INSIDER THREAT INCIDENTS REPORT
FOR
June 2024

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

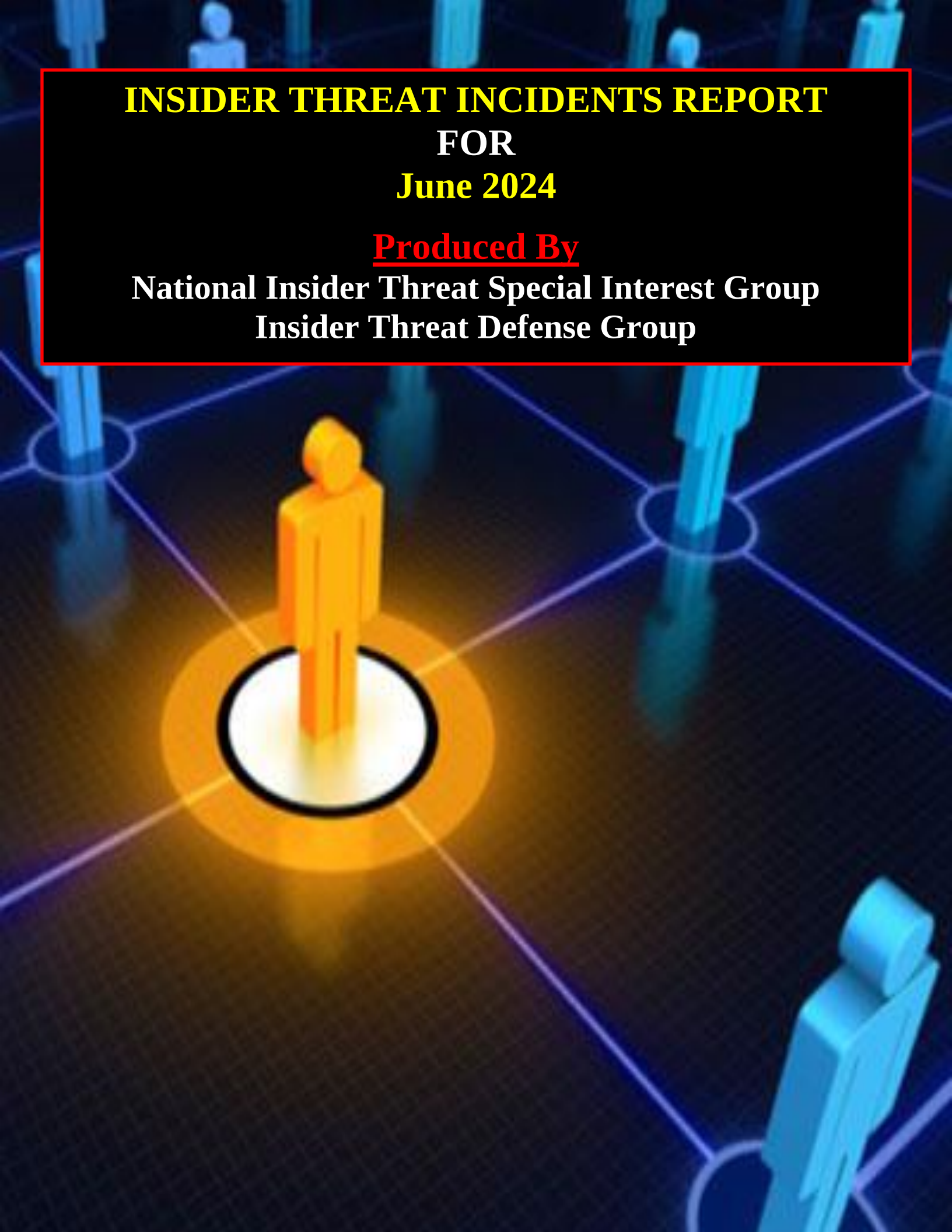


TABLE OF CONTENTS

INSIDER THREAT INCIDENTS

A Very Costly And Damaging Problem

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

The National Insider Threat Special Interest Group (NITSIG) in conjunction with the Insider Threat Defense Group (ITDG) have conducted extensive research on the Insider Threat problem for 15+ years. This research has evaluated and analyzed over **5,400+** Insider Threat incidents in the U.S. and globally, that have occurred at organizations of all sizes.

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

The traditional norm or mindset that malicious Insiders just steal classified information, an organizations data, trade secrets or other sensitive information, is no longer the case. There continues to be a drastic increase in financial fraud and embezzlement committed by employees', and this very evident in the Insider Threat Incidents Reports that are produced monthly by the NITSIG and the ITDG.

According to the Association of Certified Fraud Examiners 2024 Report To the Nations, the 1,921 fraud cases analyzed, caused losses of more than **$3.1 BILLION.**

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

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

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

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

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

These monthly reports are recognized and used by Insider Risk Program Managers and security professionals working for major corporations, as an educational tool to gain support from CEO's, C-Suite, key stakeholders and supervisors for Insider Risk Management (IRM) Program's. The incidents listed on pages **4 to 26** of this report provide the justification, return on investment and the funding that is needed for an IRM Program. These reports also serve as an excellent Insider Threat Awareness Tool, to educate employees' on the importance of reporting employees' who may pose a risk or threat to the organization.

INSIDER THREAT INCIDENTS
FOR JUNE 2024

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

No Incidents To Report

U.S. GOVERNMENT

Former Federal Investigator Sentenced To Prison For Fabricating 22 False Reports For Background Checks Interviews He Never Conducted - June 20, 204

Christopher Laughlin began working at the United States Office of Personnel Management as a federal background investigator in May of 2018. His position was transferred to the Defense Counterintelligence and Security Agency (DCSA) on September 30, 2019.

On August 2, 2021, as part of DCSA's internal control process, an individual reported that Laughlin never interviewed them, contrary to Laughlin's statements in an investigation report. DCSA investigated and identified three other sources Laughlin claimed to have interviewed in the same investigation who all stated they'd never been interviewed. DCSA's Office of the Inspector General then initiated a formal investigation into Laughlin's conduct.

Investigators determined that between February 18 and September 1, 2021, Laughlin submitted at least 22 false reports containing fabricated statements from at least 43 interviews that never actually happened. The reports included statements that the sources purportedly made to Laughlin by people he never spoke with. DCSA spent $69.846.214 in payroll and travel to conduct the investigations that Laughlin fabricated. (Source)

U.S. Postal Service Employee Charged With Stealing Ten Of Thousands Of Dollars Worth Of Checks From Mail & For Fraud / Identity Theft Scheme - June 7, 2024

Kierra Blount while employed by the U.S. Postal Service in Stamford, Connecticut stole mail and obtained stolen mail for the purpose of obtaining checks that were payable to other individuals.

In approximately November 2021, Blount opened a bank account using the name and social security number of an individual without the identity theft victim's knowledge. Blount and others fraudulently changed the payee names on stolen checks to the name of the identity theft victim, forged the victim's signature on the back of the checks, and deposited them into the bank account Blount opened. From November 2021 until the account was closed in April 2022, Blount and others deposited tens of thousands of dollars in fraudulent checks into the account. They then used the funds for their own purposes. (Source)

U.S. Postal Service Employee Sentenced To Prison For Stealing $90,000 Worth Of Money Orders - June 11, 2024

Jamesa Rankins worked as a Sales & Service Distribution Associate at the Montello Post office in Brockton, Massachusetts for approximately four and a half years.

Prior to her termination in January 2021, Rankins had the ability to generate postal money orders, including replacement money orders. Customers could obtain replacement money orders without paying any additional fees if the original postal money orders were lost, damaged or erroneous. Beginning around September 2020, Rankins issued approximately 126 fictitious replacement money orders to an associate for money orders that were not lost, damaged or erroneous.

In many instances, the fictitious replacement money orders actually invalidated properly issued money orders. In total, Rankins issued nearly $90,000 worth of replacement money orders.

Beginning in May 2020, Rankins also applied for and obtained Pandemic Unemployment Assistance from the Massachusetts Division of Unemployment Assistance despite being employed by USPS and thus being ineligible to receive unemployment assistance. In total, Rankins collected at least $15,000 in unemployment benefits to which she was not entitled. (Source)

Former IRS Employee Charged For Preparing $237,000+ Of Fraudulent Tax Returns - June 12, 2024

Sandra Mondaine is a former IRS employee .

Mondaine is charged with 39 counts of aiding and assisting in the preparation and filing of false and fraudulent income tax returns. The indictment alleges that Mondaine assisted at least 11 individuals to file at least 39 false and fraudulent income tax returns for the tax years 2018 through 2021. The tax loss associated with those false returns is approximately $237,329. (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Former Navy Civilian Employee Pleads Guilty To Bribery Scheme Involving $100 Million+ In Government Contracts - June 12, 2024

James Soriano is a former civilian employee of the San Diego based Naval Information Warfare Center (NIWC).

Soriano pleaded guilty to multiple bribery conspiracies, admitting that while he was a public official at NIWC, he accepted hundreds of thousands of dollars from defense contractors in the form of free meals, tickets to premier sporting events, jobs for family and friends, and other things, in exchange for helping those contractors win and maintain hundreds of millions of dollars in government contracts.

According to Soriano's plea agreement, from approximately March 2016 through at least October 2019, Soriano and a coworker, Dawnell Parker, received bribes from Philip Flores, the President and CEO of Intellipeak Solutions, Inc., a defense contractor headquartered in Fredericksburg, Virginia. Soriano also admitted that from approximately May 2015 through at least October 2019, he and Parker separately received bribes from another defense contractor, with offices in San Diego and Stafford, Virginia, who also gave him things of value, such as expensive meals, a job for his wife, and rounds of golf at private country clubs.

Further, according to Soriano's plea agreement, from approximately June 2014 through at least October 2019, Soriano received bribes from Russell Thurston, the Vice President of Cambridge International Systems, Inc., a defense contractor headquartered in Arlington, Virginia. In return for these bribes, Soriano used various methods to steer contracts to these defense contractors and kept his contracting activities hidden from the Naval Information Warfare Center.

According to Soriano's plea agreement, the defense contractors acting through their presidents, officers, and employees gave various things of value to Soriano, including dinners at Ruth's Chris, Island Prime, and Providence; tickets to the 2018 MLB All-Star Game, 2018 World Series, and 2019 Superbowl; and jobs for Soriano's family and friends, including a member of Soriano's family and Soriano's family friend, Liberty Gutierrez, who was giving Soriano $2,000 a month from her salary at one of the companies working under a defense contract. (Source)

Navy Admiral (Now Retired) & Business Executives Arrested For Alleged Bribery Scheme - May 31, 2024

From 2020 to 2022, Robert Burke was a four-star Admiral who oversaw Naval operations in Europe, Russia, and most of Africa, and commanded thousands of civilian and military personnel.

Yongchul "Charlie" Kim and Meghan Messenger were the co-CEOs of a company (Company A) that provided a workforce training pilot program to a small component of the Navy from August 2018 through July 2019.

The Navy terminated a contract with Company A in late 2019 and directed Company A not to contact Burke.

Despite the Navy's instructions, Kim and Messenger then allegedly met with Burke in Washington, D.C., in July 2021, in an effort to reestablish Company A's business relationship with the Navy. At the meeting, the charged defendants allegedly agreed that Burke would use his position as a Navy Admiral to steer a sole-source contract to Company A in exchange for future employment at the company. They allegedly further agreed that Burke would use his official position to influence other Navy officers to award another contract to Company A to train a large portion of the Navy with a value Kim allegedly estimated to be "triple digit millions."

In furtherance of the conspiracy, in December 2021, Burke allegedly ordered his staff to award a $355,000 contract to Company A to train personnel under Burke's command in Italy and Spain. Company A performed the training in January 2022. Thereafter, Burke allegedly promoted Company A in a failed effort to convince a senior Navy Admiral to award another contract to Company A. To conceal the scheme, Burke allegedly made several false and misleading statements to the Navy, including by creating the false appearance that Burke played no role in issuing the contract and falsely implying that Company A's employment discussions with Burke only began months after the contract was awarded.

