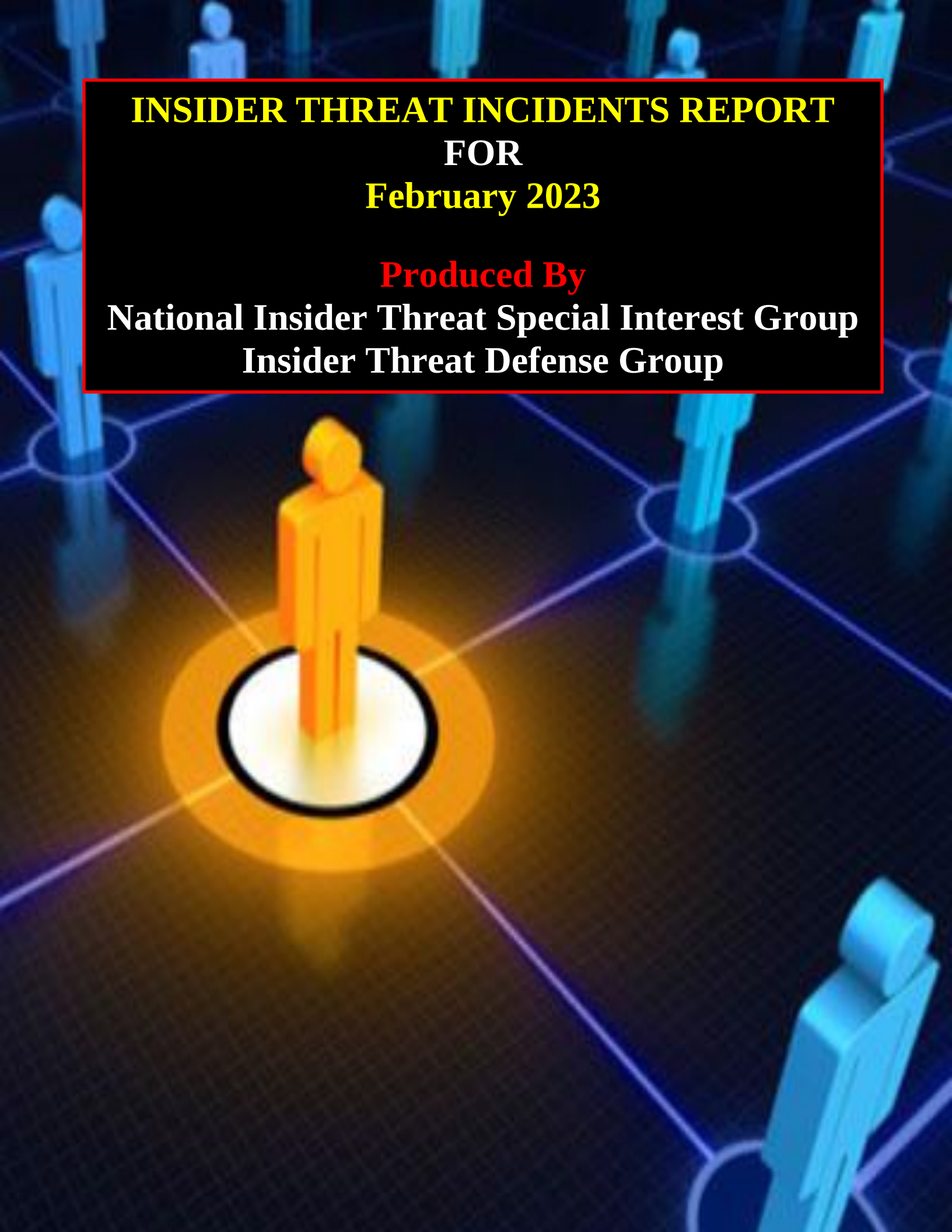


INSIDER THREAT INCIDENTS REPORT
FOR
February 2023

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

INSIDER THREAT INCIDENTS

A Very Costly And Damaging Problem

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

The National Insider Threat Special Interest Group (NITSIG) in conjunction with the Insider Threat Defense Group (ITDG) have conducted extensive research on the Insider Threat problem for 10+ years. This research has evaluated and analyzed over **4,300+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations and businesses of all sizes.

The NITSIG and ITDG maintain the largest public repositories of Insider Threat incidents, and receive a great deal of praise for publishing these incidents on a monthly basis to our various websites. This research provides interested individuals with a "***Real World***" view of the how extensive the Insider Threat problem is.

The traditional norm or mindset that Malicious Insiders just steal classified information, an organizations data, trade secrets or other sensitive information, is no longer the case. Over the years there has been a drastic increase in financial fraud and embezzlement committed by employees.

According to the Association of Certified Fraud Examiners 2022 Report to the Nations, organizations with less than 100 employees suffered larger median losses than those of larger companies.

To grasp the magnitude of the Insider Threat problem, one most look beyond Insider Threat surveys, reports and other sources that all define Insider Threats differently. How Insider Threats are defined and reported is not standardized, so this leads to significant underreporting on the Insider Threat problem.

Another problem is how surveys and reports are written on the Insider Threat problem. Some simply cite percentages of how they have increased and the associated remediation costs over the previous year. In many cases these surveys and reports only focus on the technical aspects of an Insider stealing data from an organization, and leave out many other types of Insider Threats. Surveys and reports that are limited in their scope of reporting do not give the reader a comprehensive view of the "***Actual Malicious Actions***" employees are taking against their employers.

If you are looking to gain support from your CEO and C-Suite for detecting and mitigating Insider Threats, and want to provide them with the justification, return on investment, and funding ($$$) needed for developing, implementing and managing an ITP, the incidents listed on pages 5 to 20 of this report should help. The cost of doing nothing, may be greater then the cost of implementing a comprehensive Insider Threat Mitigation Framework.

DEFINITIONS OF INSIDER THREATS

The definition of Insider Threats can be vast, and must go beyond current definitions (By Sources Such As: National Insider Threat Policy, NISPOM CC2 & Other Sources) and be expanded.

