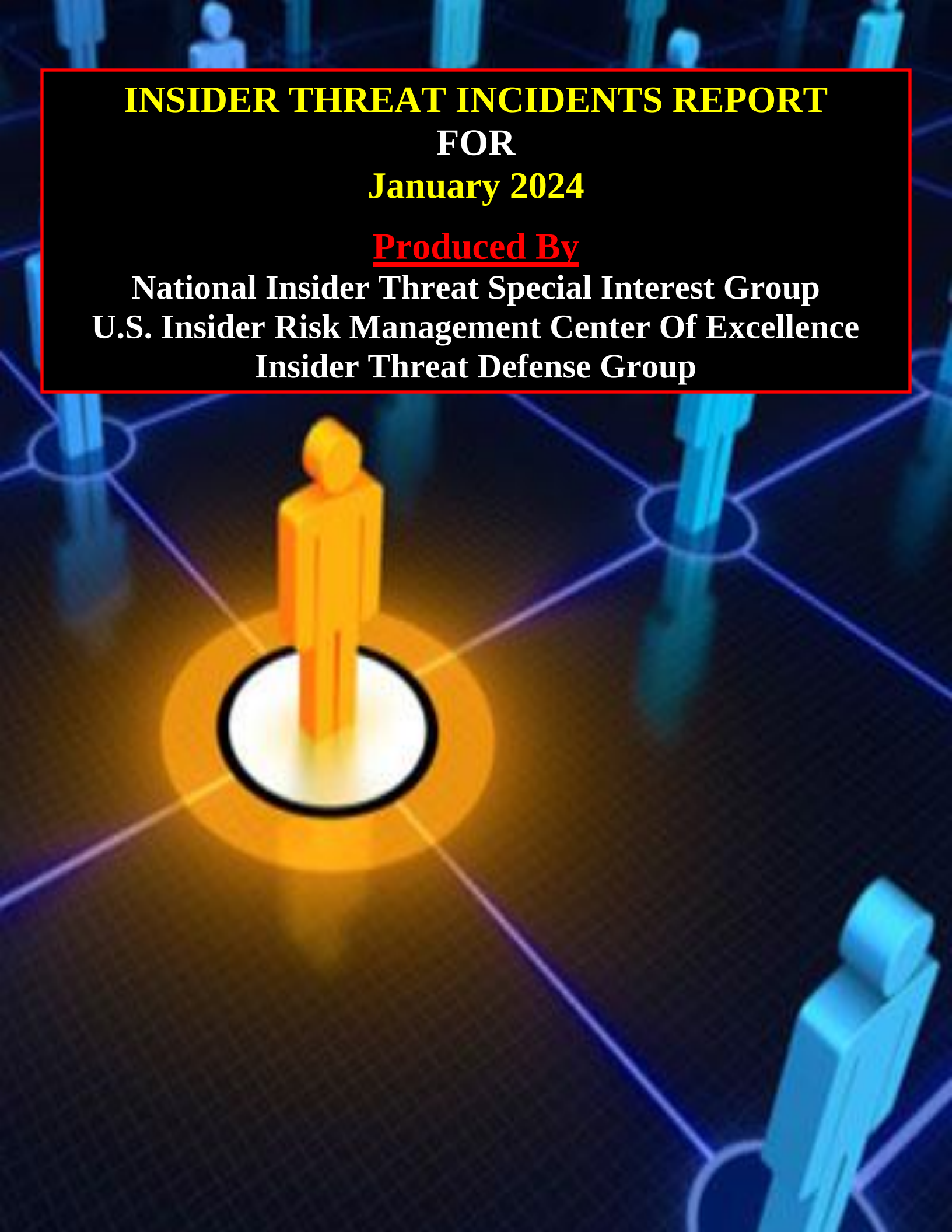
INSIDER THREAT INCIDENTS REPORT
FOR
January 2024

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 15+ 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 21** 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 JANUARY 2024

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

UK National Crime Agency Director Fired For Sending Sensitive & Secret Information Using WhatsApp And Through Her Personal E-Mail - January 15, 2024

A Senior Director at the National Crime Agency (NCA) lost her job after sending sensitive and secret information over her personal email and on WhatsApp in what was described as a "serious information security" breach.

Nikki Holland, former Director of Investigations at the NCA, was responsible for some of the UK's most high-profile criminal investigations, including the NCA's Operation Venetic investigation into the use of EncroChat encrypted phones by organised crime. She led county lines crime investigations and liaised with Five Eyes partner countries on criminal intelligence.

Holland was sacked after an internal disciplinary hearing on 21 December 2023 found that the former Senior Director had sent classified and secret NCA material via a personal email account and on WhatsApp groups in breach of NCA standards.

