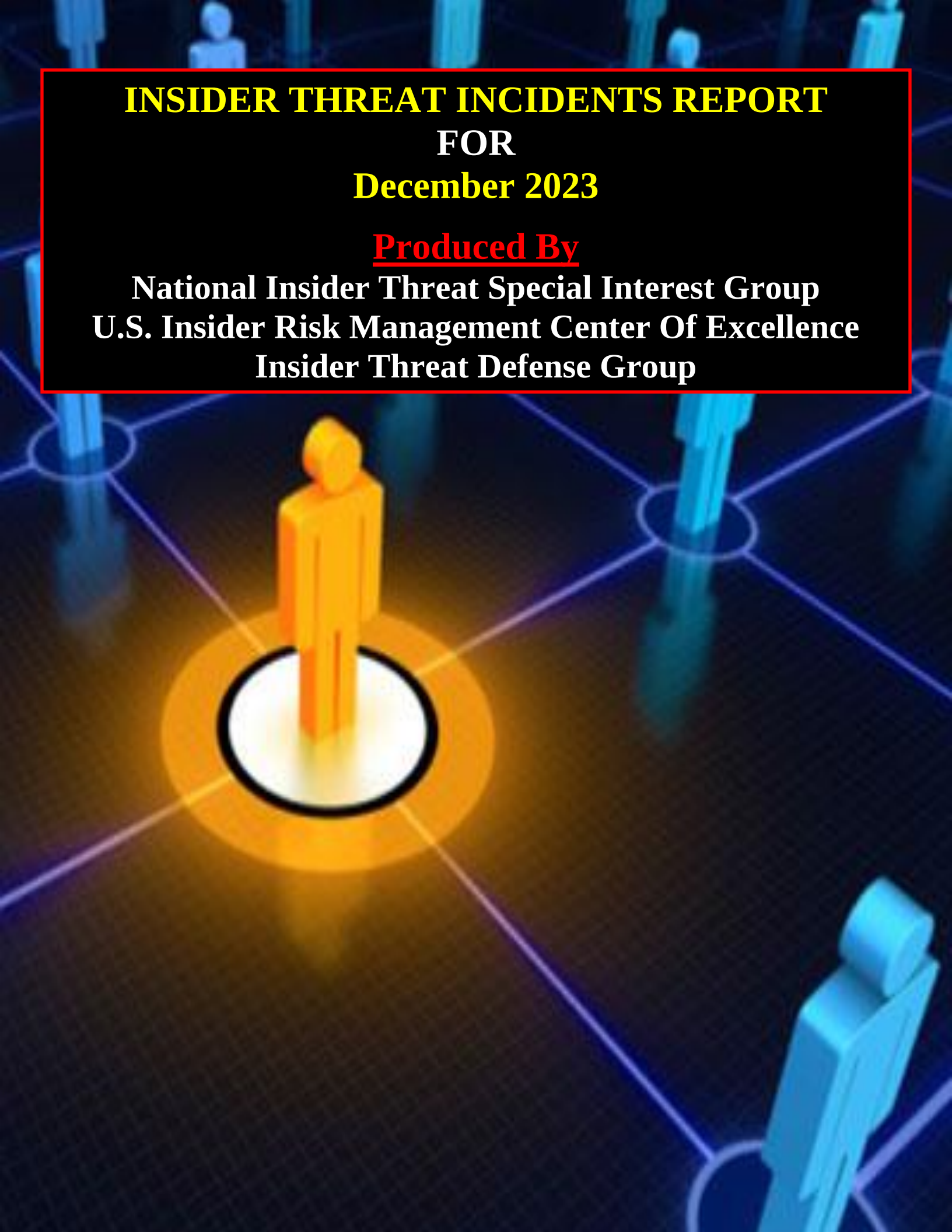
INSIDER THREAT INCIDENTS REPORT
FOR
December 2023

Produced By

National Insider Threat Special Interest Group
U.S. Insider Risk Management Center Of Excellence
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 are negligent, malicious or opportunists. 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 **5,000+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations of all sizes.

The NITSIG and ITDG maintain the largest public repositories of Insider Threat incidents. This monthly report provides clear and indisputable evidence of how very costly and damaging Insider Threat incidents can be to organizations of all types and sizes.

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 these monthly reports, you might have a different perspective on Insider Threats.

The Human Operating System (Brain) is very sophisticated and underestimating the motivations and capabilities of a malicious or opportunist employee can have severe impacts for organizations.

Taking a **PROACTIVE** rather than **REACTIVE** approach is critical to protecting an organization from employee risks / threats, especially when the damages from employees' can be into the **MILLIONS** and **BILLIONS**, as this report shows.

These monthly reports are recognized and used by Insider Risk Program Managers working for major corporations, as a **TRUSTED SOURCE** for education to gain support from CEO's, C-Suite, Key Stakeholders and Supervisors for detecting and mitigating Insider Threats. The incident listed on pages **7 to 20** of this report provide the justification, return on investment and funding needed for developing, managing or optimizing an Insider Risk Management Program.

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.

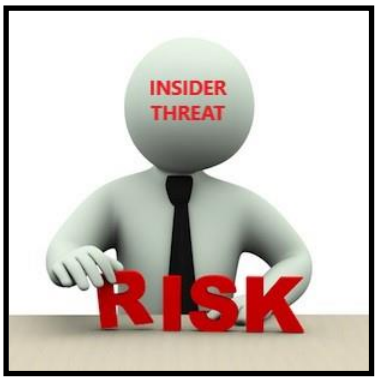
TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH