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

TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH

- ☐ Non-Malicious But Damaging Insiders (Un-Trained, Careless, Negligent, Opportunist, Job Jumpers, Etc.)
- ☐ Disgruntled Employees Transforming To Insider Threats
- ☐ Theft Of Organizations Assets (Physical, Etc.)
- ☐ Theft / Disclosure Of Classified Information (Espionage), Trade Secrets, Intellectual Property, Research / Sensitive - Confidential Information
- ☐ Stealing Personal Identifiable Information For The Purposes Of Bank / Credit Card Fraud
- ☐ Financial / Bank / Wire / Credit Card Fraud, Embezzlement, Theft Of Money, Money Laundering, Overtime Fraud, Contracting Fraud, Creating Fake Shell Companies To Bill Employer With Fake Invoices
- ☐ Employees Involved In Bribery, Kickbacks, Blackmail, Extortion
- ☐ Data, Computer & Network Sabotage / Misuse
- ☐ Employees Working Remotely Holding 2 Jobs In Violation Of Company Policy
- ☐ Employees Involved In Viewing / Distribution Of Child Pornography And Sexual Exploitation
- ☐ Employee Collusion With Other Employees, Employee Collusion With External Accomplices / Foreign Nations, Cyber Criminal - Insider Threat Collusion
- ☐ Trusted Business Partner Corruption / Fraud
- ☐ Workplace Violence(WPV) (Bullying, Sexual Harassment Transforms To WPV, Murder)
- ☐ Divided Loyalty Or Allegiance To U.S. / Terrorism
- ☐ Geopolitical Risks (Employee Loyalty To Company Vs. Country Because Of U.S. - Foreign Nation Conflicts)

ORGANIZATIONS IMPACTED

TYPES OF ORGANIIZATIONS THAT HAVE EXPERIENCED INSIDER THREAT INCIDENTS

- ☐ U.S. Government, State / City Governments
- ☐ Department of Defense, Intelligence Community Agencies, Defense Industrial Base Contractors
- ☐ Critical Infrastructure Providers
  - Public Water / Energy Providers / Dams
  - Transportation, Railways, Maritime, Airports, Aviation / Airline Industry (Pilots, Flight Attendants)
  - Health Care Industry, Medical Providers (Doctors, Nurses, Management), Hospitals, Senior Living Facilities, Pharmaceutical Industry
  - Banking / Financial Institutions
  - Food & Agriculture
  - Emergency Services
  - Manufacturing / Chemical / Communications
- ☐ Law Enforcement / Prisons
- ☐ Large / Small Businesses
- ☐ Defense Contractors
- ☐ Schools, Universities, Research Institutes
- ☐ Non-Profits Organizations, Churches, etc.
- ☐ Labor Unions (Union Presidents / Officials)
- ☐ And Others

INSIDER THREAT DAMAGES / IMPACTS

The Damages From An Insider Threat Incident Can Many:

Financial Loss

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

Operational Impact / Ability Of The Business To Execute Its Mission

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

Reputation Impact

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

Workplace Culture - Impact On Employees

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

Legal & Liability Impacts (External Costs)

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

INSIDER THREAT INCIDENTS
FOR FEBRUARY 2023

FOREIGN GOVERNMENT INSIDER THREAT INCIDENTS
No Incidents To Report

U.S. GOVERNMENT
Former Arkansas State Senator Sentenced To Prison For Stealing $10,000+ In Campaign Funds / Accepting Bribes - February 3, 2023

Jeremy Hutchinson is a former Arkansas State Senator.

From 2010 through 2017, Hutchinson stole and misappropriated thousands of dollars in state campaign contributions for his own personal use and then filed false federal income tax returns from 2011 to 2014 to conceal his conduct.

Hutchinson was hired as outside counsel by Dr. Benjamin Burris, an Orthodontist who owned and operated orthodontic clinics throughout the state of Arkansas. In exchange for payments and legal work, Hutchinson pushed legislation beneficial to Burris. Hutchinson was provided legal work to conceal the corrupt nature of his arrangement. Hutchinson stole over $10,000 in state campaign funds for his own personal use and also falsified his 2011 tax returns, including failing to report $20,000-per-month-payments he received from one law firm and other sources of income he knowingly and intentionally concealed from his taxes. (Source)

Former Puerto Rico Legislator Sentenced To Prison For Theft Of $81,000+ Of Government Funds - February 23, 2023

Between April 2018 and September 2020, Nestor Alonso-Vega authorized several salary adjustments for his assistant. It was agreed that his assistant would kickback to Alonso-Vega half of the total amount of the pay raise, split between each pay day. The total loss for the House of Representatives was $81,500, of which defendant received more than $40,000.

It was further alleged that the assistant, who testified during the trial, used a variety of means to transfer the kickbacks to Alonso-Vega. For example, he made withdrawals around the time he received his paycheck and paid Alonso-Vega in cash, and, at times, made payments to Alonso-Vega's Home Depot account. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY
Hundreds Of Classified Documents Found In Home Of Retired Air Force Officer - January 30, 2023

This investigation dates back to January 24, 2017 when the Air Force's Office of Special Investigations (AFOSI) received information indicating that Robert Birchum had been storing classified information on a thumb drive at his home in Tampa, Florida.

Birchum will make an Initial Appearance and Change of Plea Hearing that us is set for February 21, 2023 in Tampa, Florida.

A search of his home found a thumb drive containing 135 files that were marked as containing Top Secret, Top Secret / ACCM, Secret, and / or Confidential classified information. Some of the documents contained information discussing the NSA's collection of information and that their unauthorized release could be expected to cause exceptionally grave damage to the national security of the United States.

During the search, officers also seized the hard drive of a Dell computer and found more files containing information marked as secret as well as 48 paper documents. Another search found a hard drive from temporary quarters overseas, that revealed 117 additional files containing classified national defense information. A final search of a storage pod at Birchum's home in Tampa, found 28 paper documents marked as Secret.

Birchum served on active duty as a Commissioned Officer in the United States Air Force from May 1986 to July 2018, when he retired at the rank of Lieutenant Colonel. (Source)

CRITICAL INFRASTRUCTURE

Church Employee Sentenced To Prison For Stealing $570,000 Over 13 Years / Used Money For Gambling & Vacations - February 16, 2023

Marie Carson was the sole staff member responsible for processing checks received from parishioners, and for conducting financial transactions on behalf of the church and school, for over a decade. From 2008 to 2021, she illegally transferred at least $573,836.59.