The NCA said it did not find any malign intent in the security breaches.

The NCA is assessing another allegation that Holland instructed staff to set WhatsApp messages on NCA phones to automatically delete following a hearing during a case under Operation Venetic in late 2020. (Source)

U.S. GOVERNMENT

3 Former DHS Employees Sentenced To Prison For Conspiracy To Steal Proprietary U.S. Government Software & Databases - January 26, 2024

3 former Department of Homeland Security (DHS) employees (Charles K. Edwards, Sonal Patel, Murali Venkata) were sentenced for a conspiracy to steal proprietary software and sensitive law-enforcement databases from the U.S. government for use in a commercial venture.

Edwards was the former Acting Inspector General of the DHS Office of Inspector General (DHS-OIG). Patel and Venkata were employed in DHS-OIG's information technology department. Edwards, Patel, and Venkata were all previously employed at the U.S. Postal Service Office of Inspector General (USPS-OIG).

Edwards, Patel, and Venkata conspired to steal proprietary U.S. software and databases containing sensitive law-enforcement information and the personally identifiable information (PII) of over 200,000 federal employees from DHS-OIG and USPS-OIG. They planned to use the stolen software and databases to create a commercial software product to be offered for sale to government agencies. As part of the scheme, the co-conspirators disclosed the stolen software and databases containing PII to software developers located in India. After Venkata learned of the investigation, he deleted incriminating text messages and other communications in an effort to obstruct the investigation. (Source)

TSA Director Arrested By U.S. Customs & Border Protection For Falsifying Documents For Relative Suffering From Dementia - January 5, 2024

An offical with the Transportation Security Administration (TSA) has been arrested on an outstanding warrant.

TSA Assistant Federal Security Director Maxine McManaman was arrested in Atlanta by U.S. Customs and Border Protection on Dec. 28.

McManaman had an outstanding warrant for her arrest, as posted by the St. Lucie County (Florida) Sheriff's Office, which claimed she and an alleged accomplice named Delroy Chambers Sr. exploited a relative suffering from dementia by falsifying documents in their name, according to Port St. Lucie Police.

"TSA holds its employees to the highest professional and ethical standards and has no tolerance for misconduct on or off duty," a TSA spokesperson said in the statement. The spokesperson added, "Any employee who fails to meet our fundamental ethical standards is held accountable."

McManaman has been placed on leave pending a law enforcement investigation. (Source)

Former IRS Contractor Sentenced To Prison For Disclosing The Tax Returns Of President Trump To News Organizations - January 29, 2024

Charles Littlejohn while working at the IRS as a government contractor, stole tax return information associated with a high-ranking government official (Donald Trump - Public Official A). Littlejohn accessed tax returns associated with Public Official A (And Related Individuals &d Entities) on an IRS database after using broad search parameters designed to conceal the true purpose of his queries. He then uploaded the tax returns to a private website in order to avoid IRS protocols established to detect and prevent large downloads or uploads from IRS devices or systems.

Littlejohn then saved the tax returns to multiple personal storage devices, including an iPod, before contacting News Organization 1. Between around August 2019 and October 2019, Littlejohn provided News Organization 1 with the tax return information associated with Public Official A. Littlejohn subsequently stole additional tax return information related to Public Official A and provided it to News Organization 1. Beginning in September 2020, News Organization 1 published a series of articles about Public Official A's tax returns using the tax return information obtained from Littlejohn. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

U.S. Navy Sailor Sentenced To Prison For Transmitting Sensitive U.S. Military Information To Chinese Intelligence Officer / Received 14 Bribe Payments - January 8, 2024

Thomas Zhao pleaded guilty in October 2023 to one count of conspiracy and one count of receiving a bribe in violation of his official duties.

Zhao, who was stationed at Naval Base Ventura County in Port Hueneme, held a U.S. security government clearance and underwent routine trainings on efforts by hostile nation states to acquire sensitive information.

Between August 2021 and at least May 2023, Zhao received at least $14,866 in 14 separate bribe payments from the intelligence officer, who directed Zhao to surreptitious collect and transmit sensitive U.S. military information and offered to pay Zhao bonuses for controlled and classified information.

In exchange for the illicit payments, Zhao repeatedly entered restricted military and naval installations to secretly collect non-public information regarding U.S. Navy operational security, military trainings and exercises, and critical infrastructure. Zhao used encrypted communications to transmit that sensitive, non-public information to the intelligence officer. Zhao transmitted plans for a large-scale maritime training exercise in the Pacific theatre, operational orders, and electrical diagrams and blueprints for a Ground/Air Task Oriented Radar system located in Okinawa, Japan. (Source)

Former Hotel Manager Sentenced To Prison For Paying $103,000+ In Bribes To Army Training Center Manager - January 29, 2024

On May 3, 2023, a federal grand jury returned a twelve-count Indictment against Alfred Palma and Candy Hanza.