- ☐ 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

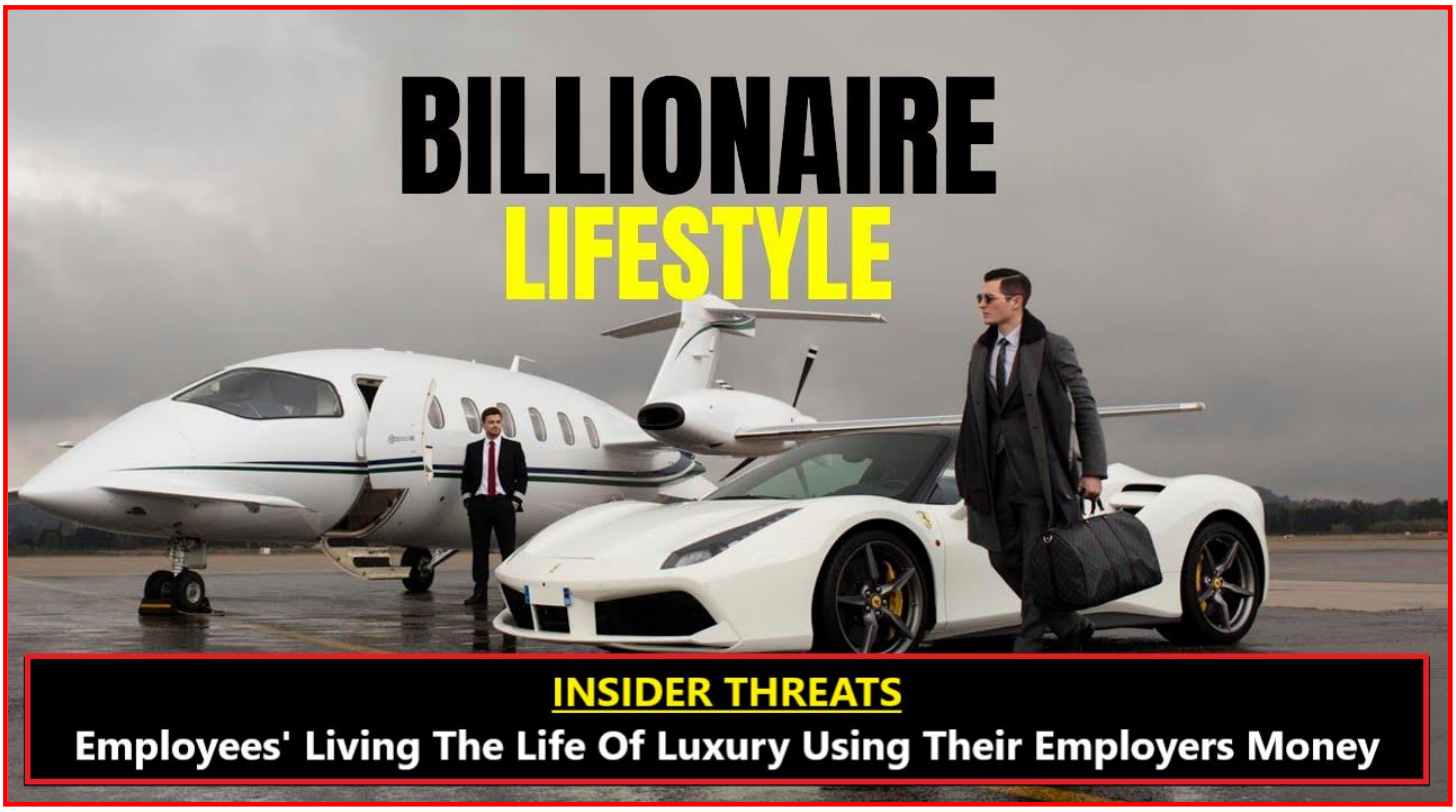
- ☐ Public Relations Expenditures
- ☐ Customer Relationship Loss
- ☐ Devaluation Of Trade Names
- ☐ Loss As A Leader In The Marketplace

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 DECEMBER 2023

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

870+ Australian Federal Public Servants Acted Corruptly For Over 6 Years, Investigation Finds - December 5, 2023

More than 870 federal public servants were found to have acted corruptly over a six-year period, according to internal investigations, with another 162 acting dishonestly or without integrity in the last 12 months.

The code of conduct breaches have been confirmed by the Australian Public Service Commission (APSC), which has also revealed the creation of a new "central team" to investigate serious misconduct allegations in response to the robotdebt scandal.

The APSC's report reveals 29 public servants did not take reasonable steps to avoid real or apparent conflicts of interest that may have interfered with their work last financial year.

More than 50 public servants were found to have not acted with care or diligence in their work last financial year. Another 389 undermined the "integrity and good reputation" of their department and the public service more broadly.

About 4,000 of the 127,000 public servants (3.2%) who participated in the annual survey run by the APSC said they "had witnessed another APS employee within their agency engaging in behaviour they considered may be serious enough to be viewed as corruption". (Source)

U.S. GOVERNMENT

Former U.S. Ambassador Charged With Secretly Acting As An Agent Of The Cuban Government - December 4, 2023

Victor Rocha is a former U.S. Department of State employee who served on the National Security Council from 1994 to 1995 and ultimately as U.S. Ambassador to Bolivia from 2000 to 2002, with committing multiple federal crimes by secretly acting for decades as an agent of the government of the Republic of Cuba.

Beginning no later than approximately 1981, and continuing to the present, Victor Rocha, a naturalized U.S. citizen originally from Colombia, secretly supported the Republic of Cuba and its clandestine intelligence-gathering mission against the United States by serving as a covert agent of Cuba's General Directorate of Intelligence.

Rocha obtained employment in the U.S. Department of State between 1981 and 2002, in positions that provided him access to nonpublic information, including classified information, and the ability to affect U.S. foreign policy. After his State Department employment ended, Rocha engaged in other acts intended to support Cuba's intelligence services. From in or around 2006 until in or around 2012, Rocha was an advisor to the Commander of the U.S. Southern Command, a joint command of the United States military whose area of responsibility includes Cuba.

Rocha kept his status as a Cuban agent secret in order to protect himself and others and to allow himself the opportunity to engage in additional clandestine activity. Rocha provided false and misleading information to the United States to maintain his secret mission; traveled outside the United States to meet with Cuban intelligence operatives; and made false and misleading statements to obtain travel documents. (Source)

Former IRS Employee Pleads Guilty To $171,000+ Of Money Laundering In Connection With COVID-19 Fraud - December 6, 2023

Brian Saulsberry was employed by the IRS as a Program Evaluation and Risk Analyst in the Human Capital Office.

Saulsberry submitted false Economic Injury Disaster Loan (EIDL) applications and obtained $171,400 in loan funds. After obtaining the fraudulent loan funds, Saulsberry transferred the funds to his personal checking account. He then used the loan funds for purposes not authorized by the EDIL program, but instead transferred $100,000 to an investment account, knowing that the property involved in the transaction was derived from unlawful activity. (Source)

U.S. Postal Employee Admits To Stealing $170,000+ In Cash From Mail - December 1, 2023

From November 2021 to August 2022, Joseph Fenuto was employed as a U.S. Postal Service letter carrier.