Carson transfered nearly $574,000 from the Catholic Church and its associated school to her personal accounts for gambling and month-long vacations. The Department of Justice (DOJ)
said the actual monetary loss is likely to be much higher, as Carson admitted to church officials she began her scheme in 2004

The theft was exposed in November 2021 when Carson was on leave from her position, and her temporary replacement noticed suspicious transfers from the parish's gaming account to an external bank account, according to the DOJ. Further investigation into the transactions led to the discovery of over $289,000 moved into multiple accounts, including a phantom account in the church's name.

Carson was reportedly able to maintain the scheme for so long because she was making false entries into a database used by the parish to track payments. (Source)

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

Former FBI Special Agent Sentenced To Prison For Accepting Bribes Paid by Attorney Linked to Organized Crime Figure - February 27, 2023

Babak Broumand was an FBI special agent from January 1999 until shortly after search warrants were served on his home and businesses in 2018. He was responsible for national security investigations and was assigned to the FBI Field Office in San Francisco.

Broumand accepted $150,000 in cash bribes and other items of alue in exchange for providing sensitive law enforcement information to a corrupt lawyer with ties to Armenian organized crime.

From January 2015 to December 2018, Broumand accepted cash, checks, private jet flights, a Ducati motorcycle, hotel stays, escorts, meals, and other items of value from the organized crime linked lawyer.

In return for the bribe payments and other items of value, Broumand conducted law enforcement database inquiries and used those inquiries to help the lawyer and his associates avoid prosecution and law enforcement monitoring. (Source)

STATE / CITY GOVERNMENTS / MAYORS

Former Township Official Sentenced To Prison For Embezzling $150,000 Over 8 Years - February 23, 2023

Linda Baun was formerly employed as the Secretary / Treasurer for Jackson Township, in Mercer County, in Pittsburgh, Florida.

Between 2011 and 2019, she embezzled at least $150,000 from the Township by making unauthorized ATM withdrawals and by charging personal purchases on Amazon to the Township's debit card. (Source)

Former City Building Inspector Found Guilty Of Facilitating $50,000 Bribery Scheme - February 28, 2023

Between February to April of 2018, Lester Crowder met nine times with an individual who said he was looking to open a nightclub.

In those meetings, Crowder communicated that the individual would need to pay up to $50,000 in cash bribes in order to obtain the nightclub property and obtain the necessary permits.
Crowder collected approximately $13,000 in bribe payments from the individual, who was cooperating with the FBI and recording their conversations. During the same time, Crowder was captured on court-authorized recordings communicating with another individual confirming their intent to take bribes. (Source)

Former Puerto Rico Senator / Mayor Senced To Prison For The Misappropriation Of $50,000 Of Municipal Funds To Finance His 2016 Senatorial Campaign - February 10, 2023

Abel Nazario-Quiñones is the former Puerto Rico (PR) Senator and Mayor of the municipality of Yauco.,

According to court documents, in August 2016, during a routine audit of the municipality's records, the PR Comptroller's Office discovered that there were irregular employees paid by the municipality of Yauco who either never showed up for work or showed up sporadically. The subsequent investigation by the FBI resulted in the indictment of Nazario-Quiñones. On September 30, 2022, he pleaded guilty to conspiring with others to misappropriate municipal funds.

Nazario-Quiñones admitted that from 2014 through 2016, he conspired and agreed with co-defendants [2] Edwin Torres-Gutierrez and [3] Claribel Rodríguez-Canchani that co-defendants [4] Humberto Pagán-Sánchez, [5] Kelvin Ortiz-Vegarra, [6] Ramón Martes-Negrón, [7] Juan Rosario-Núñez, and [8] Eric Rondón-Rodríguez would be hired, on paper, as employees of the municipality and paid from municipal funds knowing that they would not actually work for the municipality but would, instead, work on Nazario-Quiñones' 2016 senatorial campaign. In total, $50,426.00 in municipal funds were paid for the benefit of Nazario-Quiñones' campaign.(Source)

Puerto Rico Mayor Pleads Guilty For $32,000 Accepting In Bribes To Award Contracts - February 10, 2023

The former Mayor of Aguas Buenas, Puerto Rico, Javier García-Pérez, pleaded guilty today to one count of conspiracy for his involvement in a bribery scheme in which he received cash payments in exchange for the awarding of municipal contracts and the payment of invoices related on those contracts.

García-Pérez was involved in the bribery conspiracy from 2017 through 2021, in he received and accepted cash payments from two businessmen in exchange for awarding municipal contracts for waste disposal services, asphalt and paving services, and debris removal and paying outstanding invoices on the contracts.

García-Pérez received at least $32,000 in cash payments from August 2020 through September 2021 from the two businessmen. (Source)

New York City Housing Authority (NYCHA) Superintendents Sentenced To Prison For Accepting Bribes - February 9, 2023

In February 2020, Leroy Gibbs was employed as the Resident Buildings Superintendent at Douglass Houses in New York, New York.

Gibbs solicited and accepted approximately $2,000 in bribes from a confidential informant (CI) in exchange for awarding no-bid contracts to the CI worth a total of approximately $9,950 from NYCHA for work at that NYCHA facility.

Between July 2021 and August 2022, Julio Figueroa was employed as the Assistant Resident Buildings Superintendent in the Bronx, New York

Figueroa solicited and accepted approximately $6,000 in bribes from the CI in exchange for awarding no-bid contracts to the CI worth a total of approximately $46,622 from NYCHA for work at that NYCHA facility. Figueroa continued to solicit bribes even after learning about the arrests of nine NYCHA contractors in September 2021 for paying bribes, telling the CI that he hoped he would not be the subject of an undercover investigation and that he would probably only deal with the CI from then on because the news of the arrests scared him. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

Former School Bookkeeper Sentenced To Prison For Stealing $975,000 / Used Money For Personal Expenditures / Gambling - February 28, 2023

Carla Burke served as the Anderson Community School Corporation (ACSC) Food Service Department's Bookkeeper since 2007. As part of her employment duties, Burke maintained the financial records, bank account, and vendor invoices for the Food Service Department, and generated checks in the name of the Department for payments to vendors.

From January 1, 2014, to June 30, 2019, Burke issued checks in the name of ACSC Food Service to herself as the payee and then cashed the checks at her personal bank. Burke falsified records by recording that the payee was a vendor, rather than herself. Burke then cashed the checks and used the money for her own personal expenditures, including gambling.