Palma was a United States Army employee and the Manager of the Institutional Training Directed Lodging and Meals (ITDLM) program at Fort Sill, Oklahoma. Palma booked hotel rooms for soldiers who attended off-post trainings. Hanza worked as the general manager of a local hotel. The Indictment alleges that Hanza paid Palma bribes to direct soldiers to Hanza's hotel.

In July 2023, Palma and Hanza pleaded guilty to the bribery scheme. Palma pleaded guilty to receiving bribes totaling $103,200.00 from Hanza in return for favoring the hotel at which Hanza worked as General Manager. Palma further admitted that he used the cash bribes to purchase money orders from Walmart, which he later deposited into his personal checking account, along with the checks that Hanza gave him. Hanza pleaded guilty to paying a bribe to Palma as a public official. (Source)

U.S. Army Soldier Sentenced To Prison For Drug Trafficking And $700,000+ In Money Laundering - January 26, 2024

On May 7, 2021, U.S. Homeland Security Investigations was notified by the French Customs Service stationed at Charles De Gaulle International airport that a package from Cameroon had been intercepted containing approximately three kilograms of ketamine. The package was delivered to Gordon Ray Custis, then a soldier at Fort Liberty, at his home in Fayetteville, by Federal Task Force Officers with the Cumberland County Sheriff's Office.

Custis pled guilty to possession with the intent to distribute ketamine and he was released pending sentencing. While awaiting sentencing, the Army Criminal Investigative Division and Defense Criminal Investigative Service received information that Custis was laundering money. The subsequent investigation revealed that Custis, acting in a leadership role involving co-defendant and others, laundered over $700,000.

On February 1, 2023, a second search warrant was executed at Custis's home and investigators recovered 28.5 kilograms of ketamine, $164,200 in cash, digital scales and vacuums sealing materials. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

Former New York City Correction Officer Pleads Guilty To $171,000+ Salary & Overtime Fraud Scheme - January 26, 2024

A former New York City Department of Correction (DOC) Officer James Internicola pleaded guilty to federal program fraud, admitting that he fraudulently obtained a significant amount of salary and overtime pay by lying about the hours he worked.

Internicola fraudulently obtained more than $171,000 in salary and overtime pay by lying about the hours he worked from at least July 2021 to January 2023. During this time, Internicola claimed to work large amounts of overtime nearly every week. In fact, based on license plate reader data, E-Z pass toll records and cell site location information, Internicola frequently showed up to work more than two hours late and left work several hours early. In many instances, Internicola claimed to be at work when he actually never showed up to Rikers Island at all, including when he was at his home on Staten Island, visiting the Jersey Shore or vacationing in Aruba. In total, Internicola claimed to have worked more than 2,250 hours more than he actually did in a period of approximately 18 months and he fraudulently received the equivalent of more than a year of his base salary. (Source)

Former Police Officer / Union President Pleads Guilty To $40,000 Overtime Fraud Scheme - January 26, 2024

Paul Helring is a former Scranton Police Officer and the former elected Police Union President. He pleaded guilty to the offense of Theft Concerning Programs Receiving Federal Funds.

Helring pleaded guilty and alleges that from approximately March 2021 to May 2022, while serving as the coordinator of Scranton Police Department's extra duty overtime program, Helring knowingly obtained by fraud over $5,000.00 in compensation that was paid to him for certain extra duty patrol shifts at local, Scranton-area, lower-income housing complexes that Helring claimed to work but did not in fact work.

Helring acknowledged that the monetary loss attributable to his conduct was between $15,000 and $40,000, and that he abused a position of public trust in a manner that significantly facilitated the commission of his offense. Helring also agreed to make restitution to the affected housing complexes in the amount of $17,831.40. (Source)

Police Officer Pleads Guilty To $13,000+ Overtime Fraud Scheme - January 12, 2024

Between January 2020 and January 2021, Jeffrey Peters and a fellow supervisor (Officer 1) devised a scheme to defraud the Shreveport Police Department (SPD) by claiming overtime for hours they had not worked. Peters and Officer 1 would each fill out and sign a Report of Overtime which stated they worked a specific time and date on the CBCR grant. Peters, in his role as Officer 1's supervisor, would certify that Officer 1 had actually worked the dates and times listed on the Report of Overtime.

Peters would also create and submit an SPD activity report which would falsely state that he and Officer 1 were doing patrols in District 3, an area around SPD Headquarters. On these reports, Peters and Officer 1 were the only officers listed. When in truth and in fact, neither Peters nor Officer 1 were working overtime for SPD.