Fenuto admitted he had stolen more than 50 such parcels containing cash from numerous retail stores at the Gloucester Premium Outlets. Fenuto said he stole $171,110 from parcels that he was required to ensure remained in the mail stream for their delivery to a bank. (Source)

U.S. Postal Worker Sentenced To Prison For Stealing $18,000+ - December 1, 2023

From August 2018, Zeon Johnson worked as a Sales and Service Distribution Associate for USPS. As part of his job, Johnson sold stamps and processed money order transactions for USPS customers.

From approximately July 2019 through June 2020, Johnson converted over $18,000 in USPS funds for personal use by stealing cash funds paid by customers for stamps and issuing USPS money orders payable to himself. (Source)

U.S. Postal Service Employee Sentenced To Prison For Stealing $2,400+ Of Money Orders - December 13, 2023

While working for the USPS in Ithaca, New York, Stephen Perrine stole 10 money orders totaling $2,480, by issuing them to himself and entering fraudulent justifications in a USPS accounting system. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Naval Commander Pleads Guilty To Distributing Child Sexual Abuse Material And Retaining Classified Information - December 6, 2023

State law enforcement in Rhode Island received a cyber tipline report that a user of a particular messaging application had shared videos depicting the sexual abuse of young children. The investigation identified the user as Gregory McLean, who was at that time an active-duty officer in the U.S. Navy, with the rank of Lieutenant Commander and serving as the Executive Officer of a ship stationed aboard Naval Station Mayport in Florida.

NCIS agents executed a federal search warrant at McLean's residence, during which they seized numerous electronic devices and storage media. A forensic review revealed that several of these items contained files depicting the sexual abuse of minors.

The forensic review also identified a flash drive – which had been recovered from McLean's kitchen counter – that contained approximately 150 documents containing national defense information classified at the Secret level and 50 documents containing national defense information classified at the Confidential level.

An investigation by NCIS and the FBI revealed that throughout his service as a naval officer, McLean had access to classified information and held a Top-Secret security clearance. McLean had entered into various agreements with the United States regarding the protection and proper handling of classified information and was aware that his home was not an authorized location to store classified national defense information. In particular, the criminal information and plea agreement identify two documents McLean unlawfully retained which contained national defense information related to foreign governments and their combat aircraft and naval capabilities. Disclosure of this information could reasonably be expected to cause damage and, in some instances, serious damage to the national security of the United States. (Source)

Air Force Disciplines 15 Members Over Leak of Classified Documents - December 11, 2023

The United States Air Force announced on Monday it has disciplined 15 members from a Massachusetts base following an inspector general's investigation into 21-year-old Airman 1st Class Jack Teixeira's alleged leak of national security documents on the social media platform Discord that was exposed earlier this year.

The inspector general's investigation was separate from the probe conducted by the Justice Department that resulted in Teixeira's arrest in April and subsequent indictment in June on six counts for the unauthorized disclosure of national defense information. Teixeira pleaded not guilty in June, remains behind bars and is still awaiting a trial date.

The Department of the Air Force released its report on Monday on the results of an Air Force Inspector General (IG) investigation that found individuals in Teixeira's unit, the 102nd Intelligence Wing, Otis Air National Guard Base, Massachusetts, "failed to take proper action after becoming aware of his intelligence-seeking activities."

Beginning on Sept. 7, Air National Guard leaders "initiated disciplinary and other administrative actions against 15 individuals, ranging in rank from E-5 to O-6, for dereliction in the performance of duties," the Air Force said.

The actions taken ranged from relieving personnel from their positions, including command positions, to non-judicial punishment under Article 15 of the Uniform Code of Military Justice. (Source)

Army Civilian Employee Charged For $100 Million Fraud Scheme / Used Funds For Jewelry, Clothing, Vehicles, Real Estate - December 6, 2023

Janet Mello allegedly stole more than $100 million in Army funds by regularly submitting fraudulent paperwork that indicated an entity she controlled, Child Health and Youth Lifelong Development (CHYLD), was entitled to receive funds from the Army. Mello claimed that CHYLD provided services to military members and their families, when, in reality, CHYLD did not provide any services. The indictment alleges that Mello instead used the funds to buy millions of dollars in jewelry, clothing, vehicles, and real estate. Additionally, Mello is alleged to have falsified the digital signature of one of her supervisors on multiple occasions. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

2 Men Accused Of Impersonating Federal Agents & Tricking Secret Service Agents Sentenced To Prison - December 1, 2023

Arian Taherzadeh was sentenced o 33 months in prison for pretending to be a federal law enforcement officer to curry favor with members of the U.S. Secret Service, and to lease several luxury apartments for which he then failed to pay rent.

Taherzadeh and a co-conspirator, Haider Ali operated a business called United States Special Police LLC (USSP), which was described as a private law enforcement, investigative, and protective service based in Washington, D.C. The company was not associated in any way with the U.S. government or the District of Columbia and had never done business with the federal or D.C. governments.

Taherzadeh falsely claimed at various times to be, among other things, a Special Agent with the DHS, a member of a multi-jurisdictional federal task force, a former U.S. Air Marshal, and a former U.S. Army Ranger. He used these false claims to recruit others to USSP, under the guise that it was part of a covert federal law enforcement task force, to defraud owners of three apartment complexes into providing him with multiple apartments and parking spaces for his supposed law enforcement operations, and to ingratiate himself with members of federal law enforcement and the defense community. Both Taherzadeh and Ali used these false claims to recruit others to join their "task force" or "unit," which these individuals believed to be part of DHS and federal law enforcement.

Taherzadeh also provided these Secret Service employees with tangible and intangible gifts. For instance, Taherzadeh provided one employee and his wife with a generator and a doomsday/survival backpack.

He provided another employee with a rent-free penthouse apartment for approximately one year, worth approximately $40,200. He provided a third employee with a rent-free apartment for approximately one year, worth an estimated $48,240, as well as a drone, a gun locker, and a Pelican case. (Source)

Former FBI Special Agent Sentenced To Prison For Conspiring To Violate U.S. Sanctions On Russia - December 14, 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.