The scheme was uncovered during a routine, scheduled Indiana State Board of Accounts (SBOA) audit. SBOA conducted a disbursement of funds test and found missing documentation. In total, Burke cleared approximately 312 fraudulent checks totaling $976,773.29 in losses to ACSC. (Source)

School District Bookkeeper Pleads Guilty To Stealing $130,000+ / Used Funds To Pay Student Loans & Credit Cards - February 23, 2023

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

Burley used her access at Barnstead School District to alter her payroll information, make student loan payments and payments to personal creditors, and pay for an Amazon account charged to Barnstead but controlled by Burley, totaling $110,295.26.

Following her termination from Barnstead, Burley was hired as a Bookkeeper at Hampton School District, where she used her position to use district funds to pay student loans and credit cards belonging to her or her family members, totaling $20,966.52. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

Former Church Business Manager Pleads Guilty To Using Church Credit For $1.5 Million+ For Personal Expenses - February 27, 2023

From 2014 through 2021, David Apps, was the Business Manager of Broad Street United Methodist Church in Cleveland, Tennessee.

Apps devised a scheme in which he used an official church credit card to pay for personal expenses in excess of $1.5 million dollars. Some of these expenses included payment for personal travel, automobiles, medical bills for family members, boat / watercraft and marina fees, and firearms, none of which was related to church business.

Apps also wrote checks to himself under the guise of church member donations to support supposed medical bills relating to his false claim that he had brain cancer. The specific count of conviction involves the use of the church credit card to buy a luxury watch from an expensive retailer in California for $3,711. (Source)

Former Account Manager For 2 Churches Sentenced To Prison For Embezzling $150,000+ - February 16, 2023

Michelle Miller worked from September 2017 to February 2020 as a Business Manager for St. Teresa Catholic Church as well as St. Luke Catholic Church.

During her time as an employee, she was an authorized signatory on both bank accounts and wrote numerous checks payable to herself. In total, she stole an estimated $153,940.38. To conceal her fraud, Miller forged signatures and made false bookkeeping entries. (Source)

BANKING / FINANCIAL INSTITUTIONS

Former Bank Employee Convicted For Role In $2 Million Fraud Scheme - February 27, 2023

Diape Seck was convicted for his role in a bank fraud scheme in which he and his co-conspirators obtained or attempted to obtain almost $2 million by fraud, including by stealing checks from the mail of churches and religious institutions.

From at least January 2019 to January 2020, Diape Seck, who was a Customer Service Representative with Bank A, conspired with Mateus Vaduva, Marius Vaduva, Vlad Baceanu, Nicolae Gindac, Florin Vaduva, Marian Unguru, Daniel Velcu, Vali Unguru and others to commit bank fraud.

Seck fraudulently opened bank accounts in fake identities in exchange for cash bribes. Co-conspirators engaged in fraud that included fraud involving rental cars and the deposit of checks stolen from the incoming and outgoing mail of churches and other religious institutions, into the fraudulently opened bank accounts. The co-conspirators then withdrew the funds and spent the fraudulently obtained proceeds

Seck violated numerous bank policies in opening approximately 412 checking accounts in a one-year period from approximately January 2, 2019 through January 3, 2020, relying predominantly on purported Romanian passports and driver's license information.

Checks payable to and written from churches and other religious institutions from around the country were deposited into many of the 412 checking accounts which were not opened in the names of the churches.

The co-conspirators fraudulently negotiated the stolen checks by depositing them into the victim bank accounts, including the fraudulent accounts opened by Seck at Bank A, often by way of automated teller machine (ATM) transactions. After depositing the stolen checks into the bank accounts, the conspirators made cash withdrawals from ATMs and purchases using debit cards associated with the bank accounts. (Source)

Customer Service Rep Charged With Stealing $1 Million+ From Bank Customers - February 16, 2023

From May 2021 to October 2021, Ashley Miller was employed as a Customer Service Agent for Dial American, a third-party vendor for U.S. Bank contracted to do various customer service duties over the telephone.

Court documents state that during this timeframe, Miller allegedly devised a scheme to obtain funds from U.S. Bank customers by changing an account holder's original mailing address for debit cards issued by U.S. Bank, causing debit cards to be mailed to a residential address in Akron owned by Miller.

Miller then used these debit cards for personal use by making fraudulent withdrawals from various ATMs. In total Miller compromised approximately 299 accounts for about $1,118,391.82.
(Source**)**

Former Bank Teller Sentenced To Prison For Embezzling $349,000+ - February 3, 2023

From January 2013, to November 2016, Karen Tigler was employed as a multi-service banker with the Hancock Whitney Bank, in New Orleans.

From February 9, 2015, to October 28, 2016, Tigler used her position with the bank to embezzle approximately $349,556 from a clients account by using 100 counter checks to debit funds from the clients account.

Tigler used her position with the bank to access personal information from other legitimate banking transactions to create the fraudulent counter checks. Tigler forged the signatures of various clients accounts on the counter checks in an effort to conceal her embezzlement scheme.

Tigler cashed 21 counter checks totaling $73,924 that were supposedly for roofing, market / garden work, light fixtures / cleaning, extras plumbing, misc. work, renovations and "maintenance. Tigler cashed the other 79 counter checks totaling approximately $275,632 payable to another individual that were supposedly for house, maintenance and for happy birthday. (Source)

Former Bank President Sentenced To Prison For Role In $200,000 Bank Loan Fraud Scheme - February 16, 2023

Between 2019 and 2021, while Brady Torgerson was employed at separate times as the President of First Security Bank-West and as a loan officer at the Union Bank, Torgerson conducted banking transactions, which caused harm to both these banks and the banks' individual customers.

Specifically, while employed at First Security Bank-West, Torgerson funded loans without obtaining: 1) necessary financial information; 2) security interest documents; or 3) promissory notes. Additionally, Torgerson engaged in deceptive banking transactions by entering false information into the bank's computer system, increasing loans so that they exceeded the original loan amounts, and extending loan maturity dates to conceal

his activities. Most notably, while employed at the Union Bank, Torgerson created fraudulent loan obligations in the amounts of $225,487.44 and $225,487.45 in the names of three separate individuals who neither knew about the creation of these loans nor received the funds described in these obligations. (Source)

Bank Employee Admits To Role In Stealing $45,000 From 11 Elderly Customers - February 8, 2023

Kazeem Adelekan faces a felony charge accusing him of stealing nearly $45,000 from elderly victims while working as a bank employee.