Peters submitted false Reports of Overtime and Activity Reports on over 50 dates falsely claiming he worked overtime that he had not. He was paid for hours he did not work in is bi-weekly paychecks which were deposited into his own personal account. Peters received a total of $13,084.74 in overtime that he was not entitled to receive. (Source)

Corrections Officer Pleads Guilty To Taking $12,000 In Bribes In Exchange For Smuggling Contraband Into Prison - January 11, 2024

Quandelle Joseph became a Corrections Officers at the Metropolitan Detention Center (MDC) in Brooklyn, New York in May 2020.

During his employment, Joseph accepted tens of thousands of dollars from inmates in exchange for smuggling narcotics, cigarettes, and cell phones into the MDC. In one instance, Joseph entered a unit he was not guarding during a lockdown, opened an inmate's cell and provided him with contraband.

Several hours later, MDC staff smelled marijuana in that inmate's cell and recovered a contraband cell phone during a search of the cell; Joseph was to be paid $12,000 from this inmate for bringing in contraband. Joseph also accepted bribes to smuggle contraband into the MDC to another inmate, who then sold the contraband widely throughout his unit. Joseph also warned the inmate about upcoming contraband searches at the MDC. For example, on January 26, 2021, Joseph texted an inmate from whom he was taking bribes: "Tighten up search comin clean phones out call logs n text n try to stash it." The next day, Joseph texted the inmate: "keep your phones cleannnnnnnnn erase texts and call logs every night." (Source)

U.S. Customs & Border Protection Officer Charged With Stealing $2,000+ From Airline Passenger - January 10, 2024

William Timothy is a U.S. Customs and Border Protection Officer (CBP).

An international airline passenger reported that more than $2,000 in cash was missing after it had been inspected by a CBP officer at Naples Airport. An investigation was undertaken by agents from CBP's Office of Professional Responsibility. During the investigation, surveillance video was examined which showed Timothy hiding and taking approximately 22 bills of U.S. currency belonging to the airline passenger during a border enforcement examination in May 2023. (Source)

STATE / CITY GOVERNMENTS / MAYORS

State Unemployment Insurance Examiner Sentenced To Prison For Stealing $583,000+ Of Unemployment Insurance Benefits - January 18, 2024

Shortly after Autumn Mims began working with the Michigan Unemployment Insurance Agency in August 2020, she began using her insider access to fraudulently process claims in the names of third parties without their knowledge or authorization. Mims had help from William Haynes.

As part of the scheme, Mims and / or Haynes (1) altered direct deposit information for third-party unemployment insurance assistance; (2) accessed third-party unemployment insurance assistance claim information without authorization; (3) completed false and fraudulent certifications for third-party unemployment insurance assistance benefits; (4) opened unauthorized bank accounts in the names of third

parties; (5) conducted cash withdrawals of unemployment insurance assistance issued in the names of third parties; and (6) conducted financial transactions utilizing unemployment insurance assistance funds issued in the names of third parties.

Mims also admitted that while she was working with the MUIA and executing her fraud, she was also fraudulently obtaining unemployment insurance benefits for herself by falsely claiming that she was unemployed. Mims was also ordered to pay $583,409 in restitution. (Source)

Former County Master Commissioner / Court Appointed Trustee Sentenced To Prison For Scheme To Steal $435,000+ From 2 Trusts - January 8, 2024

John Schmidt is an attorney and the Former Bullitt County Master Commissioner. He was sentenced to 2 years and 11 months in prison, followed by a 3-year term of supervised release, with a special condition of 100 hours of community service, for one count of wire fraud and two counts of bank fraud.

The charges in this case were in connection with Schmidt's scheme to steal over $435,000 while he was serving as the court appointed trustee for two trusts, the beneficiaries of which relied on Schmidt to manage the trusts' assets.

As part of his scheme, Schmidt stole from the trusts to pay for his own personal expenditures, including to pay debts he incurred to individuals he had represented or purported to represent in the course of his legal practice and to replace missing funds from the Bullitt County Master Commissioner bank account. (Source)

County Social Worker Pleads Guilty To Role In $400,000+ Medicaid Fraudulent Billing Scheme - January 24, 2024

Felicia Jones was a Social Worker in New Hanover County in North Carolina.

