INSIDER THREAT INCIDENTS REPORT
FOR
May 2024

Produced By

National Insider Threat Special Interest Group
Insider Threat Defense Group

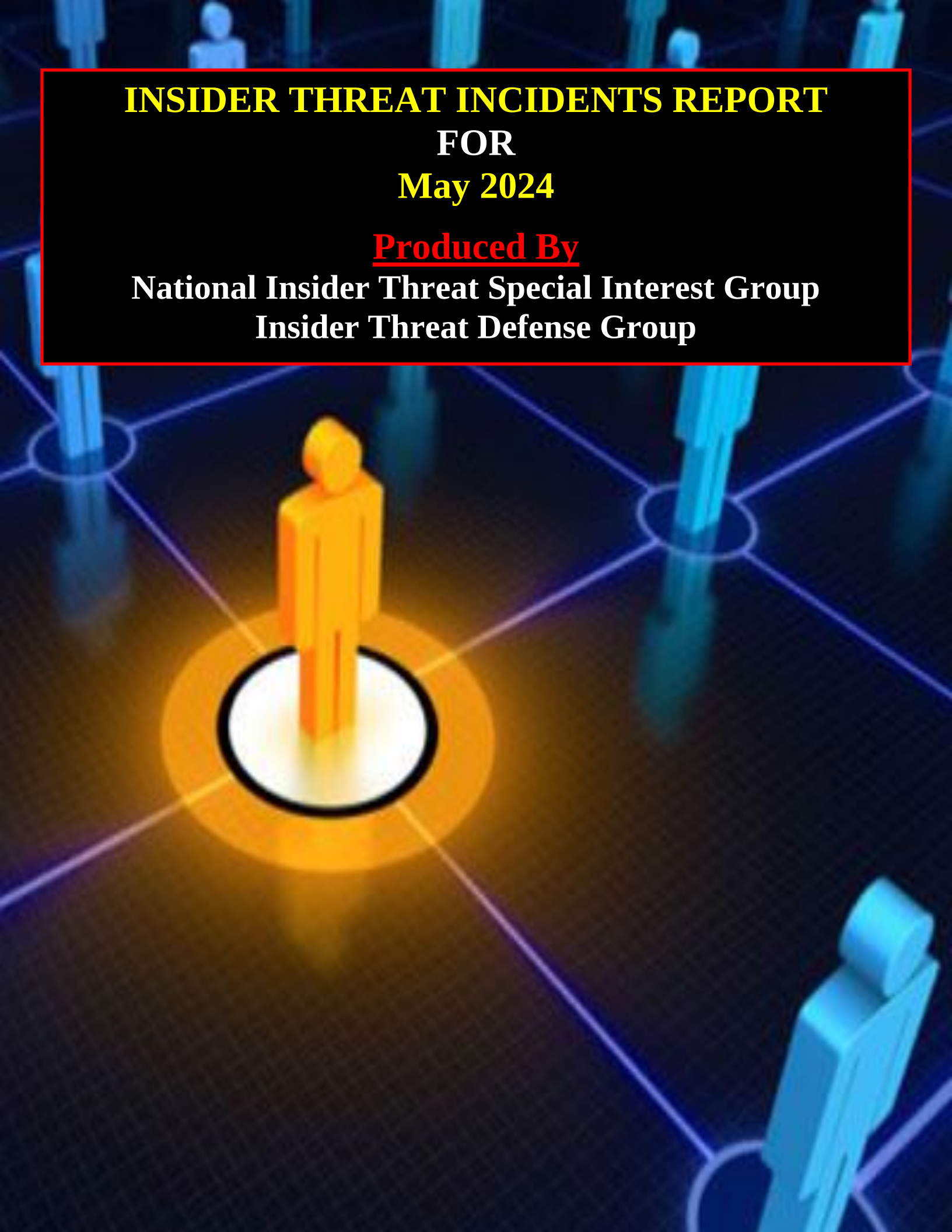

TABLE OF CONTENTS

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 IRM. The incidents listed on pages **4 to 31** of this report provide the justification, return on investment and the funding that is needed for an Insider Risk Management Program. These reports also serve as an excellent Insider Threat Awareness Tool, to educate employees' on the importance of reporting employees' who may pose a risk or threat to the organization.