In October 2022, Burke began working at Company A at a yearly starting salary of $500,000 and a grant of 100,000 stock options. (Source)

8 Army Civilian Employees Sentenced To Prison For Stealing Government Property Worth Millions From Army Deport & Delivering To Military Surplus Store To Sell - May 30, 2024

8 Army Civilian Employees have been sentenced to prison for conspiring to steal United States property from Anniston Army Depot (ANAD), in Alabama.

These civilian employees at ANAD stole millions of dollars in military property from warehouses at the depot over a period of several years and delivered it to middlemen. The middlemen delivered the stolen property to the owner of a military surplus store to sell.

The conspirators split the money from the sale of the stolen property. The stolen items included equipment that was designed to be attached to military weapon systems to provide operators with instant nighttime engagement capabilities and/or improved target acquisition. (Source)

Department Of Energy Employee Agrees To Pay $96,000+ To Settle False Claims For COVID Economic Injury Disaster Loan For Her Fake Business - June 5, 2024

Lisa Phillips has agreed to pay the United States $96,757.95 to resolve allegations that she violated the federal False Claims Act by submitting false claims to the U.S. Small Business Administration (SBA) to obtain an Economic Injury Disaster Loan (EIDL) and EIDL advance during the height of the COVID-19 pandemic.

On July 10, 2020, Phillips signed and submitted a Loan Authorization and Agreement for an EIDL in the amount of $26,200.00. The United States contends that in her this EIDL application, the defendant made several material misrepresentations including, among other things, that, in 2019, her business had four employees, a gross annual revenue of $150,500, and $90,000 in cost of goods expenses. Phillips also stated that her business opened on January 25, 2017, and that the business was in the Educational Services industry. These misrepresentations were knowingly false; Phillips knew that she did not own or operate a business in the Educational Services industry, that she did not have any employees, and that she had neither the revenue nor cost of goods as stated in the application. In addition to the $26,200 Loan, Phillips received a $4,000 advance. (Source)

CRITICAL INFRASTRUCTURE

Former Water District General Manager Pleads Guilty For Role In Stealing $3 Million Of Federally Owned Water - May 28, 2024

From 1992 through approximately April 2015, Dennis Falaschi was the General Manager for a public water district in Fresno and Merced Counties (PWD) in California, that sold water to farmers with over 38,000 acres of farmland. PWD obtained water that it sold by purchasing water from the federal government and collecting drainage water from farms. The federal water that PWD purchased came from the Delta-Mendota Canal (DMC), which is a federally owned canal operated by the United States Department of the Interior's Bureau of Reclamation. PWD purchased federal water from the DMC pursuant to a contract that it entered into with the Bureau of Reclamation.

The federal water that PWD purchased from the DMC was fresh water that could be used for farming immediately. The drainage water that PWD collected from farms was high in salt content and toxins, and it needed to be blended down with fresh water before it could be reused.

Falaschi learned that water from the DMC was leaking from an old standpipe into a parallel canal in PWD. The parallel canal was owned by the then-president of PWD's board of directors. PWD employees subsequently modified the old standpipe so that it would not leak and could be opened and closed. This allowed for water to be taken from the DMC on demand.

The amount of federal water that was illegally taken for which Falaschi was responsible was valued at over $1.5 million but under $3.5 million. Nearly all of that water was taken to blend down and reuse drainage water.

From 2011 through 2016, Falaschi entered into private water sales where he received payments. The water sold was legitimately sourced from outside PWD and was not federally owned water. Thereafter, in March 2016, Falaschi signed and filed an individual income tax return with the Internal Revenue Service where he did not report the income that he received from the private water sales. (Source)

Former Airport Customs Officer Pleads Guilty To Stealing $18,000+ In Cash From Airline Passengers - June 18, 2024

Between mid 2023 and early 2024, William Timothy stole approximately $18,700 in cash from airline passengers during 17 incidents of theft uncovered by CBP's Office of Professional Responsibility Investigators.

Evidence collected during the investigation showed that Timothy was surreptitiously stealing cash from arriving international passengers during border enforcement examinations and currency verifications performed as part of his official duties as an assigned CBP Officer at Naples Airport in Florida. (Source)

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

Florida Deputy Sheriff Sentenced To Prison For $31,000+ COVID 19 Relief Fraud - May 30, 2024

Stephanie Smith was employed as a Deputy Sheriff with the Broward Sheriff's Office when she applied for the PPP loans in 2021. The PPP loans were based upon false gross income information for two sole proprietorship businesses, Children 1st Basketball Training and Agape Smith Vending. The scheme resulted in Smith's unlawful receipt of $31,108. (Source)

Police Officer Who Was Also Police Union President Sentenced To Prison $17,000 Fraud Scheme For Hours Not Worked - June 4, 2024

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

The investigation found a total of 526 hours that Helring claimed to work patrolling the complexes but that he did not actually work. At his sentencing, Helring was ordered to pay restitution in the amount of $17,831.40 and to pay a fine of $5000.00. He was also ordered to complete 100 hours of community service as a condition of his supervised release. (Source)

Police Sergeant Sentenced To Prison For $9,000+ Overtime Fraud Scheme / 14 Other Police Officers Charged - June 20, 2024

William Baxter was a Police Sergeant with the Boston Police Department's (BPD) Evidence Warehouse.

From March 2015 through June 2016, Baxter submitted false and fraudulent overtime slips for overtime hours that he did not work for two overtime shifts at the evidence warehouse. The first, called "purge" overtime, was a 4 – 8 p.m. weekday shift intended to dispose of old, unneeded evidence. The second shift, called "kiosk" overtime, involved driving to each police district in Boston one Saturday a month to collect old prescription drugs to be burned.

For the "purge" shift, Baxter claimed to have worked from 4 – 8 p.m., but he routinely left at 6 p.m., and sometimes earlier. Additionally, Baxter knowingly endorsed the fraudulent overtime slips of his subordinates who, allegedly, also left early from this shift. For the "kiosk" shift, Baxter and, allegedly, others routinely submitted overtime slips claiming to have worked eight-and-one-half hours, when in fact he and, allegedly, other members of the unit, only worked three-to-four hours of those shifts.

Between March 2015 and June 2016, Baxter personally collected approximately $9,223 for overtime hours he did not work.

Baxter was one of 15 police officers charged in connection with committing overtime fraud at the Boston Police Department's evidence warehouse, 10 of whom were convicted either by guilty plea or jury verdict. Of the remaining officers charged, four were acquitted in April 2023 and one officer passed away while charges were pending. (Source)

Former County Sheriff's Office Deputy Pleads Guilty Accepting Bribes From Inmate For Drugs, Cell Phone & Law Enforcement Sensitive Information - June 5, 2024

From May 2021 to June 21, 2023, Robert Sanford was a Correctional Officer at the Fairfax Virginia Adult Detention Center (ADC), which holds detainees arrested by the Fairfax County Police Department and federal agencies.

From Dec. 2022 through May 2023, Sanford smuggled contraband into Fairfax ADC and provided the contraband and confidential, law-enforcement-sensitive information to an inmate. The contraband included a cell phone and distribution quantities of fentanyl, cocaine, and Suboxone. Sanford also supplied latex gloves and glue to the inmate to help conceal the contraband. The inmate then trafficked the drugs to other inmates.

Sanford provided the inmate with information such as advance warning of cell searches by deputies, cell blocks to which deputies were proceeding in those searches, whether deputies would be conducting strip searches, and where drug-sniffing dogs were being utilized. Sanford also provided the inmate with information regarding other inmates, including which inmates might be providing information to law enforcement, which assisted Sanford's co-conspirator in intimidating potential witnesses.

Outside Fairfax ADC, Sanford procured drugs from the inmate's associates. In addition to the drugs Sanford smuggled into Fairfax ADC, Sanford distributed drugs to women who lived in and prostituted themselves out of an apartment that Sanford leased. (Source)

Corrections Officer Sentenced To Prison For Smuggling Contraband Into Prison & In Exchange For $45,000+ In Bribes - June 18, 2024

From approximately January 2020 through June 2022, Jason Skeet conspired with others to smuggle contraband, including marijuana, cigarettes, and food, to inmates housed at the Northern Infirmary Command on Rikers Island, New York in exchange for bribes. Skeet smuggled contraband for inmates housed on Rikers Island approximately 100 times between the start of the COVID-19 pandemic and June 2022 in exchange for tens of thousands of dollars in bribe payments.

Skeet was ordered to forfeit $45,644. (Source)

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS

District of Columbia Public Official Pleads Guilty For Role In $2 Million Contracting Fraud Scheme / Kickbacks Included New Car, $10,000 Cash, Etc. - June 6, 2024

Bridgette Crowell is a former public official who managed government contracts at the District of Columbia's Office of Contracting and Procurement (OCP) and, before that, the Washington Metropolitan Area Transit Authority (WMATA). She pleaded guilty today for participating in a scheme in which she reaped benefits from steering lucrative government contracts to her co-conspirators' private companies.

Crowell began working at the OCP in 2019 as a contracting specialist. Before that, she worked at WMATA as a contract administrator. Crowell first met her co-conspirators when working at WMATA. Obinna Ogbu was a WMATA employee. Ifediora Oli was an employee at the U.S. Department of Agriculture, but separately held himself out as the Principal of Highbury Global Group, Inc. (Highbury). By 2021, Crowell understood that her co-conspirators had orchestrated a bribery scheme in which Ogbu received things of value for misusing his position at WMATA and steering WMATA-related business opportunities to Oli and Highbury.

While at OCP, Crowell agreed to steer government contracts to Highbury and another company created by Ogbu, The Nupath Company (Nupath), in exchange for things of value.

Crowell misused her official position at OCP by, among other things: alerting her co-conspirators to upcoming solicitations; providing them with non-public information about the solicitations, including information regarding contract pricing; helping Highbury and Nupath secure government contracts; and taking multiple steps to conceal her personal connections to Highbury and Nupath.

Crowell's misconduct led to Highbury obtaining a $630,000 contract with the District to provide the District's Department of Forensic Sciences (DFS) with COVID-19 Testing Supplies; Nupath receiving a $27,000 contract to provide the Metropolitan Police Department (MPD) with certain equipment; and Nupath being awarded a nearly $850,000 contract to provide MPD with assistance carrying out pre-employment suitability background investigations for officer candidates.

For her official actions and participation in the fraudulent schemes, Crowell received things of value from her co-conspirators, including as much as $10,000 cash per month, a new car, and assistance with closing costs for a new home.

Ogbu admitted that his misconduct began in 2018 and ultimately resulted in Highbury and Nupath receiving roughly $2 million in funds originating from WMATA and District contracts. (Source)

City Employee Pleads Guilty To Role In Embezzling $465,000+ From Homeless Program - June 17, 2024

Amy Dixon worked for the City of Amarillo's (Texas) as a Homeless Management Information Specialist.

In her role, Dixon was responsible for distributing funds to local landlords through the U.S. Department of Housing & Urban Development's Emergency Solutions Grant (ESG) Program. She communicated with Amarillo property owners who were willing to lease their properties through the program, assisted in completing lease agreements, coordinated physical inspections of their properties, and assembled payment voucher packages. (The program paid market-rate rents to landlords willing to house those who needed assistance.)

In September 2020, Ms. Dixon used a relative's personally identifiable information to create a fictitious landlord, for whom she created fraudulent payment voucher packages. She instructed Amarillo's Finance Department to call her when the payment vouchers were ready, then signed the relative's name on the checks and deposited the funds into her personal bank account.

In April 2021, when HUD announced that it would accept inspections completed by outside companies, she began to process payments for fictitious properties.

In total, Ms. Dixon created 223 fraudulent payment vouchers resulting in 66 checks written to fictitious landlords, with a total loss amount of $465,511.65. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

Former University IT Director Admits Role In $2.1 Million IT Equipment Theft & Fraud Scheme - June 18, 2024

As Director of Information Technology for the university, Ronald Simpson was responsible for repairing and replacing defective IT equipment used at his employer's multiple locations

Beginning about Nov. 29, 2018, Simpson devised a scheme to enrich himself at the expense of the University and their equipment supplier.

After receiving approval to purchase hundreds of items of IT equipment by falsely claiming the equipment would be used or installed at university locations, Simpson sold that equipment to a third-party. Simpson misappropriated at least a million dollars from the university with this part of the scheme.