Jones conspired with a licensed mental health counselor, Lakia Washington, to defraud Medicaid. Jones used her government employment to obtain personally identifying information (PII) of New Hanover County residents enrolled in Medicaid, including their Medicaid ID numbers. In exchange for an agreed-upon fee per beneficiary, Jones then provided the PII to Washington, knowing it would be used to generate fraudulent claims for services never rendered. Investigators have attributed over $400,000 of Washington's fraudulent Medicaid billing to the beneficiary PII Jones provided to Washington. Late last year, Washington pled guilty and is awaiting sentencing. Based upon the investigation, no out-of-pocket costs were borne by the individuals whose identities were used as a part of the scheme. (Source)

County Employee Pleads Guilty To Stealing $122,000+ Of Government Funds To Pay Down His Line Of Credit- January 11, 2024

John T. Cox, age 61, of Schenectady, New York, pled guilty today to mail fraud and stealing money from a federally funded governmental agency.

John Cox admitted that between June 2017 and February 2023, while employed as a Budget Analyst in the Albany County Sheriff's Office (ACSO), he stole $122,251.25 by issuing 16 fraudulent checks drawn on funds in the care of the ACSO, an agency that received more than $10,000 in federal funding each year during this time period.

Cox used the checks to pay himself directly or to pay down his line of credit.

Cox then tried to cover up his fraud by falsifying ACSO records to suggest that the funds were being used for legitimate purposes such as vehicle and equipment purchases. Cox stole some of the money from a Department of Justice program in which the federal government shares the proceeds of federal asset forfeitures with state and local law enforcement agencies. (Source)

Former City Clerk Pleads Guilty To $68,000 Fraud Scheme / Used Funds For Personal Expenses & To Buy Motorcycle - January 18, 2024

A former City Clerk for Merriam Woods, Missouri pleaded guilty in federal court to a $68,000 scheme to defraud the city.

As a part of her scheme, Breanna Gamble used the city's credit cards and bank accounts to make personal purchases on numerous occasions, without authorization from the city, including purchases from Amazon, Victoria's Secret, Walmart, PFI, Buckle, American Eagle, H&M, Ticketmaster, Reliable Chevrolet, Springfield Power Sports, Lululemon, and Ulta.

Gamble admitted that she forged a signature on a $5,500 city check that was used to purchase a motorcycle for her personal use.

In order to conceal her scheme and her use of the city's funds, Gamble recorded false financial entries and false invoices. Gamble also made misrepresentations to the city's mayor and board of aldermen, and failed to cooperate with a company hired by the city to conduct a financial audit of the city's finances. (Source)

Former Mayor Pleads Guility To Stealing $38,000+ For Personal Benefit - January 18, 2024

Shedrick Johnson was charged with devising a wire fraud scheme beginning on March 23, 2020, and continuing to November 30, 2022, in which he exceeded his authorized access by withdrawing funds belonging to Plum Springs, Kentucky, and utilizing for his personal benefit and conducting unauthorized transactions with the Plum Springs debit card with the total amount of loss being approximately $38,168.96. (Source)

Puerto Rico Legislator & Husband Convicted For Theft, Bribery & Kickback Scheme - January 12, 2024

From early 2017 until July 2020, María Milagros Charbonier-Laureano, also known as Tata, a member of the Puerto Rico House of Representatives, along with her husband, Orlando Montes-Rivera, and her assistant, Frances Acevedo-Ceballos, executed a scheme to defraud the Commonwealth of Puerto Rico by engaging in a theft, bribery, and kickback scheme.

Over the course of the scheme, Charbonier-Laureano inflated Acevedo-Ceballos's salary from $800 on a bi-weekly, after-tax basis to nearly $2,900. Out of every inflated paycheck, it was agreed that Acevedo-Ceballos would keep a portion, and kick back between $1,000 and $1,500 to Charbonier-Laureano and Montes-Rivera.

After learning of the investigation into illegal activities in her office and of a warrant that had been obtained for one of her phones, Charbonier-Laureano proceeded to delete certain data on the phone. In particular, Charbonier-Laureano deleted nearly the entire call log, nearly all WhatsApp messages, and nearly all iMessages associated with the phone. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

Former School Principal Sentenced To Prison For Misusing Nearly $40,000 In School Funds For Vacations With Friends - August 1, 2023

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

Wilson has been charged with one count of wire fraud for allegedly engaging in a scheme to defraud Boston Public Schools of approximately $38,806 by misusing school funds for her own personal use.

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

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

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

No Incidents To Report

BANKING / FINANCIAL INSTITUTIONS

Georgia Bankers Association Accountant Sentenced To Prison For Embezzling $700,000 For 7 Years - January 3, 2024

Gino Lassiter has been sentenced to prison for embezzling approximately $700,000 from the Georgia Bankers Association (GBA) and Georgia Bankers Association Trust (GBA Trust) between 2014 and 2021.

Lassiter, who had been previously convicted for federal bank fraud in the mid-1990s, served as the GBA's accountant from May 1998 to March 2021. For approximately seven years, Lassiter embezzled hundreds of thousands of dollars from the GBA and GBA Trust by using a GBA-issued credit card to make improper and unauthorized purchases.