McGonigal was sentenced to prison for conspiring to violate the International Emergency Economic Powers Act and to commit money laundering in connection with his 2021 agreement to provide services to Oleg Deripaska, a sanctioned Russian oligarch. (Source)

Police Officer Sentenced To Prison For $275,000+ Of COVID-19 Relief Fraud - December 11, 2023

Samuel Harris was a full-time Miami-Dade Police Department (MDPD) Police Officer, also was the owner and president of Oregen Digital, Inc. (Oregen). Working with an associate, on June 29, 2020, Harris submitted and caused to be submitted a false and fraudulent PPP loan application falsely claiming that Oregen had 10 employees and a monthly payroll of over $50,000 per month. In support of this application, Harris submitted a fraudulent IRS Form W-3 falsely claiming that Oregen had paid 10 employees over $602,000 in wages during 2019. As a result of this false and fraudulent application, Harris obtained a $125,579 PPP loan from a Georgia-based SBA-approved PPP lender.

Harris also admitted that on June 30, 2020, he caused to be submitted to the SBA a false and fraudulent EIDL application in the name of Oregen, seeking both an EIDL and an EIDL advance. In this fraudulent application, Harris falsely claimed that for the twelve-month period prior to January 31, 2020, Oregen had gross revenues of over $859,000 and 10 employees. As a result of this fraudulent application, Oregen obtained from the SBA a $10,000 EIDL advance that did not need to be repaid and $149,900 in EIDL loan proceeds. (Source)

Former Federal Correctional Officer Pleads Guilty To $39,000+ Disability Wire Fraud Scheme - December 4, 2023

Katrina McCoy is a former correctional officer with the Federal Bureau of Prisons (BOP).

Between March 2019, and February 2021, McCoy submitted false disability claims with fictitious supporting documentation. McCoy created the supporting documentation on BOP letterhead and affixed the names of her supervisor and a medical professional without their knowledge or permission. As a result of her fraudulent scheme, McCoy caused 14 wire transfers to be deposited into her bank account totaling $39,570. (Source)

State Troopers Convicted Of Stealing Overtime Funds And Wire Fraud - December 13, 2023

From 2015 through 2018, Daniel Griffin, William Robertson and other troopers in the Traffic Programs Section at State Police Headquarters in Framingham, Massachusetts conspired to steal thousands of dollars in federally funded overtime by regularly arriving late to, and leaving early from, overtime shifts funded by grants intended to improve traffic safety. During the course of the conspiracy, Griffin made and approved false entries on forms and other documentation to conceal and perpetuate the fraud.

When the Massachusetts State Police (MSP) overtime misconduct came to light in 2017 and 2018, Griffin, Robertson and their co-conspirators took steps to avoid detection by shredding and burning records and forms. After an internal inquiry regarding missing forms, Griffin submitted a memo to his superiors that was designed to mislead them by claiming that missing forms were "inadvertently discarded or misplaced" during office moves.

Additionally, Griffin spent significant time running his security business, Knight Protection Services, during hours that he was collecting regular MSP pay and overtime pay. From 2012 to 2019, Griffin collected almost $2 million in KnightPro revenue. Of that total, Griffin hid over $700,000 in revenue from the IRS and used hundreds of thousands of dollars in KnightPro income to fund personal expenses, such as golf club expenses, car payments, private school tuition and expenses related to his second home on Cape Cod. (Source)

STATE / CITY GOVERNMENTS / MAYORS

Career & Technical Education Organization Executive Director Sentenced To Prison For Embezzling $2.8 Million+ Of Federal Funding - December 5, 2023

While serving as the Executive Director of Alabama Association for Career and Technical Education, Doris Gilmore embezzled federal grant funds received by the association.

Statements made during her sentencing hearing indicated that the embezzlement may have taken place for more than a decade. The judge ordered Gilmore to pay $2,832,486.33 in restitution to the Alabama Association for Career and Technical Education. (Source)

City Employee Pleads Guilty To $54,000 Fake Invoices Scheme - December 20, 2023

Keyshia Sanders was a Constituent Service Manager.

Sanders pleaded guilty to engaging in a wire fraud scheme to fraudulently induce the disbursement of grant money for her own benefit. The scheme involved the use of fraudulent invoices that caused the grant's fiscal agent to disburse funds to Sanders in clear contradiction to the terms of the grant and Sander's role as a City of Jackson employee. The grant was intended to provide project support in the City of Jackson to invest in artists, artist collectives, and small arts organizations. In total, the fraudulent transactions caused by Sanders over the course of the scheme totaled a loss of approximately $54,000. (Source)

City Building Inspection Engineer Pleads Guilty To Accepting Bribers For Building Permits - December 8. 2023

Rudy Pada admitted that he accepted bribes from individuals seeking building and construction permits from the San Francisco Department of Building Inspection (DBI). Pada worked as a plan checker at DBI from 1984 to September 2017, reviewing and approving construction plans and providing builders with the permits necessary for residential and commercial construction projects in San Francisco.

The bribes to Pada, which began in 2003 and continued until September 2017, consisted of cash, free meals, drinks, and other benefits, paid by executives at a construction planning and design firm.

Pada accepted the bribes in return for expediting and approving permits for their building and construction plans. In addition, Pada solicited and accepted an interest-free $85,000 loan facilitated by one of the executives. (Source)

County Employee Sentenced To Prison For Scheming To Fraudulently Purchase And Resell Properties - December 14, 2023

Mustafaa Saleh worked as an Asset Manager for the Cook County Land Bank Authority (CCLBA), a governmental entity that promoted the redevelopment and reuse of vacant, foreclosed, abandoned, and tax delinquent real estate by acquiring and transferring the property to private ownership. The CCLBA sold the real estate at below-market rates and prohibited the buyers from selling or renting a property until the CCLBA was satisfied that the buyer had adequately improved it. CCLBA employees were prohibited from purchasing a property from the agency unless it would be used for the employee's primary residence.

From 2016 to 2021, Saleh used nominee or "straw" buyers to fraudulently purchase six properties from the CCLBA on Saleh's behalf and thereafter redeveloped, resold, and otherwise used the properties for Saleh's financial benefit.

In some instances, Saleh's duties at the CCLBA allowed him oversight over the same properties he owned and resold. The properties were located in Chicago and the nearby suburbs of Oak Lawn and Midlothian.