INSIDER THREAT INCIDENTS
FOR MAY 2024

FOREIGN GOVERNMENTS / BUSINESSES INSIDER THREAT INCIDENTS

No Incidents To Report

U.S. GOVERNMENT

Former U.S. Department Of Agriculture Program Director & Nephew Arrested For $400,000 Fake Contract / Kickback Scheme - May 22, 2024

From August 2015 through November 2022, Kirk Perry, a United States Department of Agriculture (USDA) Program Director, arranged for Jamarea Grant (Perry's Nephew) to be hired by two companies under contract with the USDA Office for Civil Rights. Grant reported directly to Perry, and the two of them conspired to bill the government for work that Grant did not actually perform. Grant is alleged to have received nearly $400,000 for work he did not do, and, in return, kicked back approximately $125,000 to Perry as part of the criminal scheme. (Source)

U.S. Postal Service Supervisor Used USPS Credit Cards To Make $54,000+ In Unauthorized Purchases For Personal Use - May 13, 2024

For approximately six months in 2022 and 2023, Austin Mahan, who worked as a United States Postal Service (USPS) supervisor, misused USPS credit cards to make personal purchases at various retail stores operating in and around New Jersey. These purchases included thousands of dollars' worth of gift cards as well as various home décor items, home renovation materials, power and handheld tools, tool storage equipment, and other personal items. The unauthorized expenses totaled $54,356. (Source)

U.S. Postal Service Mail Carrier Sentenced To Prison For Role In $129,000+ Check Fraud Scheme - May 3, 2024

Alexus Tyson was a United States Postal Service (USPS) Mail Carrier.

Tyson participated in a conspiracy whereby she used her position as a USPS) mail carrier to wrongfully access checks, money orders, and personal mail put into the mail by victims. That information was then used by a co-conspirator, Travis Nnamani, to create counterfeit checks to take money from victims' bank accounts.

Between August 2019 and October, 2020, Tyson assisted Nnamani to create fraudulent checks using victims' personal information that Tyson and others at the USPS took from checks and other documents that victims placed into the mail system. In many instances, checks or other documents mailed by victims were photographed by Tyson or other USPS employees and then the documents were put back into the mail with the victims not knowing their information had been stolen. That information would then be used by Nnamani to create false checks using that information to access funds in victims' bank accounts.

Tyson also played a role as a recruiter of other employees at the USPS to engage in similar conduct, including selling federal stimulus checks they took from the mail. (Source)

U.S. Postal Service Employee Pleads Guilty To Stealing Drug Parcels / Admits To Stealing Packages For 7 Years - May 21, 2024

Nathan Southard was an employee at the Tulare Main Post Office.

On Oct. 19, 2023, Southard stole a parcel from the post office because he believed it contained marijuana and intended to sell it for a profit. Southard admitted that over the past seven years he had stolen parcels worth approximately $50,000. (Source)

Federal Deposit Insurance Corporation Workplace Filled With Sexual Harassment According To Independent Probe - May 7, 2024

The Federal Deposit Insurance Corporation (FDIC) is a workplace rife with sexual harassment and discrimination, an independent investigation recently alleged.

The investigation was commissioned by the FDIC last year after revelations of widespread misconduct came to light via a Wall Street Journal report.

Law firm Cleary Gottlieb spoke with 500 FDIC employees, out of close to 6,000 total, many who recounted experiences of sexual harassment and described widespread fear of retaliation.

Martin J. Gruenberg is the acting Chairman of the FDIC.

According to the report Gruenberg isn't the "root cause of all the workplace issues," the authors note, but "'tone at the top' is important."

Gruenberg also has a reputation for being harsh, demeaning and insulting, they report, which "raises questions about the credibility of the leadership's response to the crisis and the 'moral authority' to lead a cultural transformation." Some lawmakers are already calling for Gruenberg's resignation, including at least one Democrat.

The highly detailed 234 age report is filled with explosive details. "A woman examiner reported on the shock of receiving a picture of an FDIC senior examiner's private parts out of the blue while serving on detail in a field office, only to be told later by others in that field office that she should stay away from him because he had a 'reputation,'" authors of the report wrote.

"A number of employees recounted homophobic statements made by their Field Office Supervisor, including referring to gay men as 'little girls,' resulting in one of them, at least, believing he had to hide that he was gay."

What did Gruenberg, the acting Chairman of the FDIC have to say: "To anyone who experienced sexual harassment or other misconduct at the FDIC, I again want to express how very sorry I am," he wrote to staff ahead of the report's release, per the WSJ. "I also want to apologize for any shortcomings on my part." (Source)

DEPARTMENT OF DEFENSE / INTELLIGENCE COMMUNITY

Largest U.S. Navy Bribery Scandal Involving 1000 Navy Officers / 91 Admirals Is Now Facing Legal Problems For Prosecution - May 23, 2024

Leonard Glenn Francis, better known as "Fat Leonard," is a 6 feet, 3 inch tall, 350 pound former Malaysian defense contractor who bribed hundreds of Navy officers for classified information for more than 20 years. He eventually defrauded the U.S. government and American taxpayers out of at least $35 million dollars until he was caught in a sting operation in 2013. After Francis' arrest, nearly 1,000 Navy officers came under scrutiny, including 91 admirals. Federal prosecutors brought criminal charges against 34 defendants.