He also fraudulently obtained 56 items from the university's IT supplier by falsely claiming that the equipment they originally had supplied was defective. Simpson then sold both the original equipment and the replacement gear. The supplier sent a total of $780,233 worth of replacement IT equipment to the university based on Simpson's misrepresentations.

Simpson was paid a total of $2,188,704 for IT equipment belonging to the university and its supplier. (Source)

Former University Employee Convicted For Staging Hoax Explosion - June 28, 2024

Jason Duhaime in September 2002 was employed as the New Technology Manager and Director of the Immersive Media Lab (Lab) at Northeastern University.

At approximately 7:00 p.m. on Sept. 13, 2022, Duhaime called the Northeastern Police Department and reported that he was injured by sharp objects expelled from a plastic case he opened inside the Lab that evening. Specifically, Duhaime told an emergency police dispatcher that he and a Northeastern student who was working in the Lab that evening had collected several packages—including two plastic "Pelican cases"—from a mail area and brought them into the Lab. Duhaime said that when he opened one of the cases inside a storage closet, "very sharp" objects flew out of the case and under his shirt sleeves, causing injuries to his arms. Duhaime also reported that the case contained an anonymous "violent note" threatening to "destroy the lab" and stating: "In the case you got today we could have planted explosives but not this time!!! Take notice!!! You have two months to take operations down or else!!!!! WE ARE WATCHING YOU."

Duhaime's report and concern about a second, unopened Pelican case triggered a significant law enforcement response that included, among other things, the assistance of the Boston Police Department's bomb squad, the assistance of multiple federal and state law enforcement agencies, and the evacuation of a portion of the Northeastern campus.

During a search of Duhaime's office at Northeastern on Sept. 14, 2022, several laptop computers were found. A subsequent forensic examination of one of the computers revealed a word-for-word electronic copy of the anonymous threat letter that Duhaime claimed was inside the Pelican case. According to evidence presented during the trial, this electronic copy of the threat letter was created and printed between approximately 2:50 p.m. and 3:56 p.m. on Sept. 13, 2022 – just hours before he reported the incident to the Northeastern Police Department. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

No Incidents To Report

BANKING / FINANCIAL INSTITUTIONS

Former Company Chief Investment Officer Pleads Guilty To Role In $3 BILLION Of Securities Fraud / Company Pays $2.4 BILLION Fine - June 7, 2024

Gregorie Tournant is the former Chief Investment Officer and Co-Lead Portfolio Manager for a series of private investment funds managed by Allianz Global Investors (AGI).

Between 2014 and 2020, Tournant the Chief Investment Officer of a set of private funds at AGI known as the Structured Alpha Funds.

These funds were marketed largely to institutional investors, including pension funds for workers all across America. Tournant and his co-defendants misled these investors about the risk associated with their investments. To conceal the risk associated with how the Structured Alpha Funds were being managed, Tournant and his co-defendants provided investors with altered documents to hide the true riskiness of the funds' investments, including that investments were not sufficiently hedged against risks associated with a market crash.

In March 2020, following the onset of market declines brought on by the COVID-19 pandemic, the Structured Alpha Funds lost in excess of $7 Billion in market value, including over $3.2 billion in principal, faced margin calls and redemption requests, and ultimately were shut down.

On May 17, 2022, AGI pled guilty to securities fraud in connection with this fraudulent scheme and later was sentenced to a pay a criminal fine of approximately $2.3 billion, forfeit approximately $463 million, and pay more than $3 billion in restitution to the investor victims. (Source)

Former Bank Chief Financial Officer Sentenced To Prison For Role In Embezzling $700,000+ With Help Of Wife / Used Funds To Pay Credit Card, Trips, Etc. - June 7, 2024

Sammy Sims is the former Chief Financial Officer at a bank in the Chinatown area of downtown Los Angeles.

The bank hired Sims in September 2017 as the lender's CFO. As a condition of his employment, Sims agreed that he would not use the bank's confidential information for his personal benefit or for others. The bank's policy also required Sims to promptly disclose any conflicts or appearances of conflict with the bank's interests. Sims's scheme to defraud his employer lasted from February 2018 until at least April 2021.

From August 2018 to October 2020, Sims wired $86,000 in bank funds to the United States Treasury and California Franchise Tax Board to make payments towards the personal federal and state income taxes for himself and his wife. Sims concealed these transactions by creating false entries in the bank's general ledger that falsely represented that the payments were for the bank's tax accounts.

In April 2019, Sims used approximately $14,161 in bank funds to a debt collection agency to help pay off a debt that he had incurred. Sims concealed this transaction by creating a false entry in the bank's general ledger that falsely stated the payment was for data processing software.

From April 2019 to December 2020, Sims took approximately $113,264 in money belonging to the bank to pay the balances on his personal credit card. Sims hid these expenses in the bank's general ledger by falsely labeling them as bank expenses. During this time, he also siphoned approximately $81,815 from the bank by using a bank credit card, meant for work purposes, for his personal expenses, including steak dinners and a trip to Las Vegas.

From February 2020 to April 2021, Sims also lied to several bank employees by telling them they had to switch their bank-funded life insurance policies because of their age.

What neither the employees nor the bank knew was these policies were obtained through Sims's wife, a licensed life insurance broker who received a commission for each life policy she sold.

For some employees, Sims obtained their personal identifying information without their consent and then used this information to purchase life insurance policies from his wife. Sims used a checking account belonging to the bank to wire approximately $311,608 of the bank's money to several life insurance companies to partially pay for the premiums for these policies.

Later, when Sims was confronted about the life insurance policies opened using bank employees' personal identifying information, he lied by saying the employees' identities could have been stolen through a cybersecurity hack or by unauthorized disclosures by the bank's personnel department. Sims resigned from the bank shortly after being confronted about the life insurance policies.

In total, Sims unlawfully took $737,849 of bank funds for his personal use and benefit. (Source)

Credit Union Employee Sentenced To Prison For Role In $400,000 Identity Theft Fraud Scheme - June 6, 2024

Jalen McMillan used his position as a Member Service Representative at a federal credit union to facilitate both the opening of accounts in the names of identity theft victims and subsequent financial transactions, including assisting with loans. Co-defendant Archie Paul and his co-conspirators obtained, possessed, and used fictitious identities and the personal identifying information (PII) of real persons (Victims), which Paul and co-defendant John Fitzgerald Washington used to manufacture and procure false identification documents displaying the PII of the victims, but photographs of others.

Paul, co-defendant Tiffany Williams and others then used the false identification documents to impersonate the victims and with the help of McMillan and other conspirators, open bank accounts and conduct financial transactions in their names, including making large withdrawals from the victims' accounts.

In addition to the conspiracy and bank fraud charges, McMillan was convicted of aggravated identity theft for providing the identifying information of a bank customer to Paul, knowing that it would be used to facilitate the fraud. Specifically, the evidence proved that McMillan used his special access to the bank's customer database to steal confidential PII belonging to Victim 5, a customer at the bank.

McMillan provided that information to Paul. A co-conspirator subsequently opened a bank account using Victim 4's PII and Victim 5's banking information. McMillan serviced the transaction and assisted the co-conspirator in obtaining a $10,000 loan in Victim 4's name, which the co-conspirator immediately withdrew in cash.

Trial evidence proved that the conspirators intended to fraudulently obtain more than $400,000 from the bank and successfully defrauded the bank of more than $150,000. (Source)

Former Bank Manager Charged For Embezzling $250,000+ From Customers Accounts / Used Funds To Make Payments For House & Car - June 27, 2024

Eric Schouest was employed at Regions Bank from 2010 to 2021 as a Branch Banager overseeing business transactions and practices at the Regions Bank Plank Road branch in Louisiana.

Beginning in or about 2020, and continuing through in or about April 2021, Schouest embezzled funds from customer accounts and deposited the money into his personal bank accounts.

Schouest would also send false and fraudulent emails and forged documents to other Regions Bank employees to conceal his scheme. Schouest used some of the traceable fraudulent funds to make loan payments on personal items such as a house and a car. Through his scheme, Schouest caused a loss to Regions Bank of more than $250,000. (Source)

Former Bank Vice President Convicted Of Fraud & Money Laundering For Obtaining Millions Of Dollars In COVID Relief Funds - June 19, 2024

Anuli Okeke is the former Vice President and manager of a New York branch of Popular Bank.

Okeke was convicted of conspiracy to commit bank and wire fraud, wire fraud, bank fraud and money laundering conspiracy. The charges arose out of a scheme the defendant led to fraudulently obtain millions of dollars from the Paycheck Protection Program (PPP) and the Economic Injury Disaster Loan (EIDL) program during the height of the COVID-19 pandemic.

Okeke boasted about her earnings from the scheme. In handwritten notes found at her desk at work, she wrote "I am making more than enough money," "money comes to me easily," "I am grateful I make $15k every month," and "I have an extra $5000 every month." Around the time of the scheme, the defendant's bank accounts saw an influx of cash deposits.

7 other co-conspirators pled guilty to wire and bank fraud conspiracy in connection with the defendant's pandemic aid fraud conspiracy at the bank. (Source)

Wells Fargo Fires 12+ Employees For Simulation Of Keyboard Activity To Fake Working - June 13, 2024

Wells Fargo fired more than a dozen employees last month after investigating claims that they were faking work.

The staffers, all in the firm's wealth and investment-management unit, were "discharged after review of allegations involving simulation of keyboard activity creating impression of active work," according to disclosures filed with the Financial Industry Regulatory Authority.

Devices and software to imitate employee activity, sometimes known as "mouse movers" or "mouse jigglers," took off during the pandemic-spurred work-from-home era, with people swapping tips for using them on social-media sites Reddit and TikTok. Such gadgets are available on Amazon.com for less than $20.

It's unclear from the Finra disclosures whether the employees Wells Fargo fired were allegedly faking active work from home. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

Financial Advisory Firm Sues 4 Ex-Employees Who Abruptly Resigned & Stole Trade Secrets For Their New Firm - June 13, 2024

The resignation of four employees from a local wealth advisory firm who left without warning to launch their own firm, has led to a lawsuit and a judge ordering them to temporarily stop soliciting their former employer's clients.

Salomon & Ludwin (S&L), is a financial advisry firm that manages $1.7 Billion in client asset.

Last month the company sued former employees Jeremiah Winters, Kate Atwood, Jen Thompson and Abbey Sorensen for allegedly stealing trade secrets and wrongfully soliciting clients upon starting their new firm, Founders Grove Wealth Partners.

The lawsuit claims the former employee immediately announced their new firm and began messaging clients about the move that same day as their departure.

The suit claims the former employee have solicited potentially hundreds of S&L's clients in violation of their employment agreements. S&L claims those contracts included non-solicitation clauses and provisions that supersede a set of industry standards that guide financial advisors when jumping from one firm to another.

S&L's court filings and a press release disseminated by the firm says it has been and continues to be harmed by the exodus, which took four of its 12 employees. Winters and Atwood were two of the firm's four advisors. Thompson and Sorenson were two of its four operations employees. (Source)

Former Chief Operating Officer Implicated In Scheme To Steal Trade Secrets For His New Company - June 26, 2024

Aimbridge Hospitality filed a lawsuit against competitor Avion Hospitality and its President and CEO, Robert Burg, alleging Avion senior leadership solicited confidential business information and trade secrets from Aimbridge employees to compete unfairly in the marketplace.

Burg had worked or Aimbridge Hospitality for 16 years. Burg most recently served as Aimbridge Hospitality COO until he departed in 2021, the lawsuit claims, after another candidate was selected as CEO.

Following his departure, Burg formed Avion Hospitality and began pursuing Aimbridge's clients, Aimbridge alleges in the lawsuit.

The lawsuit claims Burg contrived a scheme to steal Aimbridge's trade secrets, and then use those secrets to convince hotel owners to fire Aimbridge and hire Avion in its place. The scheme resulted in Avion reaping tens of millions of dollars in ill gotten gains, Aimbridge alleges. (Source)

CHINESE ESPIONAGE / THEFT OF TRADE SECRETS INVOLVING U.S. GOVERNMENT / COMPANIES / UNIVERSITIES

Chinese Spies Are Targeting Disgruntled Workers Within U.S. Corporations Warns Director Of National Counterintelligence & Security Center - June 5, 2024

The U.S. needs to prepare for more cyberattacks from an increasing number of threat actors across the globe, with China being the biggest one, said Michael Casey, Director of the National Counterintelligence and Security Center.