Kazeem Adelekan faces one charge of identity theft involving more than eight victims with a combined loss of over $35,000.

Adelekan allegedly admitted to gathering private customer information while at work and then selling it to co-conspirators.

The co-conspirators would then open an online banking account using the stolen information provided by Adelekan. The co-conspirators would then attempt to transfer money from the victims' accounts to their account by way of the newly created online banking account."

Adelekan was then allegedly paid by the co-conspirators for sharing the stolen information for the accounts.

During the investigation, it was determined that there were 11 victims and $44,835.56 was successfully stolen, but the attempted amount to be stolen totaled more than $101,000. (Source)

TRADE UNIONS

Former Teacher Union President Arrested For Embezzling $400,000 / Paid Herself Bonuses & Used Credit Cards For Unauthorized Purchases - January 26, 2023

The former president of a Virginia teachers union was arrested and charged with embezzling hundreds of thousands of dollars from the organization, according to police.

Ingrid Gant, the former President of the Arlington Education Association (AEA), was arrested after police conducted a six-month audit that showed that she embezzled $410,782.10 from the union, according to a press release from the Fairfax County Police Department.

Gant was charged with four counts of embezzlement where she allegedly used debit cards for unauthorized purchases and gave herself multiple bonuses.

An internal audit was ordered after AEA board members grew concerned about their leader's suspicious behavior. Gant allegedly failed to provide financial reports to the board and did not file tax returns, police said.

She was fired in March 2022 and her removal prompted board members to hire an outside group, the Calibre CPA Group, to conduct an internal audit which uncovered Grant's gross misuse of taxpayer's money.

After six months of reviewing her activity, investigators discovered Gant gifted herself $350,000 worth of bonuses and pay from 2020 to 2022. She also charged approximately $70,000 on business debit cards for personal items like gas, food, and even Amazon purchases. (Source)

External Co-Conspirator Sentenced To Prison For Working With Union Secretary To Embezzle $200,000 Of Labor Union Funds - February 23, 2023

Between approximately October 2016 through May 2018, James Bradley helped to embezzle approximately $205,421.82 from the American Federation of Government Employees (AFGE).

He did so by enabling co-conspirator Donnell Owens who worked at AFGE as a Secretary to the Director of Communications during the relevant period, to submit false and fraudulent check requests and invoices for non-existent videography services that the defendant purportedly provided to AFGE as an alleged vendor, but that the defendant never actually provided. As a result of these submissions, AFGE funds were subsequently disbursed for work that was never performed, including $205,421.82 to Bradley which he then split with Owens. (Source)

Former Union Treasurer Charged With Embezzling $45,000 - February 14, 2023

Donald Byers is the former Treasurer for Division 287 of the Brotherhood of Locomotive Engineers and Trainmen (BLET), which is located in Ashville, Pennsylvania.

Byers embezzled over $45,000 from union funds, and created fraudulent records to conceal his embezzlement. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Former IT Employee Pleads Guilty To Stealing Confidential Data And Extorting Company For $2 Million In Ransom / 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 Apri 1, 2021. Sharp was a Senior Developer who had administrative to credentials for companys 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 a public New York-based 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 thhe remediation of 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 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)

Facebook Terminates Contractor Employee Who Leaked Information To Outsider - February 10, 2023
Meta CTO Andrew Bosworth told employees in an internal company post that the company had identified a worker who had leaked information about its virtual reality headsets.

Bosworth told staff in the post that the company had tracked down the individual and parted ways with the worker following a month long investigation into the leaked information. The worker was a third-party contractor with Meta.

The worker had leaked details around previously unannounced Virtual Reality (VR)headsets and had shared sketches of Meta's rumored Quest 3 last year that were posted by tech review YouTuber Brad Lynch. The Quest 3 headset is expected to be released in the fall off 2023.

The worker who leaked the information had asked Lynch for a portion of his profits from the ads on his YouTube videos.

Lynch, who showed off the leaked designs in his YouTube video, told Insider he does not "normally" pay for leaked information.

"I do not make enough money as a lone VR content creator who tends to rely on viewer patronage rather than corporate sponsorships," he said in an emailed statement. He added that Meta has a more significant issue with leaks at the company than this one worker, saying Meta's response won't deter him from continuing to share unreleased details about the company. (Source)

Edward Jones Sues Former Financial Advisor / Seeks Restraining Order Against Advisor Who Stole Confidential / Trade Secret Information Prior To His Termination - January 31, 2023
Edward Jones is seeking a temporary restraining order and injunctive relief in federal court against a former financial advisor who the company alleged stole confidential and trade secret information of “five-star” clients prior to his termination.

The complaint, filed in the U.S. District Court for the Central District of Illinois on January 26, 2023 is requesting that the court require Cory Clem to return all Edward Jones confidential and trade secret client information in his possession, cease from directly or indirectly soliciting Edward Jones clients, and cease contacting Edward Jones employees.

According to the complaint, Clem was responsible for serving hundreds of clients and was fully aware of company policy regarding client information, which was clearly laid out in the employment agreement he signed and agreed to when he accepted the position.

But the complaint argued that Clem has violated the employment agreement. It said he began planning his move to Ameriprise in the fall of 2022. At that time, the complaint said, Clem traveled to Edward Jones’ headquarters in St. Louis to meet with human resources to “discuss issues they were having.” Prior to that meeting, he had asked one of the branch administrators to print a “Five-Star” relationship client list for him.

That list, the complaint explained, included clients’ account information such as number of total assets under care, their net worth, the kinds of accounts they have, the categories of investments they have, whether their account is active or not, and when to contact them.

Upon returning from the home office, the complaint said, Clem intensified his efforts to leave the company. He began bad-mouthing the company to clients and he informed his team (one financial advisor and two branch administrators) of his intention to go to Ameriprise and encouraged them to leave with him as a "team," the complaint said. He told them that he was planning to resign February 24 to join Ameriprise.

Clem worked for Edward Jones, where he began his career, since 2010. He was let go on January 20 and joined Ameriprise on January 24, 2023. (Source)

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

U.S. Army Reservist Working Under The Direction Of A Chinese State Intelligence Unit Sentenced To Prison For Spying In An Effort To Steal Aviation Trade Secrets - January 26, 2023

A Chinese engineer has been jailed for eight years for spying in the U.S., in a case linked to Chinese efforts to steal aviation trade secrets.

