chintan Sandesara have been indicted for allegedly defrauding Mohawk.

Jana Kanyadan served as Mohawk's Global Chief Information Officer. Sivakumar Thiyagasamadram, Madhu Shivalingegowda, and Chintan Sandesara were Mohawk employees with responsibility for Information Technology (IT).

In 2019, Mohawk launched a large, multi-year IT project and outsourced work for the IT project to IT consulting firms.

The indictment alleges that the defendants secretly organized and controlled a Georgia company, Meta Technology Platforms, LLC (Meta Tech), and used their positions at Mohawk to retain Meta Tech as a Mohawk vendor and divert Mohawk's outsourced IT consulting work to Meta Tech.

Between approximately May and October of 2022, Meta Tech submitted invoices to Mohawk totaling approximately $3,034,411. The invoices that Meta Tech submitted to Mohawk did not disclose the defendants' relationship to Meta Tech. The invoices also allegedly charged Mohawk for services that had not been performed, for software that had not been provided, and at inflated hourly rates that Kanyadan approved on Mohawk's behalf. Mohawk paid Meta Tech approximately $1,857,741.40 based on these fraudulent invoices. (Source)

Former Employee Pleads Guilty To Embezzling $1.7 Million Over 8 Years By Creating Fake Invoices - September 19. 2023

Gina Lone star was a Director in the Facilities Department of Men's Wearhouse. She was promoted to Senior Director of Facilities and Corporate Services and then to Vice President of Construction, Maintenance, and Facilities.

Gina Lonestar admitted that, in December 2010, she devised a scheme to create a fake vendor to defraud Men's Wearhouse and later Tailored Brands (Men's Wearhouse's parent company) of money by submitting and approving false invoices for the fake vendor to the accounts payable department.

Lonestar created a document stating the vendor was a sole proprietorship associated with a family member and then began submitting and approving invoices falsely claiming the vendor was performing work at Men's Wearhouse stores throughout California, such as inspections and handyman work. Lonestar admitted that she submitted and approved false invoices in the name of the fake vendor for approximately eight years, defrauding her employer of over $1.7 Million, which was paid to her joint checking account. Lonestar admitted that the vendor did not exist and the family member with whom she co-owed the company performed none of the work for which she provided invoices.

In all of her roles, she had the authority to approve invoices for work done by vendors. Lonestar's scheme ended in 2019 when the company discovered the conduct during an internal audit. (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

Former Chief Operating Officer For Pain Clinics Charged For Role In Health Care Fraud And Illegal Drug Distribution Scheme - September 29, 2023

Jen Adams served as the Chief Operating Officer (COO) and Practice Manager for several pain clinics throughout Central and Southwest Virginia.

The clinics represented themselves as largely focused on pain management, which involved the prescribing of Schedule II opioids, as well as opioid addiction treatment, which involved prescribing Suboxone and other drugs.

The indictment alleges that Adams permitted medical providers who lacked DEA registration numbers to use the registration numbers of others. She did so by instructing employees to continue to use the registration numbers of doctors who were not present and by assisting in making payments to doctors who were not present for the use of their registration numbers.

Adams was aware when clinic employees knowingly wrote prescriptions for Schedule II and Schedule III controlled substances to patients who exhibited warning signs of drug abuse, drug addiction, and drug diversion.

In addition, Adams allowed employees who lacked medical training, experience, and licensing to provide medical treatment and to make and influence medical decisions. (Source)

OTHER FORMS OF INSIDER THREATS

No Incidents To Report

MASS LAYOFF OF EMPLOYEES' AND RESULTING INCIDENTS

No Incidents To Report

EMPLOYEES' MALICIOUS ACTIONS CAUSING COMPANY TO CEASE OPERATIONS

No Incidents To Report

WORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES'

O'Reilly Auto Parts Employee Charged With Murder After Fight Ends In Death Of Shoplifter - September 26, 2023

A store worker in Kansas was charged with second-degree murder after a suspected shoplifter died following a fight, authorities said.

Carl Kemppainen was arrested in connection with the death of Diamond Steen outside O'Reilly Auto Parts in Kansas City last week, the Wyandotte County District Attorney's Office said.

"Based off the autopsy, it is clear that strangulation was the cause of death," District Attorney Mark Dupree told reporters during a news conference. "The deceased's airway was completely stopped and that ultimately caused his death."

Steen and another male suspect had entered the store and allegedly began to shoplift, police said. A fight then broke out between the men and store employees that spilled outside the store, which resulted in Steen's death. The other suspect was treated for minor injuries.(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 Sentenced To Prison For Role In $1 BILLION Fraud Scheme, Resulting In 500 Lost Jobs & Causing Bank To Cease Operations - September 6, 2023

Ashton Ryan was the President, CEO, and Chairman of the Board at First NBC Bank.

According to court documents and evidence presented at trial, Ryan and others conspired to defraud the Bank through a variety of schemes, including by disguising the true financial status of certain borrowers and their troubled loans, and concealing the true financial condition of the Bank from the Bank's Board, external auditors, and federal examiners. As Ryan's fraud grew, it included several other bank employees and businesspeople. Several of the borrowers who conspired with Ryan, used the banks money to pay Ryani ndividually or fund Ryan's own businesses. Using bank money this way helped Ryanconceal his use of such money for his own benefit.