As the GBA's accountant, Lassiter was able to conceal his embezzlement in a variety of ways, including by making fictious entries, misrepresenting the nature of payments, and overstating the number of payments in the GBA's general ledger.

For example, Lassiter would record in the ledger overinflated payments that supposedly reflected other employees' legitimate credit card expenditures. In actuality, the amount would be the exact same amount that Lassiter embezzled over a given period.

Lassiter was also able to conceal his scheme by over inflating invoices that GBA issued to the GBA Trust. This was possible because the GBA was responsible for paying off the credit card expenses of the GBA Trust's employees. The GBA Trust would in turn reimburse the GBA for these expenses. Lassiter inflated these invoices by the amount of his fraudulent credit card purchases. (Source)

Former Credit Union Employee Sentenced To Prison For Embezzling $325,000+ - January 16, 2024
Tracy Mikulencak embezzled approximately $144,000 from her teller drawer and the vault while working at A+ Federal Credit Union.

Auditors also revealed that Mikulencak had made unauthorized withdrawals from customer accounts, including a deceased account holder. In total, Mikulencak embezzled $325,708 from the credit union. In addition to her imprisonment, Mikulencak was also ordered to pay $302,668 in restitution. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION
United Health Group Accuses 2 Former Executives Of Stealing Trade Secrets - January 3 2024
UnitedHealth Group is suing a group of corporate entities founded by two of its former executives after they allegedly stole and used confidential information from the company to create their own competing product for diabetes management.

The lawsuit was filed Dec. 28 in a Minnesota federal court against Ken Ehlert, UnitedHealth's former Chief Scientific Officer, and Mark Pollmann, former Chief Technology Officer at Optum Labs, who both departed the company in 2021.

The suit claims the two former employees took 500,000 emails and files on a UnitedHealth hard drive that held confidential information and trade secrets, including internal growth plans, board meeting minutes, contract negotiation details, financial statements and potential acquisition targets.

The defendants then allegedly created a group of corporate entities, including shell companies, using the confidential information.

UnitedHealth claims the individuals violated the noncompete and confidentiality clauses of their employment contracts, including sharing, using and failing to return the company's confidential information.

UnitedHealth also claims the former employees purposefully "tried to cover their tracks" by erasing or altering incriminating information.

The relationship between the former executives and UnitedHealth dates to at least 2017, when they sold research and development company Savvysherpa to UnitedHealth for $46.8 million and became employees of the company.

Mr. Ehlert and Mr. Pollmann sued UnitedHealth in 2022, alleging that when they were terminated, the company wanted them to sign separation agreements that would release them of their equity claims in Level2, a diabetes management platform they said was developed by Savvysherpa. The case closed in December 2022 and neither party disclosed the outcome of the case.

The relationship between the former executives and UnitedHealth dates to at least 2017, when they sold research and development company Savvysherpa to UnitedHealth for $46.8 million and became employees of the company.

Mr. Ehlert and Mr. Pollmann sued UnitedHealth in 2022, alleging that when they were terminated, the company wanted them to sign separation agreements that would release them of their equity claims in Level2, a diabetes management platform they said was developed by Savvysherpa. The case closed in December 2022 and neither party disclosed the outcome of the case. (Source)

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

No Incidents To Report

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

2 Surgical Sales Representatives Plead Guilty To $850,000 Of Fraud Involving Veterans Administration Medical Center / Received $80,000 In Bribes - January 25, 2024

Eric Smith and Landon Chester worked as a surgical sales representative for an independent distributor of a nationwide orthopedic company that manufactured replacement joints and products used during surgeries in which those joints were implanted. Both routinely sold products to the James H. Quillen VA Medical Center in Mountain Home, Tennessee.

In June 2018, Chester and Smith formed a separate company and began selling their own acquired inventory to the VA at inflated prices or when not necessary, resulting in losses to the VA in excess of $850,000. Chester and Smith agreed that they conspired and paid cash bribes of more than $80,000 to two VA Medical Center employees (indicted separately) for their agreement to commit, collude, and aid in the fraud against the VA. (Source)

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

Bookkeeper For Funeral Service Company Charged With Embezzling $500,000+ For 8 Years - January 5, 2024

LaSaundra Simmons worked as the Bookkeeper for Farwell Funeral Service, Inc. for several years.

Starting in 2015, and continuing until it was discovered in January 2023, Simmons employed a scheme to embezzle funds from the company. On more than 100 occasions, she either made unauthorized wire transfers of funds from the funeral home's bank account to her own account, or drafted unauthorized checks which she deposited by electronic wire transfer into her own account.