Ji Chaoqun had identified scientists and engineers for possible recruitment, according to the DOJ. He also enlisted in the U.S. Army Reserves and lied to recruiters.

Authorities said Ji worked under the direction of a key Chinese State Intelligence Unit. Last September he was convicted for acting as an agent of a foreign government without notifying the U.S. and of making false statements to the Army. Ji had arrived in the U.S. on a student visa a decade ago, according to the DOJ. He was accused of supplying information to the Jiangsu Province Ministry of State Security about eight individuals for possible recruitment. (Source)

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

Former Medical Office Nurse Admits Role In $1.2 Million+ Health Care Fraud Conspiracy - February 28, 2023

Ashley Valenti was previously an Advanced Practice Nurse at a medical office in Pennsville, New Jersey during this fraud conspiracy.

Valenti was previously charged with Vincent Tornari and Brian Sokalsky in a 33-count indictment in June 2020.

Tornari hired Valenti's live-in boyfriend to be a Sales Representative for his company which promoted compound medications, even though Valenti's boyfriend had no background or experience in medicine and pharmaceutical sales.

Tornari and Valenti's boyfriend had an agreement that the boyfriend would receive a commission on all prescriptions authorized by Valenti. Valenti then authorized numerous medically unnecessary prescription medications associated with Tornari and her boyfriend, including for her patients, staff members and co-workers at the medical office where she worked, and her children, for the sole purpose of financially benefitting herself, her boyfriend, and Tornari.

In exchange for authorizing the prescriptions, Valenti's boyfriend paid her half of his commissions that he received from Tornari. As a result of the scheme, health insurance paid over $1.2 Million for medically unnecessary medications and Valenti received over $90,000 in kickbacks for signing the prescriptions. (Source)

Employee Of Assisted Living Facility Stole Credit Cards From Elderly Residents - February 8, 2023
An employee of an Alamance County assisted living facility in North Carolina is in custody for stealing financial cards from two elderly residents.

After an investigation, deputies identified and established probable cause to arrest an employee of the facility, Beverly Jeffers.

Jeffers was charged with two counts of Felony Theft of Financial Card, two counts of Felony Identity Theft, two counts of Felony Obtain Property by False Pretense, and two counts of Misdemeanor Exploitation of Elder. (Source)

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

Former NSA Contractor Convicted For Submitting False Claim For 90% Of Hours Worked - February 15, 2023
A federal jury convicted Jacky Lynn McComber of Elkridge, Maryland, on federal charges of submitting false claims and making false statements, in connection with the hours she claimed to have worked on a federal contract with the National Security Agency (NSA). McComber was the CEO and owner of InfoTeK, an information technology (IT) services corporation, which had an ongoing contract with the NSA.

A subsequent review and comparison by the NSA OIG in the fall of 2017 of McComber's NSA access control records with the time InfoTeK billed for her work on the Ironbridge contracts established that McComber was not within access control at the NSA's Fort Meade location for 2,342.5 (90%) of the 2.603.5 hours she had recorded on her timesheets and that InfoTeK subsequently billed to NSA.

In addition to not being physically present at the worksite for the vast majority of hours she billed to the Ironbridge contract, the evidence showed that McComber did not work the number of hours on the Ironbridge contract that she recorded on her timesheet.

For example, on occasions when McComber billed a full eight-hour day to the Ironbridge contract, she participated in charity events, attended her high school reunion, vacationed in Texas and in Ocean City, Maryland, and performed business development efforts on behalf of InfoTeK that were unrelated to the Ironbridge contract. Other testimony by former InfoTeK officers indicated that McComber was only in InfoTeK's Columbia, Maryland offices irregularly and when she was there, she did not appear to be working on Ironbridge-related matters. As a result of McComber's false claims as to the time she worked on the Ironbridge contract between March 2016 and September 2017, the NSA substantially overpaid InfoTeK. (Source)

Chief Financial Officer Sentenced To Prison For Embezzling $1.3 Million+ In Company Funds - February 27, 2023
The former Chief Financial Officer of a IT consulting firm has been indicted on federal fraud charges for allegedly embezzling more than $1.3 Million in company funds.

Anthony Fremarek fraudulently caused funds from two of the company's bank accounts to be used to pay his personal credit cards. Fremarek attempted to conceal the embezzlement by falsifying entries in the company's accounting system to disguise the payments as seemingly legitimate business expenses, the indictment states. The alleged fraud scheme spanned from 2013 to 2019. (Source)

Pharmaceutical Executive And Cousin Charged In $700,000+ Insider Trading Of Kodak Stock - February 23, 2023

Between June and July 2020, Andrew Stiles conducted an insider trading scheme in which he misappropriated material, non-public information (MNPI) and used it to trade in the stock of the Eastman Kodak Company (Kodak) and further provided that MNPI to his cousin, Gray Stiles that Gray would likewise trade on the MNPI.

During that time, Andrew was an executive at a company (Company-1) that was working with Kodak to collaborate on the production of chemicals for pharmaceutical manufacturing in connection with the COVID-19 pandemic. Company-1 was also assisting Kodak in its application for a significant government loan, which ultimately resulted in the news, on July 27, 2020, of a government "letter of interest" to provide Kodak with a loan of $765 million (LO"). In the following days, Kodak stock rose substantially, at one point increasing to more than 2,500% above the closing price prior to the news of the LOI.

During June and July 2020, Andrew was kept apprised of Kodak's efforts to obtain the government loan, and he both traded using that non-public information and passed that information to Gray.

Andrew and Gray Stiles each sold the entirety of their shares in the days and weeks after the announcement. Andrew realized profits of more than $500,000, and Gray realized profits of more than $700,000. (Source)

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

Former Employee Sentenced To Prison For $270,000+ Of Fraud / Used Money For Motorcycle, Motor Home, Cargo Trailer - February 22, 2023

Jordyn Culp stole $273,698 from the Federal Employees' Group Life Insurance (FEGLI) Program.

From approximately October 2019 to September 2021, Culp accessed FEGLI trust accounts through her employment and fraudulently transferred money from the FEGLI accounts to her personal bank account.