In addition to the property fraud scheme, Saleh fraudulently obtained maintenance work from the CCLBA. In 2016, Saleh formed a property maintenance company called Evergreen Property Services and directed another individual to pose as its owner. Over the next three years, Saleh caused the CCLBA to contract with Evergreen and pay it more than $1 million for property maintenance services, even though CCLBA employees were prohibited from having a financial interest in property maintenance companies contracting with the agency. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

School Payroll Administrator Pleads Guilty To Stealing $600,000+ December 12, 2023

Between January 11, 2016, and April 10, 2023, Danielle Liles devised a scheme to defraud Silver River Mentoring and Instruction (SRMI), an alternative school for middle and high school students.

During this time, Liles handled the payroll at SRMI. Liles had 137 unauthorized paychecks issued in her name by logging false information into SRMI's accounting software. She then received the paychecks through Automated Clearinghouse Services (ACH) wire transfers directly into her bank account. During a financial review with the school's executive staff in April 2023, Liles admitted that she had been "paying herself extra money" and had become addicted to stealing the payroll funds.

Liles will also be ordered to forfeit $616,793.43, which represents the proceeds of her offenses. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

Union Chief Financial Officer Sentenced To Prison For Embezzling $19,000+ - December 5, 2023

From December 2018, until June 2019, Gary Fridley was a Union Officer while employed by American Electric Power (AEP). As the union's elected Financial Secretary, Fridley was the union's Chief Financial Officer and was responsible for preparing and co-signing union checks and maintaining financial records. Fridley was one of three signatories on the union's checking account. As financial secretary, Fridley was entitled to an officer's salary as well as reimbursement for lost time or wages from his employment when he took off from work for union business.

On about June 12, 2019, Fridley received a check for $1,321.55 as reimbursement for lost time. Fridley admitted that he had not lost any time with AEP during that pay period. Fridley submitted a false voucher to receive an unauthorized lost time payment and forged the signature of another union official in order to cash the check for the fictitious lost time.

Fridley submitted additional false vouchers to receive unauthorized lost time payments from the union and forged the signatures of other union officials to cash the union checks he wrote payable to himself for the fictitious lost time payments. Fridley admitted that he improperly received $19,732.88 through his wrongful actions as the union's financial secretary. (Source)

BANKING / FINANCIAL INSTITUTIONS

Bank Teller Supervisor Sentenced To Prison For Stealing $375,000 - December 6, 2023

Between July 2022 and December 2022, Pablo Rocha worked as a Bank Teller Supervisor at a federally insured bank in Massachusetts.

Rocha used his access to the bank's vault to steal cash. Rocha then covered his tracks by writing false entries in the bank's records and by processing fake transactions in the electronic records system to make it appear that the cash had been shipped to the Federal Reserve Bank of Boston. In total, Rocha stole approximately $375,000. (Source)

Bank Employee Charged With Stealing $105,000+ Federal Benefits Intended For Deceased Customer - December 13, 2023

In 2014, Jorge Nova was an employee at a commercial bank in Nutley, New Jersey, where a customer received Social Security Administration (SSA) retirement benefits via direct deposit.

The Social Security Administration was not notified of the beneficiary's death and continued to deposit retirement benefits into the beneficiary's bank account for more than four years, until October 2018. Nova fraudulently obtained funds from the beneficiary's account by causing debit cards to be issued to himself in the beneficiary's name, which he then used to drain the retirement benefits from the beneficiary's bank account. Nova also registered new accounts with a money service provider in the name of the deceased beneficiary and withdrew money from a second bank account held in the beneficiary's name. Nova fraudulently obtained more than $105,000 intended for the deceased beneficiary. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

2 Former Samsung Employees Charged For Stealing Trade Secrets - December 18, 2023

Two ex-employees of a prominent South Korean technology firm, known as Mr. Kim and Mr. Bang, have been taken into custody for purportedly stealing and trading the organization's 16-nanometer DRAM technologies to a rival CXMT Chinese firm in the memory technology sector.

The accused are said to have made several million dollars by divulging the company's confidential memory technology information. This unauthorized sharing of sensitive data has reportedly caused substantial financial damage and a competitive setback for the company. Law enforcement and regulatory agencies are working closely together to investigate the case and bring the alleged perpetrators to justice.

This violation could have considerably diminished Samsung, the South Korean organization's tech advantage over its Chinese counterpart, potentially affecting years of research and development. As a result, the company may face severe setbacks in its competitive edge, technological innovation, and global market share. Furthermore, this incident highlights the need for stronger cybersecurity measures in protecting intellectual property and sensitive information in an increasingly competitive technology landscape. (Source)

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

No Incidents To Report

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

No Incidents To Report

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

Former CEO Non-Profit Charged For Stealing $1.4 Million+ Over 5 Years - December 7, 2023

On Nov. 16, 2023, a federal grand jury returned an indictment against Richard Alan Abrusci, 45, of South Lake Tahoe, charging him with nine counts of wire fraud, one count of aggravated identity theft, and three counts of monetary transactions with proceeds of specified unlawful activity. The indictment was unsealed after the arrest.

In 2014, Richard Abrusci began working at a non-profit organization that operates a chain of retail stores in California and Nevada. Abrusci became the Chief Operating Officer of the organization in 2016 and its president and CEO in 2018.

From 2016 through 2021, Abrusci fraudulently caused the non-profit organization and one of its subsidiaries to pay approximately $1.4 million to Resolution Arrangement Services (RAS).

RAS consisted of nothing more than a fictitious business name that Abrusci registered in 2008 and a bank account that he opened the same year. Abrusci caused the fraudulent payments into the RAS bank account that he controlled by using various false documents, including invoices and purchase orders.

In one instance, Abrusci used a forged letter purporting to be from an attorney representing the non-profit organization to convince the organization's CFO to pay RAS $55,000 under false pretenses related to a lawsuit.

The payments to RAS were supposedly for information-technology services, helping to facilitate settlement of a lawsuit, and assisting the non-profit organization in running call centers for the State of California during the COVID-19 pandemic. In fact, RAS provided none of the services for which it billed the non-profit organization and its subsidiary. (Source)

Former Law Firm Paralegal Pleads Guilty To Embezzling $600,000 From Bankruptcy Estate Funds Over 9 Years - December 18, 2023

Becky Sutton fraudulently embezzled $600,000+ from 2009 to 2018 while working on bankruptcy matters at the law firm.