In what has become one of the largest scandals in U.S. Navy history, Francis bribed the Navy officers with lavish meals, expensive gifts and orgies.

The officers looked the other way as he grossly overcharged on U.S. Navy contracts for his Singapore-based maritime services supply company, Glenn Defense Marine Asia Ltd., which supplied food, water and fuel to U.S. Navy assets.

A San Diego judge recently dismissed the felony convictions for five military officers who admitted to accepting bribes from Francis. The convictions were dismissed at the request of the government due to "prosecutorial errors."

Francis' bribing did not stop when he was arrested. Later hospitalized and treated for cancer, he convinced the judge to let him go on house arrest to have a more comfortable recovery. In 2022, he cut off his GBS tracker and called an Uber to escape house arrest. He ended up in Tijuana, Mexico, and eventually made his way to Venezuela, where he was captured and sent back to the U.S. in a prisoner swap in December 2023. Prosecutors are waiting until Francis is sentenced to bring charges related to his escape. (Source)

Former CIA Officer Pleads Guilty To Conspiracy To Commit Espionage With China - May 24, 2024

Alexander Yuk Ching Ma, a former Central Intelligence Agency (CIA) officer, pleaded guilty to conspiring to gather and deliver national defense information to the People's Republic of China (PRC).

Ma and a blood relative of his (Identified As Co-Conspirator #1 / CC #1) were naturalized U.S. citizens who were born in Hong Kong and Shanghai, respectively. Both Ma and CC #1 worked for the CIA , CC #1 from 1967 until 1983, Ma from 1982 until 1989. As CIA officers, both men held top secret security clearances that granted them access to sensitive and classified CIA information, and signed non-disclosure agreements that required them to maintain the secrecy of that information.

Ma admitted in the plea agreement, in March 2001, when he no longer worked for the CIA, at the request of intelligence officers employed by the PRC's Shanghai State Security Bureau (SSSB), Ma convinced CC #1 to meet with SSSB intelligence officers in a Hong Kong hotel room. Over the course of three days, Ma and CC #1 provided the SSSB with a large volume of classified U.S. national defense information. At the conclusion of the third day, the SSSB intelligence officers provided CC #1 with $50,000 in cash, which Ma counted. Ma and CC #1 also agreed at that time to continue to assist the SSSB.

In March 2003, while living in Hawaii, Ma applied for a job as a contract linguist in the FBI Honolulu Field Office. The FBI, aware of Ma's ties to PRC intelligence, hired Ma, as part of an investigative plan, to work at an off-site location where his activities could be monitored and his contacts with the PRC investigated. Ma worked for the FBI from August 2004 until October 2012.

Ma further admitted that in February 2006, during this monitored employment by the FBI in Honolulu, Ma convinced CC #1 to provide the identities of at least two individuals depicted in photographs that were provided to Ma by SSSB intelligence officers. The individuals' identities were and remain classified U.S. national defense information. Ma confessed that he knew that this information, and the information communicated in March 2001, would be used to injure the United States or to benefit the PRC, and he deliberately engaged in the criminal conspiracy with CC #1 and the SSSB anyway. (Source)

Former NSA Employee Sentenced To Prison For Attempted Espionage - April 29, 2024

Jareh Dalke pleaded guilty in 2023 to six counts of attempting to transmit classified information to a foreign agent.

From June 6 to July 1, 2022, Dalke was an employee of the National Security Agency (NSA) where he served as an Information Systems Security Designer. Dalke admitted that between August and September 2022, in order to demonstrate both his legitimate access and willingness to share, he used an encrypted email account to transmit excerpts of three classified documents to an individual he believed to be a Russian agent. That person was an FBI online covert employee. All three documents from which the excerpts were taken contained classified as Top Secret / Sensitive Compartmented Information (SCI) and were obtained by Dalke during his employment with the NSA.

On or about Aug. 26, 2022, Dalke requested $85,000 in return for all the information in his possession. Dalke claimed the information would be of value to Russia and told the FBI online covert employee that he would share more information in the future, once he returned to the Washington, D.C. area.

Dalke subsequently arranged to transfer additional classified information in his possession to the purported Russian agent at Union Station in downtown Denver. Using a laptop computer and the instructions provided by the FBI online covert employee, Dalke transferred five files, four of which contained Top Secret information. The other file was a letter, which begins (In Russian & Cyrillic characters) "My friends!" and states, in part, "I am very happy to finally provide this information to you… I look forward to our friendship and shared benefit.