China is "by far the most prolific actor out there and the one coming after us across the board and in the hardest way possible," he said at the CNBC CEO Council Summit in Washington, D.C.

Casey said there has been a 100% increase in cyber incidents and ransomware demands across the board. Over the years, he said, China realized that America's advantage in the world was technology and that made it a huge target. And it won't stop, "because it works, because they keep succeeding," Casey said. "China has published their list of desired technologies and then they go get it and it works."

Among the threats that CEOs need to have on their radar when it comes to any IP threat is a rise in the use of what he called "human assets." These are people within organizations that can be recruited to steal IP, data, or whatever the bad actor is targeting.

Given that CEOs and others in the C-suite can't keep track of every employee conversation and interaction around the globe, Casey told CNBC Senior Washington Correspondent Eamon Javers that the best course of action to stop nation states from recruiting human assets is to deploy a layered defense.

"A CEO needs to really look at what secrets a company wants to protect and then who needs to have access to that information," he said.

Another issue to focus on is the potential for employees to become human assets in the first place. "These are the employees who are having money problems, marital problems that someone can take advantage of," Casey said. That's why there needs to be a program in place to identify these employees and get them the help they need. "I'm stunned by the number of companies that have no concept of their insider threat," he added.

And with China and Russia already targeting critical U.S. infrastructure, such as water supplies, CEOs must run worst-case scenario drills should these systems be taken down.

"Leaders need to know what they would do if the worst thing happens," Casey said. (Source)

Employee / Resident Of China Pleads Guilty To Stealing Trade Secrets For His Own Business - June 13, 2024

Klaus Pflugbeil, a resident of the People's Republic of China and a Canadian and German national, pleaded guilty to conspiring to send trade secrets that belonged to a leading U.S.-based electric vehicle company . Pflugbeil and his co-defendant, Yilong Shao, who remains at large, are owners of a PRC-based business that sold technology used to make batteries, including batteries used in electric vehicles. (Source)

FOREIGN GOVERNMENTS EMBEDDING NON U.S. CITZIENS INTO U.S. COMPANIES

No Incidents To Report

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

193 Individuals Charged (Doctors, Nurses, Medical Professionals) For Participation In $2.75 BILLION Health Care Fraud Schemes - June 27, 2024

The Justice Department brought criminal charges against 193 defendants, including 76 doctors, nurse practitioners, and other licensed medical professionals in 32 federal districts across the United States, for their alleged participation in various health care fraud schemes involving approximately $2.75 billion in intended losses and $1.6 billion in actual losses.

The government seized over $231 million in cash, luxury vehicles, gold, and other assets.

The charges alleged include over $900 million fraud scheme committed in connection with amniotic wound grafts; the unlawful distribution of millions of pills of Adderall and other stimulants by five defendants associated with a digital technology company; an over $90 million fraud committed by corporate executives distributing adulterated and misbranded HIV medication;

over $146 million in fraudulent addiction treatment schemes; over $1.1 billion in telemedicine and laboratory fraud; and over $450 million in other health care fraud and opioid schemes. (Source)

Former Hospital CEO Pleads Guilty To Stealing $68,000+ In Hospital Funds For Personal Use / Caused Hospital To File For Bankruptcy - May 30, 2024

Charles Hatfield pleaded guilty and admitted that while serving as the Chief Executive Officer of Williamson Memorial Hospital he stole $34,872.62 in hospital funds for personal use and without authorization.

Hatfield became the hospital's interim CEO in September 2018. As CEO, Hatfield had control over the hospital's finances and bank accounts, directed payments of the hospital's funds, and had custody and control of the hospital's checkbook. Hatfield was the permanent CEO when he was relieved of those duties in September 2019. Around that time, on Oct. 21, 2019, the rural, 76-bed hospital filed for bankruptcy.

On May 16, 2019, Hatfield directed that $9,197.62 in hospital funds be used to purchase a cashier's check made payable to an individual at Venice Sands Apartments-Argus Management of Venice in Florida. Hatfield admitted that he used the hospital funded-check to settle a personal lawsuit demanding the payment of delinquent real estate taxes and homeowners' fees he owed for personal condominium property he owned in Venice.

On September 25, 2019, Hatfield directed the transfer of $25,675 in hospital funds to Mid Mountain Properties, a real estate company owned and operated by Hatfield. The transaction occurred just days prior to Hatfield being relieved as CEO, and shortly before the hospital filed for bankruptcy.

Hatfield admitted that he was aware that the hospital could not appropriately fund its employee benefits programs, including retirement and healthcare plans at the time he directed the transfer. Hatfield further admitted to telling his business partners that he used the transferred funds to pay a personal obligation.

Hatfield also admitted that he never requested or received authorization from the hospital's board of directors or anyone else at the hospital to direct the payments from the hospital to himself. (Source)

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

Chief Financial Officer For Media Company Charged With Participating In Scheme To Launder At Least $67 Million In Fraud Proceeds - June 3, 2024

From at least 2020, through May 2024, Bill Guan worked as the Chief Financial Officer of a multinational media company headquartered in New York.

Guan conspired with others to participate in a sprawling, transnational scheme to launder at least approximately $67 million of illegally obtained funds to bank accounts in the names of the media company and related entities, media entities.

In furtherance of the money laundering conspiracy, Guan managed, among other teams, the Media Company's "Make Money Online" team (MMO Team), which was located in a particular foreign office of the Media Company. Under Guan's management, members of the MMO Team and others used cryptocurrency to knowingly purchase tens of millions of dollars in crime proceeds, including proceeds of fraudulently obtained unemployment insurance benefits, that had been loaded onto tens of thousands of prepaid debit cards.

The crime proceeds were generally purchased by the scheme participants, including members of the MMO Team and others working with them, using a particular cryptocurrency platform, at discounted rates of approximately 70 to 80 cents per dollar, and in exchange for cryptocurrency.

Once the crime proceeds were purchased, the MMO Team and other participants in the scheme used stolen personal identification information to open accounts, including prepaid debit card accounts, cryptocurrency accounts, and bank accounts, that were used to transfer the crime proceeds into bank accounts associated with the Media Entities. After the crime proceeds reached those bank accounts, they were often further laundered through other bank accounts held by the Media Entities, GUAN's personal bank accounts, and through GUAN's personal cryptocurrency accounts.

In or around the same time the money laundering scheme began, the Media Company's internal financial accounting reflected an increased annual revenue over the previous year of approximately 410% from approximately $15 million to approximately $62 million.

When banks asked Guan about the increase in transactions entering the bank accounts of the Media Entities, Guan lied, including to two U.S.-based banks, and claimed that the increase in funds came from donations. However, in 2022, Guan wrote a letter addressed to a congressional office falsely stating donations constitute "an insignificant portion of the overall revenue" of the Media Company. (Source)

Company Finance Director Charged With Embezzling $5.7 Million - June 20, 2024

Paul Schnitzer worked as the Finance Director for his company. He embezzled at least approximately $5.7 million from his employer, a Florida-based portfolio company owned by a Massachusetts investment firm.

Between January 2022 and May 2024, Schnitzer made over 100 transfers, most disguised as "equity distributions," from the company's operating account into his personal account. To hide these transfers, Schnitzer allegedly provided falsified financial reports with inflated cash balances for the company to the investment firm. It is also alleged that Schnitzer secretly used a line of credit to replenish the company's operating account after he had stolen from it. (Source)

Former Energy Company President Sentenced To Prison For $5.5 Million+ Illegal Kickback & Commodities Insider Trading Scheme - June 7, 2024

Matthew Clark has been ordered to federal prison for his role in an illegal kickback scheme and a commodities insider trading scheme involving natural gas futures contracts. Clark must also pay $7,709,509 in restitution and forfeit $6,532,360.

Clark conspired with others to direct his employer's trades to a Houston based Classic Energy LLC, a brokerage firm operated by Matthew Webb, in exchange for illegal kickbacks. Clark received more than $5.5 million in illegal kickbacks for his trades. (Source)

Chief Financial Officer Sentenced To Prison For Embezzling $694,000+ - May 30, 2024

Between 2018 and 2020, John Casper misused his position as Chief Financial Officer (CFO) to embezzle more than $694,000 from the victim company.

Casper executed the embezzlement scheme by conducting approximately 112 unauthorized financial transactions, transferring funds from the victim company's accounts to bank accounts under Casper's control.

As the victim company's CFO, Casper used his access to the company's accounting system to disguise the fraud, by creating fake or incorrect financial entries in the company's books and records so that the victim company's books would reconcile. (Source)

Employee Sentenced To Prison For Stealing $430,000+ From Employer - June 24, 2024

Anthony Prizio is a former employer of a company that operates a national chain of second-hand retail stores.

From January 2019 until July 2021, while serving as manager of the company's Worcester store location, Prizio devised and carried out a scheme to steal over $430,000. As the store manager, Prizio had access to the store's timekeeping system for employees' working hours, human resources portal and un-activated payroll paycards issued to certain employees for wages. Prizio used his position as store manager to repeatedly enter false hours worked for employees, including employees who no longer worked there. Prizio caused payroll debit cards to be issued in others' names, which he then took for himself. Prizio used some or all of the wages for his own use on personal expenditures. Additionally, Prizio took steps to conceal his fraud by misrepresenting the productivity of the Worcester store to make it appear that the store processed more items, as well as by entering false paid sick and bereavement for employees to fraudulently cause payment for fictitious hours without adversely affecting the productivity measurement of the store. (Source)

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

Chief Financial Officer Charged With Embezzling $40 Million / Used Funds For Family & To Pay His Credit Cards Bills - June 5, 2024

William Smith is the former Chief Financial Officer for the Detroit Riverfront Conservancy (DRFC) in Michigan.

As early as November 2012, Smith orchestrated a scheme to embezzle millions of dollars in funds belonging to the DRFC. Smith carried out his embezzlement scheme in two distinct ways.

First, Smith is alleged to have used conservancy funds to pay for charges that he and his family accrued on an American Express account. Second, Smith is alleged to have diverted conservancy funds to a company he controlled called "The Joseph Group."

Neither of these sets of expenditures were authorized or approved by the Board of the DRFC; "The Joseph Group," was not an approved vendor and provided no services to the DRFC, and Smith had no authority to use Conservancy funds to pay his own personal credit card bills.

The complaint alleges that, between November 2012 and March 2024, Smith stole nearly $40 million from the DRFC through these two embezzlement streams. (Source)

Employee Assistant Sentenced To Prison For Embezzling $2.1 Million For 10 Years/ Used Funds To Pay Credit Card Bills - June 25, 2024

Christine Fletcher was a trusted assistant for over 38 years and worked directly for the business owner. Fletcher had access to several bank accounts and was often included in family affairs. She took advantage of her deeply trusted position by repeatedly embezzling funds for nearly ten years. Fletcher deposited funds into her personal accounts and paid personal credit card bills by forging the owner's deceased spouse's signature on hundreds of checks. Fletcher admitted that her motives were based solely on greed. She further admitted to agents that until she was confronted by the owner and fired, she had no idea how much she had stolen.

Fletcher was ordered to pay $2,188,870 to the business owner. (Source)

Employee Sentenced To Prison Stealing $536,000 From Employer For 7+ Years / Used Funds For Entertainment & Dining - June 18, 2024

From March 2014 until June 2021, Christine Bangs used her professional position as Operations Manager and access to her employer's credit card, bank accounts and payroll for her own personal gain.

Bangs used the corporate credit card to make approximately $197,936 in personal purchases, including $12,414.96 for tickets to a New England Patriots vs. Dallas Cowboys game, and stole an additional $255,645 from the victim by making approximately 213 wire transfers over the 7+ years. Of the money Bangs stole, she spent more than $176,000 on entertainment, tickets & dining. (Source)

Former Nonprofit Finance Director Pleads Guilty To Theft Of $514,000+ Of Government Funds For Personal Use - June 25, 2024

While employed as the Director of Finance and operations for Habitat for Humanity, Ashley Ingram applied for an employee retention tax credit for retaining employees during the COVID-19 pandemic from the IRS on behalf of Habitat for Humanity, but without the knowledge of the nonprofit.