She would often describe these checks as "commissions" or "consulting fees." She embezzled more than $500,000 over the course of the scheme. (Source)

Former Hotel General Manager Stole $150,000 - January 19, 2024

Angelique Patterson a hotel where she was employed as Assistant General Manager.

From March through at least October of 2023, Angelique Patterson manipulated the hotel's reservation system and altered the records of customers who had paid using cash or credit cards. Patterson changed those reservations to falsely show that the customers had used the hotel's loyalty rewards system "points" to pay for their stay. Patterson then added her own credit or debit card information into the system and had the customers' payments "refunded" to her.

Patterson fraudulently refunded to herself a total of about $153,518 during the course of her scheme, the indictment says. On Oct. 4, 2023, although not on duty, Patterson tried to use the hotel's desk computer and a coworker's credentials to fraudulently refund herself an additional $61,998, the indictment says. (Source)

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

Company Accountant Pleads Guilty To Stealing $500,000 From Employer To Pay Her Credit Cards / Personal Expenses- January 10, 2024

Tammy Myers was employed by Builders Overhead Door Service, Inc. from 1998 through 2022. Myers became the head of accounting in 2012.

Myers admitted that she engaged in a scheme to defraud Builders Overhead Door Service from January 2013 to December 2022. Myers admitted she used the company's bank account information to pay off the balances on her personal credit cards, totaling $429,025.

Myers admitted she also wrote checks to herself from the company's bank account without the authorization of the owner. Myers deposited the unauthorized checks, which had been pre-signed by the owner, into her personal bank account and spent that money on personal expenses. The total amount of unauthorized checks she wrote to herself was $86,477. (Source)

Office Manager Charged With Stealing $400,000+ From Company For Personal Expenses - January 5, 2024

From September 2019 to February 2023, Nichole Lawrence used her position as an Office Manager to unlawfully obtain funds and services totaling over $400,000 from her employer. By accessing the company's bank account, Lawrence scheduled electronic payments for her personal expenses that had been charged to various accounts and charge cards. She also used a stamp with the signature of the company's general manager to issue unauthorized company checks to herself. (Source)

Former Employee & Co-Conspirator Sentenced To Prison For Embezzling $270,000+ For Personal Expenses - January 16, 2024

Alicia Wilson and Mindi Madison conspired together to embezzle funds from WFYI Public Media into their personal checking accounts.

Madison began working as an Accounting Specialist for WFYI in January 2018. WFYI was owned and operated by Metropolitan Indianapolis Public Media, Inc., and provided television and radio programming throughout Central Indiana.

Madison's co-conspirator, Wilson, was neither an employee nor a vendor of WFYI.

As an Accounting Specialist, Madison had access to WFYI's accounting software, and was trusted to present legitimate expenses, claims, invoices, and supporting documentation along with the unsigned WFYI checks to employees at WFYI who had signature authority for their approval and signature.

Instead of presenting legitimate claims that arose out of WFYI's legitimate business expenses for signature and payment, Madison abused her position of trust, and presented at least 156 fake claims and invoices for payment. In effort to conceal the theft from WFYI and their banking institutions, Madison and Wilson agreed that Madison would falsify invoices using versions of Wilson's name and businesses connected to her.

Madison tendered WFYI checks to Wilson, and they agreed that Wilson would then deposit the checks into her bank accounts. Wilson then withdrew Madison's portion in cash, and they split the illegal proceeds. Both Madison and Wilson used WFYI's stolen funds for their own personal expenditures including but not limited to, rent, restaurants, groceries, fuel, and utilities.

In total, the pair embezzled approximately $270,876 from WFYI before the theft was discovered. Wilson's participation in the scheme made it virtually impossible for WFYI to detect the theft.
(Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

Former Company General Manager Sentenced To Prison For $1.2 Million+ Fake Invoice Scheme - January 18, 2024

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

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

Former Hospital Chief Operating Officer Pleads Guilty To $620,000+ Fake Invoice Scheme For 8 Years - January 22, 2024

Robert Spadoni was an attorney who worked as a Vice President and COO of an Illinois hospital.

Spadoni admitted in a plea agreement that from 2013 to 2021, he orchestrated a scheme in which he approved the hospital's payment of invoices to a vendor company that purportedly provided administrative support and compliance services. In reality, the vendor company Medical Education Solutions, Inc. had been established by Spadoni for the purpose of executing the scheme. Spadoni opened a bank account for the company in a relative's name and steered the hospital's payments into it. Spadoni concealed the fraud scheme by paying $1,500 a month in cash to another hospital employee to actually provide the administrative and compliance services.