Sutton admitted in a plea agreement that she embezzled money from more than 40 bankruptcy estate accounts and several liquidating trust accounts in Chapter 7 and Chapter 11 matters on which she worked. Sutton orchestrated fraudulent transfers of bankruptcy funds from fiduciary bank accounts intended for creditors to accounts she controlled, including her personal bank account, credit card account, student loan account, and mortgage account. In one instance, Sutton used a company with a name similar to a true creditor to disguise her fraudulent diversion of the funds. Sutton admitted in the plea agreement that her conduct victimized not only the creditors, but also her law firm, a partner at the firm for whom she worked, and the U.S. Trustee Program, among others.(Source)

Armored Transport Guard Sentenced To Prison For Stealing $579,000+ From Banks & Credit Unions - December 6, 2023

Austin Rutherford was sentenced to prison for stealing over $579,000 from three banks and two federal credit unions while serving as an armed transport guard.

Austin Rutherford was an Armed Transport Guard for Axiom Armored Transport from January 2019 to March 2022. Axiom provided armed transportation of U.S. currency for several banks, credit unions and ATMs. Rutherford was transferred to Axiom's Juneau branch in March 2020 and started stealing funds around that time.

An Axiom security camera recorded Rutherford taking a large amount of cash from Axiom property and into his personal vehicle, where he drove away. Bank records later showed that the defendant made multiple cash deposits into his personal bank account totaling over $338,000 and used the money for personal benefit. (Source)

Treasure That Worked For 2 Non-Profit Organizations Sentenced To Prison For Stealing $350,000+ - December 4, 2023

Charles Davis worked as a Treasurer for 2 non-profit organizations, ArtWorks Community Arts Education Center and the Russell County Arts Council.

Davis was also ordered to pay $352,336.72 in restitution to ArtWorks Community Arts Education Center and the Russell County Arts Council. (Source)

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

Jacksonville Jaguars Football Team Employee Pleads Guilty To Embezzling $22 Million From Employer / Used Funds To Purchase Condo, Tesla, Nissan Truck, Travel, Country Club Membership, Spa Treatments, Home Furnishings, Etc. - December 15, 2023

Amit Patel operated a fraud scheme through which he embezzled approximately $22,221,454 from his employer from eptember 2019, and continued until he was fired by his employer in February 2023.

Patel worked for the Jacksonville Jaguars Football Team.

Patel used his role as the administrator for companys virtual credit card (VCC) program to make hundreds of purchases and transactions with no legitimate business purpose. Then, to hide and continue to operate the scheme, rather than accurately report his VCC transactions, Patel created accounting files that contained numerous false and fraudulent entries and emailed them to the accounting department.

Patel used a variety of methods to hide his illicit transactions by omitting them from the files, while still having the total dollar amount of VCC expenditures match the balances paid by the VCC program line of credit. Patel identified legitimate reoccurring VCC transactions, such as catering, airfare, and hotel charges, and then duplicated those transactions; he inflated the amounts of legitimate reoccurring VCC transactions; he entered completely fictitious transactions that might sound plausible, but that never actually occurred; and he moved legitimate VCC charges from upcoming months into the month of the accounting file that was immediately due to the accounting department.

Patel used the proceeds of this scheme, in whole or part, to place bets with online gambling websites, to purchase a condominium in Ponte Vedra Beach, Florida, to pay for personal travel for himself and friends (including chartering private jets and booking luxury hotels and private rental residences), to acquire a new Tesla Model 3 sedan and Nissan pickup truck, to pay a criminal defense law firm, and to purchase cryptocurrency, non-fungible tokens, electronics, sports memorabilia, a country club membership, spa treatments, concert and sporting event tickets, home furnishings, and luxury wrist watches. (Source)

Former Facebook Executive Pleads Guilty To Stealing $4 Million+ To Live Luxury Lifestyle - December 12, 202

From about January 2017 to September 2021, Barbara Smiles led Diversity, Equity, and Inclusion (DEI) programs at Facebook and was responsible for developing and executing DEI initiatives, operations, and engagement programs. In her position, Furlow-Smiles had access to company credit cards. She also maintained authority to submit purchase requisitions and approve invoices for authorized vendors of Facebook.

Smiles used her position at Facebook to cheat and defraud the company. She caused Facebook to pay numerous individuals for goods and services never provided to the company. Those individuals then paid kickbacks to Smiles, often in cash.

Smiles stole more than $4 million from Facebook based on fictitious charges and fraudulent invoices for which goods and services were never provided to the company. She used the money to live a luxury lifestyle in California and Georgia. (Source)

Paralegal Pleads Guilty To Embezzling $2 Million+ From Employer's Clients / Used Funds To Pay For Mortgage, Car, Credit Card Payments - December 1, 2023

From 2007 to 2021, Jennifer Roarke was employed as an assistant and a paralegal for a law firm. The law firm handled, among other things, the administration and management of trusts for clients, including the trusts' bank accounts. As part of her duties, Roarke was responsible for opening mail, depositing checks into trust bank accounts, and processing invoices.

Roarke admitted that from 2015 to September 2021, Roarke executed the embezzlement scheme by causing at least 190 fraudulent and unauthorized bank wires, totaling more than $2 million, from the law firm's clients' trust bank accounts to bank accounts controlled by Roarke. Roarke used the embezzled funds to pay for personal items, make mortgage, car, and credit card payments, and to fund an extravagant lifestyle. (Source)

Bookkeeper For 2 Businesses Sentenced To Prison For Embezzling $500,000+ From Both Businesses To Pay Her Debts And Family Member Debts - December 11, 2023

Tara Durnell, while working as a Bookkeeper. She embezzled from Kronebusch Electric, Inc. (KEI), an electrical services company and then from Mitchell's Crash Repair, an auto repair shop, after she left KEI's employment.

From at least 1997, Durnell embezzled from her employer, Kronebusch Electric, Inc., (KEI) a small company in Conrad, where she worked as a Bookkeeper, to fund her personal lifestyle. Durnell used her access to pre-signed company checks and company bank accounts to pay hundreds of thousands of dollars toward personal credit card debt, personal car loan payments and debts belonging to family members.

To conceal her scheme, Durnell used her access to the company's accounting software to hide her illicit transactions and make them appear like legitimate businesses expenses. In total, Durnell embezzled almost $500,000 from KEI.