Ingram then received checks totaling $388,550.75 from the United States Treasury and deposited the funds into a Habitat for Humanity account that she controlled. Ingram transferred the money from the Habitat for Humanity account into multiple personal bank accounts and appropriated it to her own use. In total, Ingram misappropriated approximately $514,672.37 from Habitat for Humanity and the United States Government. (Source)

Finance Manager For Firearms Manufacturer Admits To Stealing $159,000+ / Used Funds For Hotels, Collection Agencies, Etc. - June 11, 2024

From May 2018 until December 2021, Teri Bell worked as a Finance Manager for Falkor SID Inc., a firearm manufacturing and distribution business in Kalispell, Montana.

Bell was provided pre-signed checks to make payments to Falkor vendors and had access to Falkor's bank account and its accounting software. In the fall of 2021, Falkor's owners suspected Bell was stealing money from the company, and a financial audit determined that Bell completed 45 unauthorized transactions totaling $159,131 in Falkor funds. Bell wrote checks from Falkor to herself or her creditors and then edited the payments in an accounting system so that they appeared to be for legitimate business expenses. Bell used the stolen funds for personal expenses, including hotels in Las Vegas and at Quinn's Hot Springs, payments to retail and liquor stores, collection agencies and streaming services. (Source)

Fast Food Manager Pleads Guilty To Embezzling $140,000+ From Employer / Used Funds For Jewelry, Gambling & Adult Websites - June 13, 2024

Timothy Hill was employed by a company to manage a fast-food franchise restaurant at the Minneapolis St. Paul International Airport. In his position as manager, Hill was responsible for collecting and making daily cash deposits into a safe deposit box.

Between September 2022 and October 2023, Hill collected the daily cash receipts from the restaurant and instead of depositing it into the safe deposit box, pocketed some or all of the cash.

Hill attempted to conceal his embezzlement by using future cash receipts to cover his theft, creating a false impression that the cash deposits were delayed rather than stolen. To further conceal his embezzlement, Hill sent regular emails to the company's accounting personnel representing that he was belatedly depositing cash from earlier dates, when, in fact, he was using cash collected during the ensuing time period to conceal his embezzlement.

Hill spent the stolen cash on jewelry, online sports betting, and the adult website Only Fans, among other things. He also transferred thousands of dollars through CashApp to various individuals, including several female colleagues in exchange for personal photos and videos.

In total, Hill knowingly and willfully embezzled approximately $144,000 from the companyover a period of 13 months. (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

Former Employee Pleads Guilty For Role In $2.3 Million Embezzlement Scheme Using Fake Invoices / Used Funds For New Mercedes, Engagement Ring, Wedding - June 6, 2024

Priya Bhambi is a former senior level employee in the technology operations group of Takeda Pharmaceutical Company Limited (Takeda).

Between approximately January 2022 and October 2022, Bhambi and her alleged co-conspirator orchestrated and executed a scheme to defraud Takeda of at least $2.3 million in payments for purported consulting services by submitting fabricated invoices on behalf of a sham consulting company.

In February 2022, the co-conspirator, in coordination with Bhambi, allegedly incorporated Evoluzione Consulting LLC (Evoluzione). Later, Bhambi created a website for Evoluzione with false information, including fabricated blog posts, to make it appear that Evoluzione was a legitimate consulting business.

After incorporating Evoluzione, Bhambi, allegedly in coordination with the co-conspirator, submitted a statement of work to Takeda and caused Takeda to sign a master services agreement with Evoluzione and issue a purchase order to Evoluzione for consulting services with a total cost of $3.542 million. Then, between March and May of 2022, Bhambi and the alleged co-conspirator fabricated and submitted to Takeda five separate invoices for services that Evoluzione had not performed, each in the amount of $460,000.

When questioned by Takeda employees, Bhambi and the alleged co-conspirator made false representations regarding the services purportedly provided by Evoluzione. Takeda paid all five of the invoices to business accounts allegedly opened by the alleged co-conspirator in the name of Evoluzione.

In total, Bhambi and the alleged co-conspirator defrauded Takeda of $2.3 million in payments to Evoluzione for services not provided. Bhambi and her alleged co-conspirator used the fraudulently obtained funds to purchase a Mercedes-Benz Model E; purchase a diamond engagement ring; make a down payment on a $1.875 million condominium in Boston's Seaport neighborhood; and place a deposit on a wedding venue. (Source)

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

Disgruntled Ex-Employee Costs Company $670,000+ After He Deletes All 180 Test Servers After Being Terminated - June 2024

Kandula Nagaraju is a Indian national who worked at NCS (National Computer Systems) in Singapore.

NCS is a major IT services firm in South-East Asia and is headquartered in Singapore. It also has a presence across Australia, Hong Kong, China, and India, with over 13,000 employees. Nagaraju worked in the company's quality assurance computer system, where he and his team used test servers to run apps before they were deployed to customers and end users.
Nagaraju was given a two-year-eight-month sentence after the courts found him guilty of unauthorized access to computer material.

Nagaraju illegally accessed his former employer's systems for several months after his termination, running scripts that he could use to delete its test servers. After he completed testing, he deployed the scripts overnight, resulting in the complete removal of all 180 company test servers.

Nagaraju's contract was terminated in October 2022, allegedly due to poor performance, although he stayed in his office until November 16, 2022.

Nagaraju said he was confused and upset about the firing, especially as he felt he was performing well in his position. But since he didn't have another job lined up in Singapore after that, he left the nation-state and returned to his home country.

Although Nagaraju was no longer connected with NCS, he discovered that his credentials remained valid, giving him remote access to the company's servers. Between January and March 2023, he hatched a plan of revenge against his former employer. He Googled for server delete scripts during this time and, using his still valid credentials, began testing them on NCS's test servers.

None of his former team members were aware of this, allowing him to access the system over 13 times in March of 2023 alone. It was during this time that he perfected and hid the deletion scripts. Finally, on March 18 and 19, he activated the scripts, which began to delete the servers one at a time to minimize suspicion.

When the NCS QA team logged in on March 20, they discovered that their test servers were inaccessible. It was during their troubleshooting that they found out that all 180 of their test servers were deleted.

The incident cost the company $678,000 to remedy the situation. (Source)

THEFT OF ORGANIZATIONS ASSESTS

Luxury Jewelry Company Supervisor Pleads Guilty Tor Stealing & Selling Millions Of Dollars Worth Of Precious Metals - June 6, 2024

Since 2018, Benjamin Preacher worked fulltime in a supervisory position at a Rhode Island manufacturing facility operated by the company, which manufactures and sells luxury items, including jewelry made from gold, silver and platinum. It is alleged that Preacher used his position to steal precious metals from the company's facility in Rhode Island and then sell the metals to various businesses in Massachusetts.

From in or about March 2020 to March 2023, Preacher allegedly sold precious metals to a Canton-based metals dealer roughly one to two times per month, with sales to that dealer alone totaling more than $1 million.

It is alleged that Preacher's sales of stolen metals included $50,521 in 18-carat gold in March 2020, $21,821 in 18-carat gold, platinum scrap and "sterling" in April 2021 and $30,939 in platinum in January 2022.

It is further alleged that Preacher also sold more than $177,000 in stolen precious metals to a separate metals deales between on or about May 16, 2023 and Nov. 16, 2023.

This included gold sheets used by Preacher's employer in a particular machine, which Preacher allegedly stole and sold, along with other gold scrap, for nearly $21,000.

Most recently, it is alleged that, approximately 30 minutes into his shift on March 1, 2024, Preacher was captured on company security cameras stealing a piece of white gold "flat stock," measuring approximately an inch in diameter and approximately as thick as a quarter, valued at roughly $2,200.

Precious metal in scrap form were located and seized during a search of Preacher's home on March 14, 2024. (Source)

Automotive Dealership Parts Manager Pleads Guilty To Stealing & Selling $575,00+ In Parts - June 18, 2024

Bbetween approximately March 2019 and September 23, 2022, Robert McLane was employed by Formula Nissan, Inc., an automobile sales and service dealership located in central Vermont. During this period, McLane served as the Parts Manager and then the Director of Parts and Service at Formula Nissan. In his positions, McLane oversaw the parts and service departments; supervised other employees; and ordered, received, and paid for automotive parts needed in Formula Nissan's operations. In ordering, receiving, and paying for parts, McLane typically communicated with Formula Nissan's parts supplier, Nissan North America, using dealer management software.

Starting around January 2021 and continuing until September 2022, McLane began defrauding Formula Nissan by ordering certain vehicle parts from Nissan North America. Many of the parts McLane ordered were vehicle suspension lift kits. The cost to Formula Nissan of each lift kit was in the $2,300 to $2,900 range. Nissan North America billed, and Formula Nissan subsequently paid, for the lift kits McLane had ordered.

As part of the scheme, McLane refrained from ordering the lift kits via the dealer management software parts ordering system. As a result of this bypass, the parts McLane ordered were not entered into Formula Nissan's inventory of parts-on-hand.

Instead of selling the lift kits for the benefit of Formula Nissan, McLane advertised them for sale on Facebook at prices substantially discounted from their wholesale cost to Formula Nissan. Over the course of the scheme, McLane sold more than 200 lift kits to persons around the United States. Purchasers paid for the lift kits via transfers of funds to a personal PayPal account that McLane maintained in his own name. He shipped lift kits to his own customers by using Formula Nissan's Federal Express account. McLane then used the fraudulently obtained proceeds for his own benefit.

As a result of McLane's fraud, Formula Nissan and its insurance company suffered an out-of-pocket loss of at least $575,000. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

Chief Operating Officer Of International Cargo Airline Sentenced To Prison For Role With 9 Other Individuals For $23 Million Kickback Scheme Over 12 Years - May 30, 2024

From at least about 2009 through about July 2021, Lars Winkelbauer and at least 9 other individuals participated in a massive scheme to defraud Polar Air Cargo. At all relevant times, Winkelbauer and 3 co-defendants were senior executives of Polar, and 6 co-defendants owned and operated various Polar vendors and customers.

The senior executives of Polar agreed to accept millions of dollars in kickbacks from the vendors, and also reaped substantial financial benefits as a result of their secret ownership interests in certain Polar vendors, in exchange for ensuring that those vendors received favorable business arrangements with Polar.

The fraud they perpetrated involved a substantial portion of Polar's senior management and at least 10 customers and vendors of Polar, which led to pervasive corruption of Polar's business, touching nearly every aspect of the company's operations for over a decade.

As a result of the scheme, the senior executives, along with 2 co-conspirators who also worked as senior executives at Polar, received unlawful payments, either directly or through various limited liability companies they controlled, in excess of approximately $23 million in kickback payments or disbursements as a result of their ownership of conflicted companies.

Winkelbauer was Polar's Chief Operating Officer and Executive Vice President and was the most senior of the executives. He personally received kickbacks connected to approximately 11 separate vendors or customers of Polar totaling over $6 million.

He also attempted to conceal the illegal kickback payments through a sophisticated money laundering scheme, including via falsified invoices and the use of shell companies in China. (Source)

EMPLOYEE DRUG RELATED INCIDENTS

Employee Sentenced To Prison For Selling His Co-Worker Fentanyl Pills That Resulted In The Co-Worker's Death - June 20, 2024

On May 17, 2022, Tanner Goforth met his friend and co-worker, the victim, at a local gas station where Goforth sold the victim 10 fentanyl pills. The victim went home, ingested the fentanyl intravenously, and died almost immediately. Nearly a half hour later, his girlfriend found him in their bathroom, called 911, and began performing CPR. Police department officers arrived on scene and attempted life-saving measures. Unfortunately, the victim was unable to be resuscitated. (Source)

6 Amsterdam Airport Employees Belonging To Drug Trafficking Organizations Arrested For Cocaine Trafficking - May 31, 2024

At least six employees of companies operating at the Schiphol Airport in Amsterdam have been arrested by Dutch security forces, accused of international cocaine trafficking.

The employee have been accused of introducing cocaine shipments into the country through the air terminal or carrying out preparatory acts to do so.