When the Bank's Board, external auditors, and FDIC examiners asked about loans to these borrowers, Ryan and his fellow fraudsters lied about the borrowers and their loans, hiding the truth about the deadbeat borrowers' inability to pay their debts without receiving new loans.

As a result, the balance on the borrowers' fraudulent loans continued to grow, resulting, ultimately, in the failure of the Bank in April 2017. This failure caused approximately $1 billion in loss to the FDIC and the loss of approximately 500 jobs.

Ryan was ordered to pay restitution totaling over $214 Million to the FDIC. (Source)

Bank Director Convicted For $1.4 Million Of Bank Fraud Causing Bank To Collapse - July 12, 2023

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 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

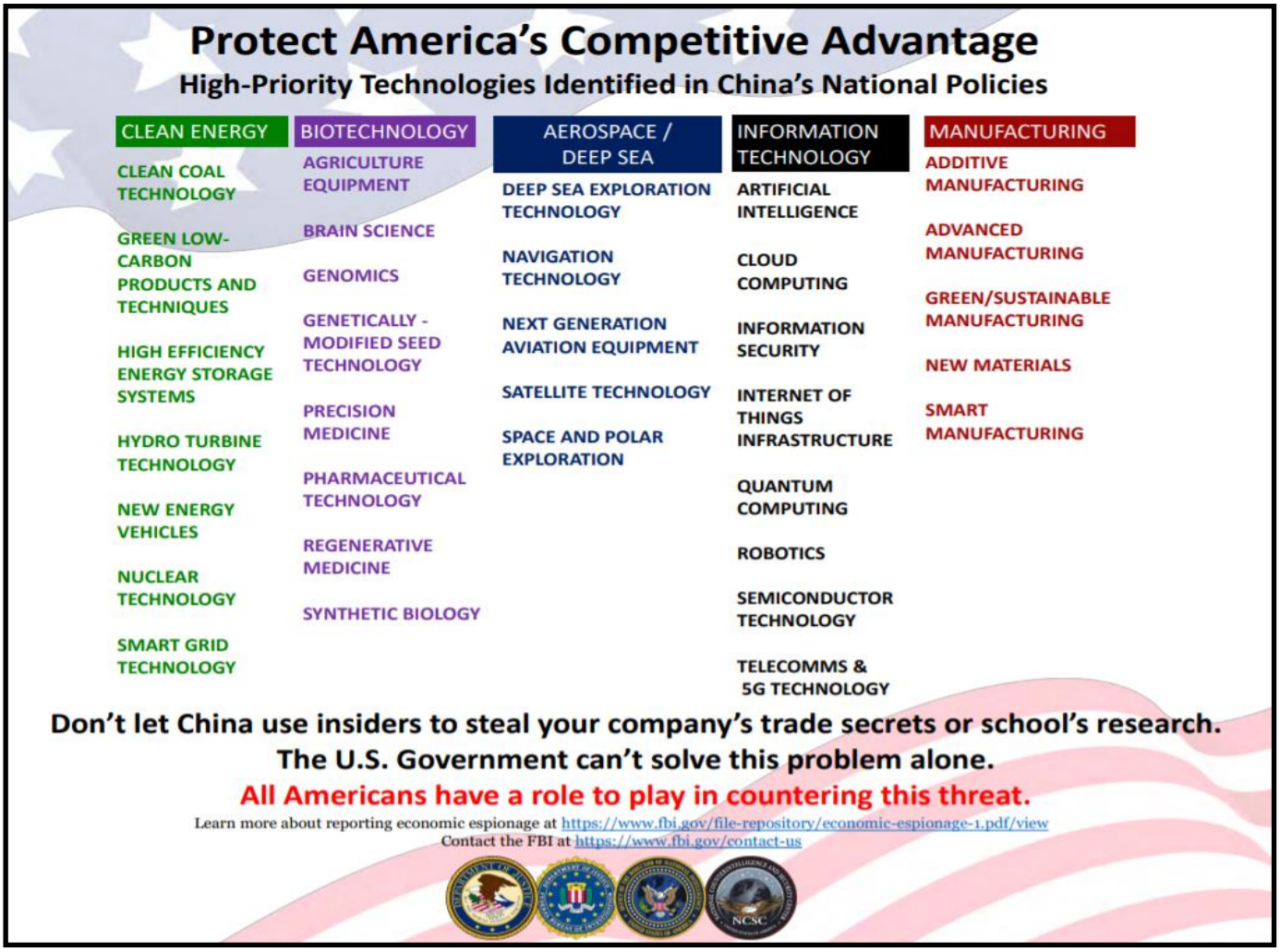
https://www.workplaceviolence911.com/node/994

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 (**4,700+ 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.insiderthreatdefensegroup.com / jimhenderson@insiderthreatdefensegroup.com
www.nationalinsiderthreatsig.org / jimhenderson@nationalinsiderthreatsig.org