Durnell left employment with KEI when the scheme was discovered and found work as a bookkeeper with Mitchell's Crash Repair in Great Falls. In January 2022, Durnell again used her access to the business's pre-signed checks and bank accounts and to pay tens of thousands of dollars toward personal expenses. Durnell embezzled approximately $15,491 from Mitchell's Crash Repair. (Source)

Employee Charged With Embezzling $280,000+ From Employer To Pay Credit Cards & Auto Loans - December 14, 2023

Jasmyne Botelho is a former employee of a Bristol County Massachusetts industrial company. See was arrested and charged with a scheme to embezzle more than $280,000 from her employer between September 2017 and April 2020.

Botelho allegedly directed payments purportedly intended for the company's vendors to bank accounts she controlled and used company funds to make payments on personal credit cards and auto loans. To hide her scheme, Botelho allegedly falsified her employer's books and records to make it appear as though the payments had in fact been sent to legitimate vendors rather than to Botelho. (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

No Incidents To Report

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

Disgruntled Cloud Engineer Sentenced To Prison For Sabotaging Banks Computer Network After He Was Fired - December 11, 2023

Miklos Brody worked as a Cloud Engineer for a bank headquartered in San Francisco. On March 11, 2020, when he was fired for violating company policy.

Later that evening, and continuing into the following morning, Brody used his company issued laptop, which he failed to return upon being fired, to access the bank's computer network without authorization and to cause substantial damage. Brody deleted the bank's code repositories, ran a malicious script to delete logs, left taunts within the bank's code for former colleagues, and impersonated other bank employees by opening sessions in their names. He also emailed himself proprietary bank code that he had worked on as an employee, which was valued at over $5,000. The judge determined the total cost of the damage to the bank's systems to be at least $220,621.22.

In the days and weeks that followed his firing, Brody engaged in a series of evasive and deceptive actions, including filing a police report in which he falsely told the San Francisco Police Department that his company issued laptop had been stolen from his car while he was working out at the gym. Brody doubled down on that false allegation in statements he made to U.S. Secret Service agents during an interview following his arrest in March 2021. (Source)

Former Public School Information Technology Manager Pleads Guilty To Sabotaging School's Computer Network - December 13, 2023

Conor LaHiff was employed as a Desktop & Network Manager at a public high school until he was terminated in June 2023.

After he was fired, LaHiff allegedly used his administrative privileges to deactivate and delete thousands of Apple IDs from the school's Apple School Manager accoun, software used to manage student, faculty and staff information technology resources. LaHiff also allegedly deactivated more than 1,400 other Apple accounts and other IT administrative accounts and disabled the school's private branch phone system, which left the school's phone service unavailable for approximately 24 hours. (Source)

THEFT OF ORGANIZATIONS ASSESTS

No Incidents To Report

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

No Incidents To Report

EMPLOYEE DRUG RELATED INCIDENTS

Pain Management Clinic Office Manager Sentenced To Prison For $1.2 Million+ Pill Mill Scheme - December 12, 2023

Andres Martinez was the Office Manager of Jomori Health and Wellness (Jomori), a purported Houston pain management clinic.

Martinez operated Jomori with Dr. Oscar Lightner as a pill mill. Lightner, who was the owner of and physician at Jomori, unlawfully prescribed dangerous combinations of controlled substances, including of hydrocodone, carisoprodol, and alprazolam to his patients without a legitimate medical purpose in exchange for cash payments ranging from $250 to $500.

Martinez, who is Lightner's stepson, coordinated with crew leaders to bring multiple people, including individuals living in homeless shelters, into Jomori to pose as patients to obtain prescriptions for opioids and other controlled substances. Jomori received over $1.2 million in cash over 14 months through its scheme that resulted in the unlawful distribution and dispensing of over 600,000 opioids and other controlled substances. (Source)

2 Nurses Working For Medical Center Charged For Removing Pain Killers Intended For Patients - December 8, 2023

Robin Nichols, on April 15, 2023, while working as a nurse at Catholic Medical Center, removed a quantity of fentanyl, a narcotic painkiller drug in liquid form, from a syringe intended for an operating room patient and which she knew was intended for that patient and replaced the fentanyl with a quantity of saline.

Lisa Richardson, on December 30, 2022, while working as a nurse at Concord Hospital, entered the room of a patient in the Intensive Care Unit and removed a quantity of fentanyl, a narcotic painkiller drug in liquid form, from an intravenous line bag attached to the patient and which she knew was being dispensed to that patient, and replaced the fentanyl with a quantity of saline. (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 EMPLOYEE LAYOFFS OR CAUSING COMPANY TO CEASE OPERATIONS

No Incidents To Report

WORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES'

Former Employees Of County Health Care Facility Plead Guilty To Hate Crime Charges / Assaults Against Disabled Residents - December 4, 202

Tyler Smith and Zachary Dinell were employees of an in-patient health care facility.

From approximately June 2016 to September 2017, they both engaged in a conspiracy to commit hate crimes against residents of the facility because of the residents' actual or perceived disabilities. Smith and Dinell carried out assaults in a variety of ways, including by punching and kicking residents, rubbing liquid irritants in their eyes, spraying liquid irritants in their eyes and mouths, and in one instance removing a resident's compression stocking in a manner intended to inflict pain.

Several of these assaults were recorded on Dinell's cell phone. In one instance, Smith admitted jumping on top of a 13-year-old minor, while the child was lying prone on his bed, and while Dinell filmed the incident on his cellular phone. Smith further acknowledged that immediately after recording the video, Dinell texted the video to him.

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

Smith further admitted that he and Dinell were able to avoid detection by, among other things, exploiting their one-on-one access to residents of the facility and the fact that the victims were non-verbal and could not report the defendants' abuse. Due to their physical disabilities, the residents also were not able to defend themselves against the assaults.

As part of his plea agreement, and subject to the approval of the judge, Smith has agreed to a term of imprisonment of not less than 60 months and not more than 120 months. Zachary Dinell previously pleaded guilty to all charges and was sentenced on January 26, 2023, to 17 years' imprisonment, followed by three years' supervised release. (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)

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

DESTRUCTION OF EMPLOYERS PROPERTY BY EMPLOYEES

Bank President Sets Fire To Bank To Conceal $11 Million Fraud Scheme - February 22, 2021

On May 11, 2019, while Anita Moody was President of Enloe State Bank in Cooper, Texas, the bank suffered a fire that investigators later determined to be arson. The fire was contained to the bank’s boardroom however the entire bank suffered smoke damage.