The suspects are all men aged 32 to 51. They came from several Dutch cities and belonged to a criminal organization dedicated to drug trafficking through the airport. They worked at logistics, transport, and parcel-delivering companies in and around the airport. (Source)

Hospital Nurse Sentenced To Prison For Stealing Intravenous Fentanyl For Her Drug Addiction - June 13, 2024

In March 2021, while working at a Massachusetts hospital, Caroline Sheehan removed a bag of intravenous fentanyl solution from an automated dispensing machine. Sheehan used a syringe to remove fentanyl from the IV bag, injected saline into the bag to replace the fentanyl she had removed and returned the bag to its drawer in the machine.

A hospital employee saw a blood stain on the IV bag and removed the IV bag, which laboratory testing confirmed contained less than the declared concentration of fentanyl, from the machine before any of the adulterated fentanyl solution was administered to a patient. Sheehan later admitted that she had withdrawn fentanyl from the IV bag and replaced it with saline to avoid getting caught. Sheehan later admitted that she had been stealing prescription drugs from the hospital for months, replacing the siphoned drugs with saline solution, to feed her substance abuse addiction. (Source)

OTHER FORMS OF INSIDER THREATS

U.S. IT Services Firm Fined $38,000 For Whites Only Job Posting By Disgruntled Recruiter – May 28, 2024

A company whose job advertisement sought only white, US-born applicants has agreed to pay a $38,500 (£30,000) fine, the federal government has announced.

The advertisment from Arthur Grand Technologies was "generated by a disgruntled recruiter in India and was intended to embarrass the company", the justice department said. It was found to violate both federal civil rights and labour laws.

Arthur Grand will pay $7,500 in civil penalties to the US treasury as well as $31,000 in total compensation to people who filed complaints over the incident.

The Virginia-based IT services firm has served federal and commercial clients since 2012, according to its website.

In March 2023, a recruiter working for its subsidiary in India posted an advertisement for a Salesforce business analyst and insurance claims vacancy on the Indeed job-hunting website.

In bolded text, the long-term contract role includes a note: "Only Born US Citizens [White] who are local within 60 miles from Dallas, TX [Don’t share with candidates]".

The position lists clients as including HTC Global in Michigan and Berkshire Hathaway in Nebraska.

As part of its settlement agreement with the two federal agencies, Arthur Grand is also required to train its employees on the U.S. Immigration and Nationality Act, which bars hiring or firing people based on their citizenship status and national origin. It must also revise its employment policies and undergo justice department monitoring.

In a statement to CNN, the company's CEO said it "vehemently denies any guilt or wrongdoing". “This unauthorized posting was made by an upset employee on a Performance Improvement Plan (PIP) from their personal email address and account," Sheik Rahmathullah said.

"Upon discovering this, we took immediate and decisive action to ensure that this type of incident will never happen again, including the immediate termination of the responsible employee.” (Source)

MASS LAYOFF OF EMPLOYEES' AND RESULTING INCIDENTS

No Incidents To Report

EMPLOYEES' NON-MALICIOUS ACTIONS CAUSING DAMAGE TO ORGANIZATION

No Incidents To Report

EMPLOYEES' MALICIOUS ACTIONS CAUSING EMPLOYEE LAYOFFS OR CAUSING COMPANY TO CEASE OPERATIONS

No Incidents To Report

WORKPLACE VIOLENCE / OTHER FORMS OF VIOLENCE BY EMPLOYEES'

Disgruntled Worker Shoots 5 People / Killing 2 - May 22, 2024

Chester Police in Pennsylvania stated that a shooting happened on May 22, 2024 at a linen company.

At least five people, including the gunman's supervisor were shot, and two had died after showing up for work. The shooting took place inside and outside the business and a handgun was used.

The shooter was an angry" worker who had issues and confrontations with colleagues in the past, including on Tuesday and early Wednesday before the incident. There were no signs pointing to the shooting taking place.

Police from nearby Trainer, Pennsylvania, stopped the shooter's car after a description of the suspect's vehicle was released. The suspected shooter was arrested by police. (Source)

Employee Dies After Being Shot Outside Workplace By Boyfriend - March 25, 2024

An ex-boyfriend (Tevin Leach) is facing a first degree murder charge for shooting and killing Barbee Battle in an isolated domestic violence-related incident.

Police say that Battle was inside the building when Leach came inside and asked her to come outside.

"I told her, don't go outside. I was getting ready to lock the door. I was on the phone with 911 but then I hung up the phone. They called me back. Battle told me it was OK. and I said, don't go out there. Then she went out there and we heard the shots," said fellow employee Kim Chance.

Leach faces a murder charge in addition to a string of arrests before for other charges including assault on a female. (Source)

EMPLOYEES' INVOLVED IN TERRORISM

No Incidents To Report

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

DEFINITIONS OF INSIDER THREATS

The definition of Insider Threats can be vast, and must go beyond current definitions (By Sources Such As: National Insider Threat Policy, NISPOM Conforming Change 2 & Other Sources) and be expanded.

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

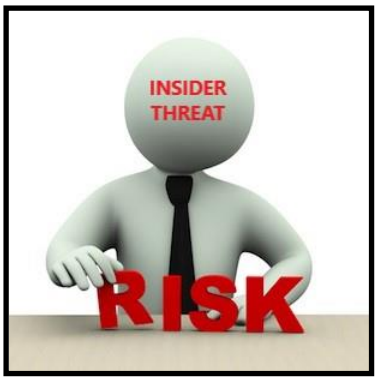
TYPES OF INSIDER THREATS DISCOVERED THROUGH RESEARCH

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

ORGANIZATIONS IMPACTED

TYPES OF ORGANIIZATIONS THAT HAVE EXPERIENCED INSIDER THREAT INCIDENTS

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



INSIDER THREAT DAMAGES / IMPACTS

The Damages From An Insider Threat Incident Can Many:

Financial Loss

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

Operational Impact / Ability Of The Business To Execute Its Mission

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

Reputation Impact

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

Workplace Culture - Impact On Employees'

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

Legal & Liability Impacts (External Costs)

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

DISSATISFACTION, REVENGE, ANGER, GRIEVANCES (EMOTION BASED)

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

MONEY / GREED / FINANCIAL HARDSHIPS / STRESS / OPPORTUNIST

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

IDEOLOGY

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

COERCION / MANIPULATION BY OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

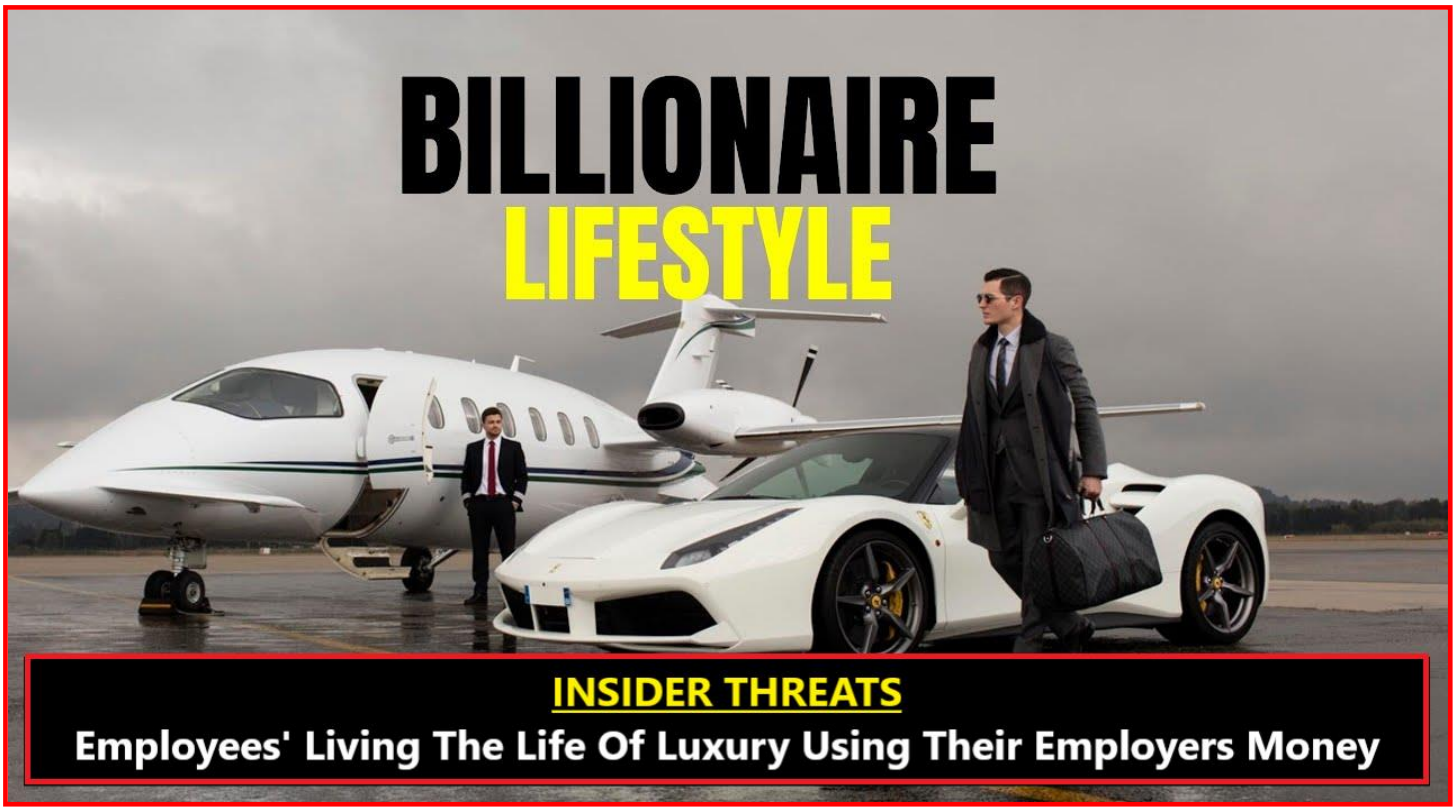
- ☐ Bribery, Extortion, Blackmail

COLLUSION WITH OTHER EMPLOYEES / EXTERNAL INDIVIDUALS

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

OTHER

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



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

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

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

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

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

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

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS 2024 REPORT ON FRAUD

If you are an Insider Risk Program Manager, or support the program, you should read this report. Insider Risk Program Managers should print the infographics on the links below, and discuss them with the CEO and other key stakeholders that support the Insider Risk Management Program. If there is someone else within the organization who is responsible for fraud, the Insider Risk Program Manager should be collaborating with this person very closely.

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. There continues to be a drastic increase in financial fraud and embezzlement committed by employees'.

Could your organization rebound / recover from the severe impacts that an Insider Threat incident can cause?

Has the Insider Risk Program Manager conducted a gap analysis, to analyze the capabilities of your organizations existing Network Security / Insider Threat Detection Tools to detect fraud?

Can your organizations Insider Threat Detection Tools detect an employee creating a shell company, and then billing the organization with an invoice for services that are never performed?

This report states that more than half of frauds occurred due to lack of internal controls or an override of existing internal controls.