Please let me know if there are desired documents to find and I will try when I return to my main office." The FBI arrested Dalke on Sept. 28, 2023, moments after he transmitted the files. (Source)

Former Defense Contractor Pleads Guilty To Attempted Espionage - April 30, 2024

John Rowe was employed for nearly 40 years as a Test Engineer for multiple cleared defense contractors. In connection with his employment, Rowe held various national security clearances from SECRET to TOP SECRET / SCI and worked on matters relating to U.S. Air Force electronic warfare technology, among other things. After committing a number of security violations and revealing a devout interest in Russian affairs, Rowe was identified as a potential insider threat and terminated from employment.

In March 2020, he met with an undercover FBI agent who was posing as an agent of the Russian government. During this meeting, Rowe disclosed national defense information classified as SECRET that concerned specific operating details of the electronic countermeasure systems used by U.S. military fighter jets, among other things. Over the course of the next eight months, Rowe exchanged over 300 emails with the purported Russian agent, confirming his willingness to work for the Russian government and discussing his knowledge of classified information relating to U.S. national security.

In one email, Rowe explained, "If I can't get a job here then I'll go work for the other team." In another email, Rowe disclosed classified national defense information concerning the U.S. Air Force. In September 2020, Rowe had a second in-person meeting with the undercover FBI agent. During this meeting, Rowe again disclosed classified national defense information. (Source)

U.S. Army Lieutenant Colonel Charged With Arms Export Control Act Violations - May 3, 2024

Frank Talbert is a Lieutenant Colonel with U.S. Army Explosives Ordinance Disposal (EOD) assigned to Fort Campbell.

He is facing federal criminal charges after law enforcement officers conducted an investigation and executed multiple search warrants uncovering evidence that Talbert unlawfully imported firearms parts from Russia and other countries, unlawfully dealt in firearms without a federal firearms license, and committed multiple firearms violations related to the possession of machineguns. (Source)

U.S. Army Major Found Guilty After Smuggling Guns To Ghana - April 29, 2024

A federal jury convicted a United States Army Major (Kojo Dartey), currently assigned to Fort Liberty, on charges of dealing in firearms without a license, delivering firearms without notice to the carrier, smuggling goods from the United States, illegally exporting firearms without a license, making false statements to an agency of the United States, making false declarations before the court, and conspiracy.

Between June 28 and July 2, 2021, Dartey purchased seven firearms in the Fort Liberty area and tasked a U.S. Army Staff Sergeant at Fort Campbell, Kentucky, to purchase three firearms there and send them to Dartey in North Carolina. Dartey then hid all the firearms, including multiple handguns, an AR15, 50-round magazines, suppressors, and a combat shotgun inside blue barrels underneath rice and household goods and smuggled the barrels out of the Port of Baltimore, Maryland, on a container ship to the Port of Tema in Ghana. The Ghana Revenue Authority recovered the firearms and reported the seizure to the DEA attaché in Ghana and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) Baltimore Field Division.

At the same time, Dartey was a witness in the trial of U.S. v. Agyapong. A case that involved a 16-defendant marriage fraud scheme between soldiers on Fort Liberty and foreign nationals from Ghana that Dartey had tipped off officials to. In preparation for the trial, Dartey lied to federal law enforcement about his sexual relationship with a defense witness and lied on the stand and under oath about the relationship. (Source)

Former Veterans Affairs Psychologist Sentenced To Prison For $35,000+ Medicare Fraud Scheme - May 1, 2024

Theresa Kelly was employed in southern Illinois as a Psychologist with the Department of Veterans Affairs.

Kelly engaged in a scheme to defraud Medicare and obtain payment for psychiatric services that she did not provide to residents of a Southern Illinois nursing home between May 2016 and January 2018. In addition to her full-time job at the VA, Kelly owned a company by the name of TS Onsite Mental Health through which she claimed to provide psychotherapy sessions to patients at Shawnee Christian Nursing Center in Herrin, Illinois. Kelly billed Medicare for more than 400 claims, worth more than $54,000, for services that she did not provide. Kelly billed for at least some of the services on days she was on approved medical leave from the VA. Kelly was ordered to repay $35,795.94 in restitution to the Centers for Medicare & Medicaid Services as repayment for her fraudulent claims. (Source)

CRITICAL INFRASTRUCTURE

No Incidents To Report

LAW ENFORCEMENT / PRISONS / FIRST RESPONDERS

U.S. Border Patrol Agent Sentenced To Prison For Attempting To Distribute Methamphetamine & Receiving $100,000+ In Bribes - May 24, 2024

Former U.S. Border Patrol Agent Hector Hernandez admitted that he took bribes to smuggle methamphetamine and people across the U.S.-Mexico border while on duty.