As a result of the fraud scheme, Spadoni obtained approximately $622,500 in payments from the hospital, the plea agreement states. Spadoni admitted in the plea agreement that he used the money for his own benefit, including restaurant meals and hotel stays, as well as transferring $225,805 into his 401(k) account. (Source)

Systems Engineer Pleads Guilty To Embezzling $526,000+ Using Shell Company & Fake Invoices Scheme - January 10, 2024

Scott Richard was a Systems Engineer for his company.

Richard admitted to fraudulently using the corporate credit card issued to him by his company, for his own personal benefit. Richard embezzled money from his employer by creating false invoices for a shell company he controlled, and using his corporate card to make fraudulent purchases from the shell company.

Richard also made unauthorized purchases of equipment, for his own personal use, with his corporate card. From January 1, 2012 through September 27, 2021, Richard fraudulently diverted $526,569.42 from his company to himself. (Source)

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

No Incidents To Report

THEFT OF ORGANIZATIONS ASSESTS

Information Technology Professional Pleads Guilty To Ordering / Then Selling $535,000+ Worth Of Stolen MacBooks - January 29, 2024

Andrew Halvorsen worked as the Senior Director of Information Technology for a cloud-based machine data analytics company. In his role at the company, Halvorsen was responsible for ordering Apple MacBooks for company employees.

In November 2019, Halvorsen began stealing MacBooks that he ordered and sold for cash to an individual who, in turn, resold and shipped them to buyers outside the state of California. In total, Halvorsen stole and sold at least 141 MacBooks. The cost to his employer of those MacBooks was over $535,000. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

No Incidents To Report

EMPLOYEE DRUG RELATED INCIDENTS

Former Hospital Nurse Arrested For Distribution Of Morphine That Resulted In Patient Death - January 19, 2024

Catherine Worman allegedly distributed and dispensed morphine on June 5, 2023, resulting in the death of one person. Worman was employed as a nurse at a local hospital at the time of the offense.

Worman also distributed and dispensed morphine to at least one other person. During the investigation into the death of victim one, Draper Police officers learned from another victim that Worman intravenously administered morphine to him without a prescription. According to the victim, he became extremely ill because of the morphine administered by Worman and feared for his life. Additional information extracted from Worman's cell phone reveals she was unlawfully obtaining Adderall prescribed for others and trading it. Worman was also illegally obtaining prescription medications from another healthcare worker with whom she was romantically involved. (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'

Employee Kills Co-Worker By Beating Him To Death & Leaving His Body In Warehouse - January 17, 2024

Nathan Evans was arrested for the death of his co-worker at a Salt Lake City storage facility. Evans is accused of beating the man to death and leaving his body in a back office of the warehouse.

The man who died was identified as David Hinkebein.

A witness told officials they had not seen Hinkebein at work and questioned Evans where their co-worker was after seeing bloody handprints on the wall and carpet in a back office of the storage facility on January 1, documents state.

Evans told the other coworker Hinkebein "was fine," and was not questioned further as he "did not want to talk and seemed defensive about it".

The next day the co-worker went back to work, saw the blood was still not cleaned up and once again questioned Evans where Hinkebein was. According to court documents, "He's done," was the response Evans gave the concerned co-worker, who took the statement as meaning Hinkebein was dead.

Police responded to the area and found the body of Hinkebein, as well as a hammer covered in blood and a black garbage bag filled with bloody clothes, arresting documents state.

The Utah State Medical Examiner's Office found at least 15 sharp / blunt force injuries to Hinkebein's head consistent with a hammer and three sharp force injuries to the neck and throat. It was determined that Hinkebein's death was caused by blunt force injuries to the head.

During the investigation, police spoke to a driver who picked up Evans right before the alleged homicide, in which he heard Evans say, "he was going down to a warehouse and was going to kill a guy down there by bashing his head in".

While a motive has yet to be determined, documents state the driver heard Evans say he was going to kill someone because "the guy messed with his stuff and the male did not like the way he was being treated". (Source)

Employee Who Was On Administrative Leave Charged In Gun Attack At Facility - January 3, 2024

An employee who was being administratively disciplined at one of Athens largest medical manufacturing facilities is in jail on charges that he unloaded a barrage of gunfire on the facility on New Year's Day.

Athens-Clarke police charged Zachariah Best with trespassing and felony damage to property after police said the shooting caused an estimated $12,800 in damage. No one was injured in the shooting, which occurred about 5:30 am.

Security video revealed a black Toyota Tacoma arrive and a man attempt to scan his way through the entrance gate, but his code was declined and he was denied access, police said. However, the scan attempt aided police in identifying the shooter as Best, according to the report.

The officer said it was explained to him that Best was on administrative leave, but facility security was uncertain about the details except that it was for work-related reasons.

Best allegedly made comments at the workplace that made other employees feel uncomfortable enough to report what they heard, according to the report. (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 Guilty 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