This report is based on **1,921** real cases of occupational fraud, includes data from **138** countries and territories, covers **22** major industries and explores the costs, schemes, victims and perpetrators of fraud. These fraud cases caused losses of more than **$3.1 BILLION**. (Download Report)

Key Findings From Report / Infographic
Fraud Scheme Types, How Fraud Is Detected, Types Of Victim Organizations, Actions Organizations Took Against Employees, Etc. (Source)

Behavioral Red Flags / Infographic
Fraudsters commonly display distinct behaviors that can serve as warning signs of their misdeeds. Organizations can improve their anti-fraud programs by taking these behavioral red flags into consideration when designing and implementing fraud prevention and detection measures. (Source)

Profile Of Fraudsters / Infographic
Most fraudsters were employees or managers, but **FRAUDS PERPETRATED BY OWNERS AND EXECUTIVES WERETHE COSTLIEST**. (Source)

Fraud In Government Organization's / Infographic

How Are Organization Responding To Employee Fraud / Infographic
Outcomes in fraud cases can vary based on the role of the perpetrator, the type of scheme, the losses incurred, and how the victim organization chooses to pursue the matter. Whether they handle the fraud internally or through external legal actions, organizations must decide on the best course of action. (Source)

Providing Fraud Awareness Training To The Workforce / Info Graphic
Providing fraud awareness training to staff at all levels of an organization is a vital part of a comprehensive anti-fraud program. Our study shows that training employees, managers, and executives about the risks and costs of fraud can help reduce fraud losses and ensure frauds are caught more quickly. **43% of frauds were detected by a tip**. (Source)

FRAUD RESOURCES

ASSOCIATION OF CERTIFIED FRAUD EXAMINERS

Fraud Risk Schemes Assessment Guide

Fraud Risk Management Scorecards

Other Tools

DEPARTMENT OF DEFENSE FRAUD DETECTION RESOURCES

General Fraud Indicators & Management Related Fraud Indicators

Fraud Red Flags & Indicators

Comprehensive List Of Fraud Indicators

SEVERE IMPACTS FROM INSIDER THREATS INCIDENTS

EMPLOYEE EXTORTION

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

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

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

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

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

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

DATA / COMPUTER - NETWORK SABOTAGE & MISUSE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Two days later, on May 21, 2021, Barile remotely accessed the Credit Union's file server and deleted more than 20,000 files and almost 3,500 directories, totaling approximately 21.3 gigabytes of data.

The deleted data included files related to mortgage loan applications and the Credit Union's anti-ransomware protection software. Barile also opened confidential files.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Tipton and his brother Tommy Tipton were subsequently accused of rigging other lottery drawings, dating back as far as 2005.

Based on forensic examination of the random number generator that had been used in a 2007 Wisconsin lottery incident, investigators discovered that Eddie Tipton programmed a lottery random number generator to produce special results if the lottery numbers were drawn on certain days of the year.

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

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

UNDERAPPRECIATED / OVERWORKED / NO OVERSIGHT

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

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

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

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

DESTRUCTION OF EMPLOYERS PROPERTY BY EMPLOYEES

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

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

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

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

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

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

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

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

EMPLOYEES' WHO LOST JOBS / COMPANY GOES OUT OF BUSINESS

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

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

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

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

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

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

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

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

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

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

Former Employee Admits To Participating In $17 Million Bank Fraud Scheme / Company Goes Out Of Business - April 17, 2024

A former employee (Nitin Vats) of a now-defunct New Jersey based marble and granite wholesaler, admitted his role in a scheme to defraud a bank in connection with a secured line of credit.

From March 2016 through March 2018, an owner and employees of Lotus Exim International Inc. (LEI), including Vats, conspired to obtain from the victim bank a $17 million line of credit by fraudulent means. The victim bank extended LEI the line of credit, believing it to have been secured in part by LEI's accounts receivable. In reality, the conspirators had fabricated and inflated many of the accounts receivable, ultimately leading to LEI defaulting on the line of credit.

To conceal the lack of sufficient collateral, Vats created fake email addresses on behalf of LEI's customers so that other LEI employees could pose as those customers and answer the victim bank's and outside auditor's inquiries about the accounts receivable.

The scheme involved numerous fraudulent accounts receivable where the outstanding balances were either inflated or entirely fabricated. The scheme caused the victim bank losses of approximately $17 million. (Source)

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

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

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

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

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

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

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

As a result of Cipolletti's actions and subsequent attempts to cover up the scheme, in May 2018, Discovery Tours abruptly ended operations and filed for bankruptcy.

Student trips to Washington, D.C. were canceled for dozens of schools across Ohio and more than 5,000 families lost the money they had previously paid for trip fees.

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

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

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

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

In reality, SFCU had not met all conditions precedent to closing and had suffered a material adverse effect. Unbeknownst to the United States Department of the Treasury, the SFCU was in a financial crisis. From 2015 through 2017, another individual who was the Chief Financial Officer (CFO) of SFCU had been falsifying reports. In addition, she was creating fictitious entries in the banks records to support the false reports.

This created the illusion that SFCU was profitable when, in fact, the bank was failing. The CFO embezzled approximately $1.5 million from the credit union.

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

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

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

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

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

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

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

Lyons initiated the fraud shortly after he became CEO in 1999.

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

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

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

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

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

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

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

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

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

VERY DAMAGING FRAUD SCHEMES BY EMPLOYEES'

2 Former Employees Of Mortgage Lending Business Charged For Roles In $1.4 BILLION+ Mortgage Loan Fraud Scheme

Christopher Gallo and Mehmet Elmas were previously employed by a New Jersey-based, privately owned licensed residential mortgage lending business. Gallo was employed as a Senior Loan Officer and Elmas was a Mortgage Loan Officer and Gallo's assistant.

From 2018 through October 2023, Gallo and Elmas used their positions to conspire and engage in a fraudulent scheme to falsify loan origination documents sent to mortgage lenders in New Jersey and elsewhere, including their former employer, to fraudulently obtain mortgage loans. Gallo and Elmas routinely mislead mortgage lenders about the intended use of properties to fraudulently secure lower mortgage interest rates. Gallo and Elmas often submitted loan applications falsely stating that the listed borrowers were the primary residents of certain proprieties when, in fact, those properties were intended to be used as rental or investment properties.

By fraudulently misleading lenders about the true intended use of the properties, Gallo and Elmas secured and profited from mortgage loans that were approved at lower interest rates.

The conspiracy also included falsifying property records, including building safety and financial information of prospective borrowers to facilitate mortgage loan approval. Between 2018 through October 2023, Gallo originated more than $1.4 billion in loans. (Source)

COLLUSION – HOW MANY EMPLOYEES' OR INDIVIDUALS CAN BE INVLOVED?

70 Current & Former New York City Housing Authority Employees Charged With $2 Million Bribery, Extortion And Contract Fraud Offenses - February 6, 2024

The defendants, all of whom were NYCHA employees during the time of the relevant conduct, demanded and received cash in exchange for NYCHA contracts by either requiring contractors to pay up front in order to be awarded the contracts or requiring payment after the contractor finished the work and needed a NYCHA employee to sign off on the completed job so the contractor could receive payment from NYCHA.

The defendants typically demanded approximately 10% to 20% of the contract value, between $500 and $2,000 depending on the size of the contract, but some defendants demanded even higher amounts. In total, these defendants demanded over $2 million in corrupt payments from contractors in exchange for awarding over $13 million worth of no-bid contracts. (Source)

Former University Financial Advisor Sentenced To Prison For $5.6 Million+ Wire Fraud Financial Aid Scheme (Over 15 Years - Involving 60+ Students) - August 30, 2023

As detailed in court documents and his plea agreement, from about 2006 until approximately 2021, Randolph Stanley and his co-conspirators engaged in a scheme to defraud the U.S. Department of Education. Stanley, was employed as a Financial Advisor at a University headquartered in Adelphi, Maryland. He and his co-conspirators recruited over 60 individuals (Student Participants) to apply for and enroll in post-graduate programs at more than eight academic institutions. Stanley and his co-conspirators told Student Participants that they would assist with the coursework for these programs, including completing assignments and participating in online classes on behalf of the Student Participants, in exchange for a fee. As a result, the Student Participants fraudulently received credit for the courses, and in many cases, degrees from the Schools, without doing the necessary work.

Stanley also admitted that he and his co-conspirators directed the Student Participants to apply for federal student loans. Many of the Student Participant were not qualified for the programs to which they applied. Student Participants, as well as Stanley himself, were awarded tuition, which went directly to the Schools and at least 60 Student Participants also received student loan refunds, which the Schools disbursed to Student Participants after collecting the tuition. Stanley, as the ringleader of the scheme, kept a portion of each of the students' loan refunds.

The Judge ordered that Stanley must pay restitution in the full amount of the victims' losses, which is at least $5,648,238, the outstanding balance on all federal student loans that Stanley obtained on behalf of himself and others as part of the scheme. (Source)

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

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

Washington Federal was closed in 2017 after the Office of the Comptroller of the Currency determined that the bank was insolvent and had at least $66 million in nonperforming loans. A federal investigation led to criminal charges against 16 defendants, including charges against the bank's Chief Financial Officer, Treasurer, and other high-ranking employees, for conspiring to embezzle at least $31 million in bank funds. Eight defendants have pleaded guilty or entered into agreements to cooperate with the government. (Source)

5 Current And Former Police Officers Convicted In $3 Million+ COVID-19 Loan Scheme Involving 200 Individuals - April 6, 2023

Former Fulton County Sheriff's Office deputy Katrina Lawson has been found guilty of conspiracy to commit wire fraud, wire fraud, bank fraud, mail fraud, and money laundering in connection with a wide-ranging Paycheck Protection Program and Economic Injury Disaster Loan program small business loan scheme.

On August 11, 2020, agents from the U.S. Postal Inspection Service (USPIS) conducted a search at Alicia Quarterman's residence in Fayetteville, Georgia related to an ongoing narcotics trafficking investigation. Inspectors seized Quarterman's cell phone and a notebook during the search.

In the phone and notebook, law enforcement discovered evidence of a Paycheck Protection Program (PPP) and Economic Injury Disaster Loan (EIDL) program scheme masterminded by Lawson (Quarterman's distant relative and best friend). Lawson's cell phone was also seized later as a part of the investigation.

Lawson and Quarterman recruited several other people, who did not actually own registered businesses, to provide them with their personal and banking information. Once Lawson ultimately obtained that information, she completed fraudulent applications and submitted them to the Small Business Administration and banks for forgivable small business loans and grants.

Lawson was responsible for recruiting more than 200 individuals to participate in this PPP and EIDL fraud scheme. Three of the individuals she recruited were active sheriff's deputies and one was a former U.S. Army military policeman. Lawson submitted PPP and EIDL applications seeking over $6 million in funds earmarked to save small businesses from the impacts of COVID-19. She and her co-conspirators ultimately stole more than $3 Million. Lawson used a portion of these funds to purchase a $74,492 Mercedes Benz, a $13,500 Kawasaki motorcycle, $9000 worth of liposuction, and several other expensive items. (Source)

Former President Of Building And Construction Trades Council Sentenced To Prison For Accepting $140,000+ In Bribes / 10 Other Union Officials Sentenced For Accepting Bribes And Illegal Payments - May 18, 2023

James Cahill was the President of the New York State Building and Construction Trades Council (NYS Trades Council), which represents over 200,000 unionized construction workers, a member of the Executive Council for the New York State American Federation of Labor and Congress of Industrial Organizations (NYS AFL-CIO), and formerly a union representative of the United Association of Journeymen and Apprentices of the Plumbing and Pipefitting Industry of the United States and Canada (UA).

From about October 2018 to October 2020, Cahill accepted approximately $44,500 in bribes from Employer-1, as well as other benefits, including home appliances and free labor on Cahill's vacation home.

Cahill acknowledged having previously accepted at least approximately $100,000 of additional bribes from Employer-1 in connection with Cahill's union positions. As the leader of the conspiracy, Cahill introduced Employer-1 to many of the other defendants, while advising Employer-1 that Employer-1 could reap the benefits of being associated with the unions without actually signing union agreements or employing union workers. (Source)

WORKPLACE VIOLENCE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

FBI Indianapolis Special Agent in Charge Paul Keenan said Hole's focus on proving his masculinity was partially connected to a failed attempt to live on his own, which ended with him moving back into his old house.

Investigators also learned Hole aspired to join the military. Authorities said he had been eating MREs, or meals ready-to-eat, like those consumed by members of the armed forces.

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

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

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

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

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

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

On March 27, 2016, a concerned citizen contacted the Federal Bureau of Investigation and indicated that the person who committed the crime was likely a former Xerox employee named Richard Wilbern.

The citizen indicated that the defendant worked for Xerox prior to the robbery but had been fired. The citizen also stated that they recognized Wilbern's face from the photos.