Using the funds, Culp purchased a motorcycle, motor home, and cargo trailer which were forfeited. Culp posted TikTok videos discussing her purchases. Culp was ordered to pay restitution and after her prison sentence she will serve three years of supervised release. (Source)

Executive Director For Non-Profit Charged With Embezzling $156,000+ / Used Money Shopping / Payments To Colleges - February 28, 2023

Ellen Corn served as the Executive Director for the nonprofit from March 2017 through August 2022. During her employment, Corn had various financial responsibilities including entering all income and expenses into the organization's accounting software.

Over that five-year period, Corn allegedly stole more than $156,000 by using an organizational credit card for personal expenses without authorization. She attempted to conceal her unauthorized purchases by not entering them into the accounting software.

Corn allegedly used the organization's credit card to purchase goods and services from various businesses, including Amazon, Target, Walmart, and to make payments to colleges. Further, Corn allegedly used the credit card to make electronic payments from the official business PayPal account to her personal PayPal account. Once the funds appeared in her PayPal account, she transferred them to her personal checking account. (Source)

Former City Commissioner Sentenced To Prison For Accepting $130,000 In Bribes From Contractor / Including Diamond Ring, Hotel In Dubai, Home Landscaping Work - February 24, 2023

Jo Ann Macrina served as the Commissioner of Atlanta's Department of Watershed Management from 2011 through May 2016.

Macrina accepted bribes from an Atlanta contractor in exchange for steering city business worth millions of dollars to the contractor's company.

During Macrina's tenure, the City of Atlanta awarded millions of dollars in contracts to an architectural, design, and construction management and services firm based in Atlanta. Macrina took multiple steps to steer lucrative contracts toward the firm's joint venture. Those actions included casting aside prior final scores ranking potential vendors where the joint venture ranked near the bottom, replacing two evaluators who previously represented the Department of Watershed Management with herself and Macrina's employee, and scoring the joint venture higher than all other evaluators during a reevaluation.

In exchange for providing the firm's Executive Vice President (EVP) with access to confidential information and preferential treatment on City of Atlanta projects, Macrina was offered a job and accepted things of value. Macrina accepted $10,000 in cash, a diamond ring, a room at a luxury hotel in Dubai, and landscaping work at her home from the EVP either directly or through another employee of the firm.

Shortly after Macrina's employment with the City of Atlanta ended, she began working for the firm. Between June 2016 and September 2016, the firm and its executive vice president paid Macrina $30,000 in four separate payments. (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

Former Employee Arrested For Defrauding Former Employer Of $4.4 Million In Fake Invoice Scheme - February 24, 2023

From July 2018 to August 2022, Bhaskarray Barot engaged in a scheme to defraud his former employer of approximately $4.4 Million through fake invoices designed to resemble those received from legitimate vendors of the company he worked for.

Barot used his position as a Procurement Manager at his employer to process the fraudulent invoices for payment.

When doing so, he often affixed the fake invoices to email messages that he, in some cases, sent in the names of employees of the company's real vendors so that it would appear as though the real vendors were seeking payment on the fake invoices.

The fake invoices, however, stated that payment should be made to entities with names that often differed slightly from those of the real vendor companies. Barot then incorporated companies and opened bank accounts in the names of some of the entities listed for payment on the fake invoices so that he could collect the payments that the company made on the fake invoices. (Source)

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

No Incidents To Report

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

Contract Employee Pleads Guilty To Role In Scheme To Steal Vehicles From Airport Car Rental And Transport Them To Nearby States - February 22, 2023

From May 2021, until October, 2021, Bernard Washington conspired to commit offenses against the United States, namely, transportation and receipt of stolen vehicles.

Washington admitted that he worked as a contractor for the Hertz Rent a Car at the Pittsburgh International Airport between May and July 2021. During that time, and for several months thereafter, Washington and co-conspirators accessed the Hertz parking lot and stole approximately 24 vehicles, at least three of which were transported across state lines from Pennsylvania to other states, including Maryland, Delaware, and Virginia. Washington and his co-conspirators provided these stolen vehicles to other individuals in exchange for payment. Washington also received at least two stolen vehicles from a co-conspirator, one of which had crossed state lines after being stolen. (Source)

EMPLOYEE DRUG RELATED INCIDENTS

UPS Employees Charged With Trafficking Cocaine - February 27, 2023

A total of 5 people have been arrested on charges of conspiracy to possess with intent to distribute cocaine and possession with intent to distribute cocaine.

On multiple occasions between March 24 through Oct. 3, 2022, the indictment alleges the 5 individuals conspired to transport cocaine through UPS packages.

Orlando Almanza and Fidencio Salinas Jr. are set to make their initial appearances before U.S. Magistrate Judge Medrano.

Also arrested and who made their appearance already were Javier Enrique Mendoza, Jose Lozano, Enrique Gamez.

Salinas and Almanza are both UPS employees who knowingly transported the packages of cocaine. The charges allege Mendoza provided the packages of cocaine to UPS employees, while Lozano allegedly provided fraudulent labels for the packages. Gamez stored the cocaine at his residence prior to transport, according to the charges.

Law enforcement seized approximately 60 kilograms of cocaine these individuals allegedly trafficked. (Source)

Former Office Manager For Medical Practice Admits To Conspiring With Doctor To Divert Controlled Substances - February 15, 2023

From January 2018 to March 2021, Noel DeLeon worked as an Office Manager for a New Jersey medical practice owned by a doctor.

The doctor performed no meaningful evaluation of patients and the interactions between the doctor and patients generally took less than five minutes. The medical practice kept inadequate patient medical records. For some patients, the patient files only contained contact and prescription information, but did not detail any meaningful evaluation or assessment. For other patients, no patient files were kept.

After prescribing medications to a patient, including high dosage amphetamines, DeLeon or the doctor would typically collect a cash payment from the patient before providing the prescription. For prescription refills, patients would also contact DeLeon directly by sending text messages to his personal cellular phone.

DeLeon would order the prescription refill at the patient's pharmacy and collect payment from the patient, typically through an electronic payment application on DeLeon's personal cellular phone. At times, certain patients provided cash bribes to DeLeon in order to receive their prescription refills faster. (Source)

OTHER FORMS OF INSIDER THREATS

No Incidents To Report

MASS LAYOFF OF EMPLOYEES AND RESULTING INCIDENTS

No Incidents To Report

EMPLOYEES MALICIOUS ACTIONS CAUSING COMPANY TO CEASE OPERATIONS

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

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

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

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

WORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES

Intel Employee Attacked And Killed With Baseball Bat By Co-Worker- February 16, 2023

Derrick Simmons, an Intel employee allegedly beat a coworker to death with a baseball bat in the cafeteria of an Intel building in Arizona, police said.