Investigation revealed that several files had been purposefully stacked on the boardroom table, all of which were burned in the fire. The bank was scheduled for a review by the Texas Department of Banking the very next day. The investigation revealed that Moody had created false nominee loans in the names of several people, including actual bank customers. Moody eventually admitted to setting the fire in the boardroom to conceal her criminal activity concerning the false loans.

She also admitted to using the fraudulently obtained money to fund her boyfriend’s business, other businesses of friends, and her own lifestyle. The fraudulent activity, which began in 2012, resulted in a loss to the bank of approximately $11 million dollars. (Source)

Fired Hotel Employee Charged For Arson At Hotel That Displaced 400 Occupants - June 29, 2023

Ramona Cook has been indicted on an arson charge and accused of setting fires at a hotel after being fired.

On Dec. 22, 2022, Cook maliciously damaged the Marriott St. Louis Airport Hotel.

Cook was fired for being intoxicated at work. She returned shortly after being escorted out of the hotel by police and set multiple fires in the hotel, displacing the occupants of more than 400 rooms. (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)

3 Bank Board Members Of Found Guilty Of Embezzling $31 Million From Bank / 16 Other Charged / Bank Collapsed - August 8. 2023

William Mahon, George Kozdemba and Janice Weston were members of Washington Federal's Board of Directors. Weston also served as the bank's Senior Vice President and Compliance Officer.

Washington Federal was closed in 2017 after the Office of the Comptroller of the Currency determined that the bank was insolvent and had at least $66 million in nonperforming loans.

A federal investigation led to criminal charges against 16 defendants, including charges against the bank's Chief Financial Officer, Treasurer, and other high-ranking employees, for conspiring to embezzle at least $31 million in bank funds. Eight defendants have pleaded guilty or entered into agreements to cooperate with the government. (Source)

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

In 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)

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

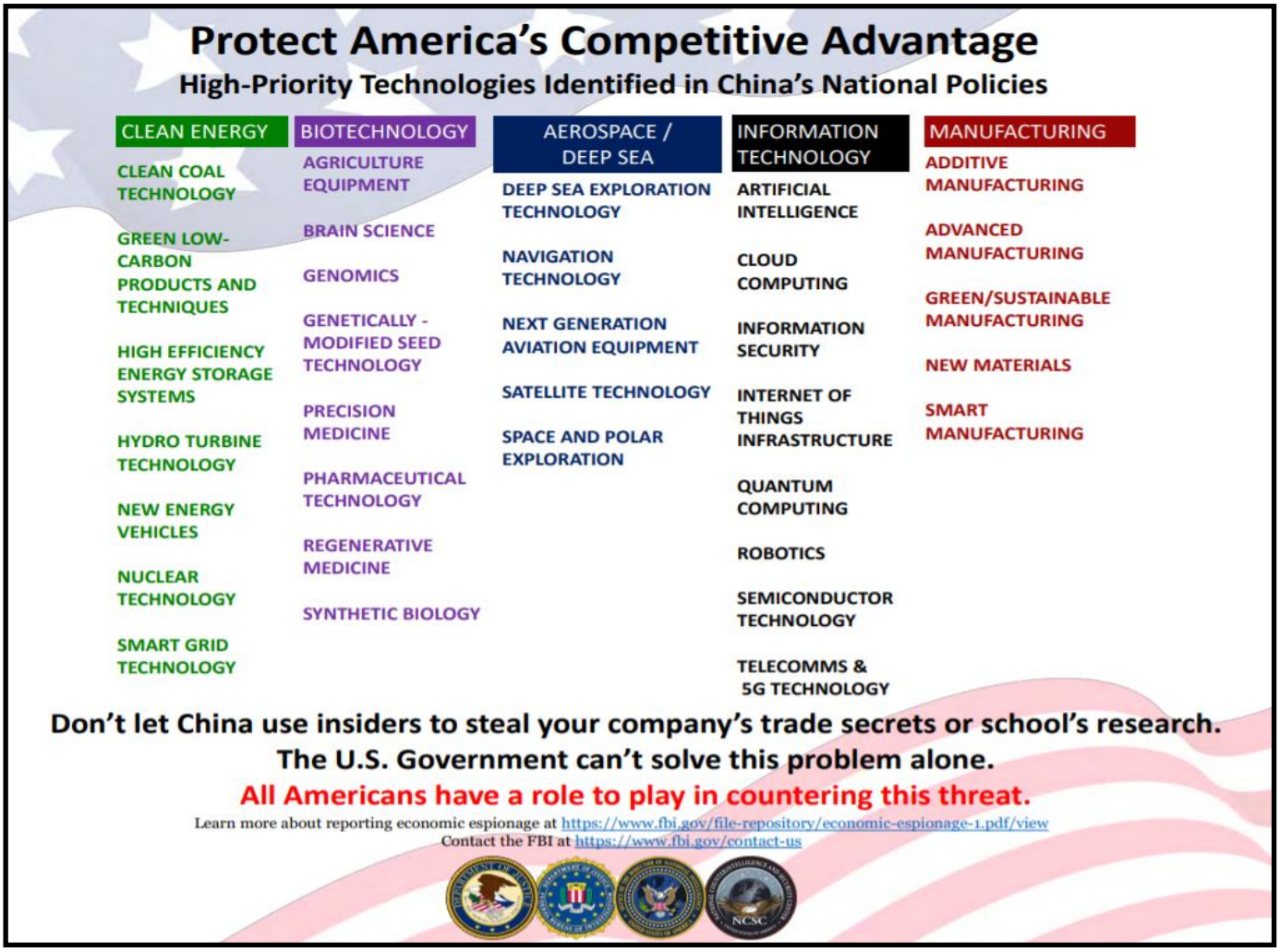
WORKPLACE VIOLENCE TODAY E-MAGAZINE
https://www.workplaceviolence911.com/node/994

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 (**4,900+ 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 SPOTLIGHT REPORT FOR 2023

This comprehensive **EYE OPENING** report provides a **360 DEGREE VIEW** of the many different types of malicious actions employees' have taken against their employers.

This is the only report produced that provides clear and indisputable evidence of how very costly and damaging Insider Threat incidents can be to organizations of all types and sizes. (U.S. Government, Private Sector)
https://nationalinsiderthreatsig.org/pdfs/insider-threats-incidents-malicious-employees-spotlight-report%20for%202023.pdf

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