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

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

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

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

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

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

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

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

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

WORKPLACE VIOLENCE (WPV) INSIDER THREAT INCIDENTS E-MAGAZINE

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

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

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

WORKPLACE VIOLENCE TODAY E-MAGAZINE

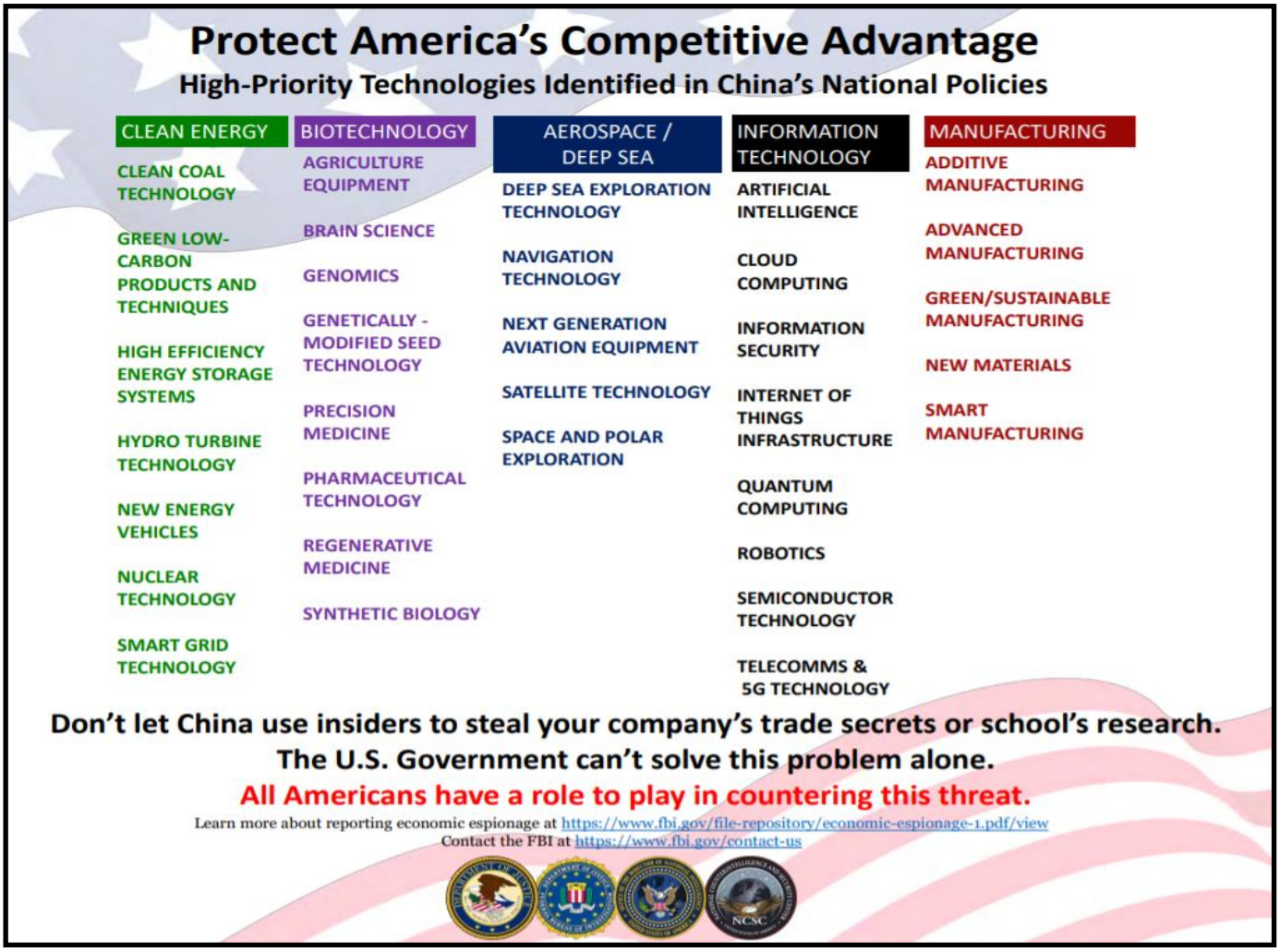
https://www.workplaceviolence911.com/node/994

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

CTTP = China Thousand Talents Plan

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

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



SOURCES FOR INSIDER THREAT INCIDENT POSTINGS

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

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

INSIDER THREAT INCIDENTS E-MAGAZINE

2014 To Present / Updated Daily

The Insider Threat Incidents E-Magazine contains the largest publicly available source of Insider Threat incidents (**5,400+ Incidents**).

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

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

INSIDER THREAT INCIDENTS MONTHLY REPORTS

July 2021 To Present

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

INSIDER THREAT INCIDENTS SPOTLIGHT REPORT FOR 2023

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

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

INSIDER THREAT INCIDENTS POSTINGS WITH DETAILS

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

Incident Posting Notifications

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

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

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

INSIDER THREAT INCIDENTS POSTINGS ON TWITTER

Updated Daily

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

CRITICAL INFRASTRUCTURE INSIDER THREAT INCIDENTS

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

National Insider Threat Special Interest Group (NITSIG)

U.S. / Global Insider Risk Management (IRM) Information Sharing & Analysis Center
Educational Center Of Excellence For IRM & Security Professionals

NITSIG Overview

The NITSIG was created in 2014 to function as a National Insider Threat Information Sharing & Analysis Center, as no such ISAC existed. The NITSIG has been successful in bringing together IRM and other security professionals from the U.S. Government, Department of Defense, Intelligence Community Agencies, universities and private sector businesses, to enhance the collaboration and sharing of information, best practices and resources related to IRM. This has enabled the NITSIG membership to be much more effective in identifying, responding to and mitigating Insider Risks and Threats.

NITSIG Membership

The NITSIG Membership (**Free**) is the largest network (**1000+**) of IRM professionals in the U.S. and globally. Our member's willingness to share information has been the driving force that has made the NITSIG very successful.

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

- ✓ Insider Risk Management Programs (Development, Management & Optimization)
- ✓ Insider Risk Management Program Working Group / Hub Operations
- ✓ Insider Threat Awareness Training
- ✓ Insider Risk / Threat Assessments & Mitigation Strategies
- ✓ Insider Threat Detection Tools (UAM, UBA, DLP, SEIM) (Requirements Analysis & Purchasing Guidance
- ✓ Employee Continuous Monitoring & Reporting Programs
- ✓ Insider Threat Awareness Training
- ✓ Workplace Violence Guidance / Active Shooter Response Guidance & Training

NITSIG Meetings

The NITSIG provides education and guidance to the membership via in person meetings, webinars and other events, that is practical, strategic, operational and tactical in nature. Many members have even stated the NITSIG is like having a team of IRM experts at their disposal FREE OF CHARGE. 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

NITSIG IRM Resources

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

NITSIG LinkedIn Group

The NITSIG has created a Linked Group for individuals that are interested in sharing and gaining in-depth knowledge related to IRM and IRM Programs. This group will also enable the NITSIG to share the latest news and upcoming events. We invite you to join the NITSIG LinkedIn Group. You do not have to be a NITSIG member to be join this group: https://www.linkedin.com/groups/12277699

NITSIG Insider Threat Symposium & Expo

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 Insider Threat Program Managers / Insider Risk Program Managers with ***Hands On Experience***.

At the expo are many vendors that showcase their training, services and products. This link provides all the vendors that exhibited at the 2019 ITS&E, and provides a description of their solutions for Insider Threat detection and mitigation.

ITS&E events were not held in 2020 to 2023 because of COVID. The next ITS&E is scheduled for March 4, 2025 at the John Hopkins University Applied Physics Lab in Laurel, Maryland

The ITS&E provides attendees with access to a large network of security professionals for collaborating with on all aspects of IRM.

NITSIG Advisory Board

The NITSIG Advisory Board (AB) is comprised of IRM Subject Matter Experts with extensive experience in IRM Programs. AB members have managed U.S. Government Insider Threat Programs, or currently manage or support industry and academia IRM Programs. Advisory board members will provide oversight and educational / strategic guidance to support the mission of the NITSIG, and also help to facilitate building relationships with individuals that manage or support IRM Programs. The link below provided a summary of AB members' backgrounds and experience in IRM.
https://www.nationalinsiderthreatsig.org/aboutnitsig.html

INSIDER THREAT DEFENSE GROUP

Insider Risk Management Program Experts

Since 2014, the Insider Threat Defense Group (ITDG) has had a long standing reputation of providing our clients with proven experience, past performance and exceptional satisfaction.

The ITDG offers the most affordable, comprehensive and practical training courses and consulting services to help organizations develop, implement, manage and optimize an Insider Risk Management Program.

Over **1000+** individuals have attended our highly sought after Insider Threat Program (ITP) Development, Management & Optimization Training Course (Classroom & Live Web Based) and received ITP Manager Certificates.

The ITDG are experts at providing guidance to help build Insider Threat Programs (For U.S. Government Agencies, Defense Contractors) and Insider Risk Management Programs for Fortune 100 / 500 companies and others. We know what the many internal challenges are that an Insider Risk Program Manager may face. There are many interconnected cross departmental components and complexities that are needed for comprehensive Insider Risk Management. We will provide the training, guidance and resources to ensure that the Insider Risk Program Manager and key stakeholders are universally aligned from an enterprise / holistic perspective to detect and mitigate Insider Risks and Threats.

INSIDER RISK MANAGEMENT (IRM) PROGRAM CONSULTING SERVICES OFFERED

Conducted Via Classroom / Onsite / Web Based

- ✓ Executive Management & Stakeholder Briefings For IRM
- ✓ IRM Program Training & Workshops For C-Suite, Insider Risk Program Manager / Working Group, Insider Threat Analysts & Investigators
- ✓ IRM Program Development, Management & Optimization Training & Related Courses
- ✓ Insider Risk - Threat Vulnerability Assessments
- ✓ IRM Program Maturity Evaluation, Gap Analysis & Strategic Planning Guidance
- ✓ Insider Threat Awareness Training For Employees'
- ✓ Insider Threat Detection Tool Gap Analysis & Pre-Purchasing Guidance / Solutions
- ✓ Data Exfiltration Assessment (Executing The Malicious Insiders Playbook Of Tactics)
- ✓ Technical Surveillance Counter-Measures Inspections (Covert Audio / Video Device Detection)
- ✓ Employee Continuous Monitoring & Reporting Services (External Data Sources)
- ✓ Customized IRM Consulting Services For Our Clients

The ITDG Has Provided IRM Training / Consulting Services To An Impressive List Of Clients:

White House, U.S. Government Agencies, Department Of Defense (U.S. Army, Navy, Air Force & Space Force, Marines), Intelligence Community Agencies (DIA, NSA, NGA), Law Enforcement (DHS, TSA, FBI, U.S. Secret Service, DEA, Police Departments), Critical Infrastructure Providers, Universities, Fortune 100 / 500 companies and others; Microsoft, Verzion, Walmart, Home Depot, Nike, Tesla, Dell Technologies, Nationwide Insurance, 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 **675+** organizations. (Client Listing)

Additional Background Information On ITDG

Mr. Henderson is the CEO of the ITDG, Founder / Chairman of the NITSIG and Founder / Director of the Insider Threat Symposium & Expo (ITS&E). Combining NITSG meetings, ITS&E events and ITDG training / consulting services, the NITSIG and ITDG have provided IRM Guidance and Training to **3,400+** individuals.

The NSA previously awarded the ITDG a contract for an Information Systems Security Program / IRM Training Course. This course was taught to **100** NSA Security Professionals (ISSM / ISSO), the DoD, Navy, National Nuclear Security Administration, Department of Energy National Labs, and to many other organizations

Please contact the ITDG with any questions regarding our training and consulting services.

Jim Henderson, CISSP, CCISO
CEO Insider Threat Defense Group, Inc.
Insider Threat Program (ITP) Development, Management & Optimization Training Course Instructor
Insider Risk / Threat Vulnerability Assessment Specialist
ITP Gap Analysis / Evaluation & Optimization Expert
LinkedIn ITDG Company Profile
Follow Us On Twitter / X: @InsiderThreatDG

Founder / Chairman Of The National Insider Threat Special Interest Group
Founder / Director Of Insider Threat Symposium & Expo
Insider Threat Researcher / Speaker
FBI InfraGard Members
LinkedIn NITSIG Group

Contact Information
561-809-6800
www.insiderthreatdefensegroup.com
jimhenderson@insiderthreatdefensegroup.com
www.nationalinsiderthreatsig.org
jimhenderson@nationalinsiderthreatsig.org