Simmons was arrested after he attacked the unnamed coworker with a bat, knife and hatchet at the Intel Arizona campus.

The police responding to the scene found one person dead with fatal blunt force trauma injuries and another person injured.

The second victim was reportedly injured after confronting Simmons. Simmons has a previous felony conviction, for aggravated assault with a deadly weapon. (Source)

EMPLOYEES INVOLVED IN TERRORISM

No Incidents To Report

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

SEVERE IMPACTS FROM INSIDER THREATS INCIDENTS

EMPLOYEE EXTORTION

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

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

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

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

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

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

EMPLOYEES WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

DATA / COMPUTER - NETWORK SABOTAGE & MISUSE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

WORKPLACE VIOLENCE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

WORKPLACE VIOLENCE (WPV) INSIDER THREAT INCIDENTS E-MAGAZINE

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

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

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

WORKPLACE VIOLENCE TODAY E-MAGAZINE

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

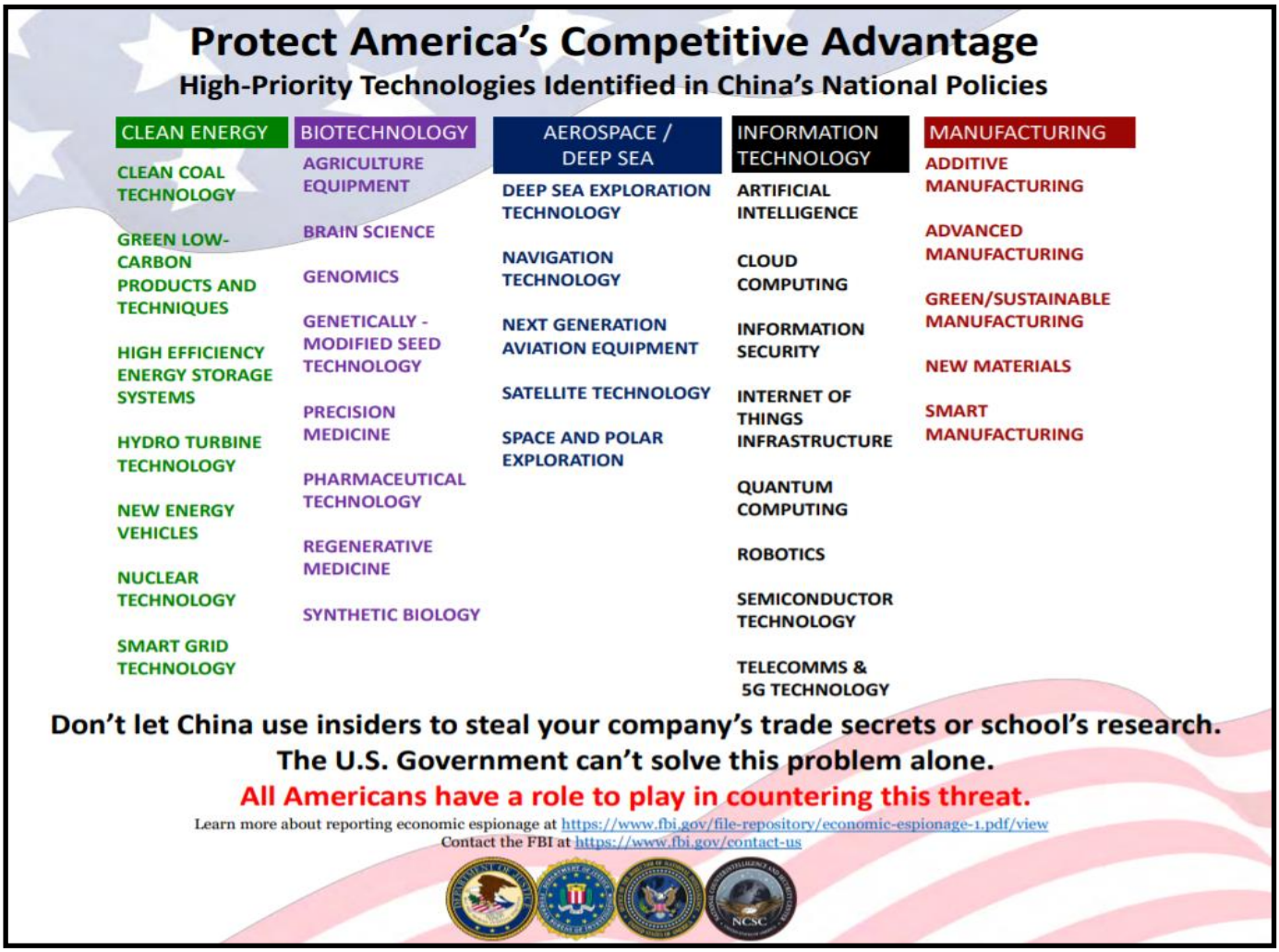
INSIDERS WHO STOLE TRADE SECRETS / RESEARCH FOR CHINA / OR HAD TIES TO CHINA

CTTP = China Thousand Talents Plan

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

- Former U.S. Navy Sailor Sentenced To Prison For Selling Export Controlled Military Equipment To China With Help Of Husband Who Was Also In Navy

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



SOURCES FOR INSIDER THREAT INCIDENT POSTINGS

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

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

INSIDER THREAT INCIDENTS E-MAGAZINE

2014 To Present

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**4,300+ Incidents**).

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

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

INSIDER THREAT INCIDENTS MONTHLY REPORTS

July 2021 To Present

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

INSIDER THREAT INCIDENTS POSTINGS WITH DETAILS

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

Incident Posting Notifications

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

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

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

INSIDER THREAT INCIDENTS POSTINGS ON TWITTER

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

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS

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

National Insider Threat Special Interest Group (NITSIG)

NITSIG Overview

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

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

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

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

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

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

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

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

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

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

Security Behind The Firewall Is Our Business

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

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

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

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

ITDG Training / Consulting Services Offered

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

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

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

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