Hernandez acknowledged he took Mexico-based smugglers on a tour of the U.S.-Mexico border, showing them the best locations to sneak unauthorized immigrants into the U.S. He also provided information about the location of monitoring devices and cameras, information only known to him by virtue of his position as a Border Patrol agent. Hernandez admitted that he opened restricted border fences on several occasions to allow people to illegally enter the United States in exchange for cash payments of $5,000 per opening.

According to court records, Hernandez admitted that on May 9, 2023, he met with someone who unbeknownst to him was, in fact, an undercover federal agent, and agreed to pick up a bag full of narcotics that would be hidden near the border fence. Hernandez agreed to pick up the bag while on duty and deliver it to the undercover agent in exchange for $20,000. Once the agreement was made, agents loaded the bag with 10 kilograms of fake methamphetamine, one pound of real methamphetamine, and a tracking device, before placing the bag in a storm drain near the border fence.

Later that evening, Hernandez drove his official vehicle to the storm drain while on duty and retrieved the bag. He drove the bag to his residence in Chula Vista and left the bag there for the remainder of his work shift. On May 10, 2023, after his shift was over, Hernandez returned home, retrieved the bag, and drove to meet with the undercover agent. Upon arrest, agents confirmed that that the bag still contained both the sham and real methamphetamine.

After Hernandez was arrested, agents searched his residence and found $131,717 in cash and 7.7 grams of cocaine. Hernandez admitted at least $110,000 of the cash represented proceeds he received in connection with his narcotics trafficking and bribery activities. (Source)

Former State Police Trooper Sentenced To Prison For Role In $142,000+ Overtime Fraud Scheme - May 1, 2024

William Robertson is a former Massachusetts State Police (MSP) Sergeant.

Robertson was also ordered to pay restitution of $142,774 and forfeit $32,180. I

Co-conspirator former MSP Lieutenant Daniel Griffin was sentenced to five years in prison and three years of supervised release. Griffin was also ordered to pay restitution in the amount of $329,163, a fine in the amount of $176,700, as well as a $2,100 special assessment.

From 2015 through 2018, Griffin, Robertson and other troopers in the Traffic Programs Section at State Police Headquarters, conspired to steal thousands of dollars in federally funded overtime by regularly arriving late to, and leaving early from, overtime shifts funded by grants intended to improve traffic safety.

When the MSP overtime misconduct came to light in 2017 and 2018, Griffin, Robertson and their co-conspirators took steps to avoid detection by shredding and burning records and forms.

After an internal inquiry regarding missing forms, Griffin submitted a memo to his superiors that was designed to mislead them by claiming that missing forms were "inadvertently discarded or misplaced" during office moves. (Source)

Police Officer Pleads Guilty To Role In Drug Distribution Conspiracy - May 1, 2024

Regina McAtee is a former Police Officer for Greensburg, Pennsylvania.

McAtee admitted that she conspired to distribute methamphetamine with former Greensburg Chief of Police Shawn Denning and other drug suppliers. McAtee admitted that she and Denning would order the pills from online suppliers, that McAtee would pay for the pills, and that the pills would be delivered to McAtee's residence. McAtee sold some of the pills back to Denning, who would then distribute the drugs to others. (Source)

STATE / CITY GOVERNMENTS / MAYORS / ELECTED GOVERNMENT OFFICIALS

State Campaign Treasurer Pleads Guilty To Stealing Nearly $1 Million In Campaign Funds From 100 Candidates - May 9, 2024

William Curtis has served as a Campaign Treasurer for more than 100 candidates since the 1980s.

From 2008 until June 2023, Curlis defrauded candidates of approximately $995,231 of campaign funds.

Curlis admitted that he wrote checks from the bank accounts of certain candidates and one PAC to himself for personal use. The defendant transferred funds between campaign accounts without candidates' knowledge to conceal the deficit he created.

For example, from 2000 to 2023, Curlis was the primary signatory on at least 111 bank accounts, and of those, he was the only signatory on 108 accounts. Curlis wrote at least 179 checks to himself from campaign accounts belonging to 18 different candidates and one PAC.

Curlis sold his home in 2016 to cover the cost of campaign expenses, including campaign media costs and account balances, to prevent the discovery of his theft. (Source)

City Councilman Pleads Guilty To Drug Distribution Involving Vape Shops - May 3, 2024

Robert Deming is a Biloxi City Councilman.

In 2019, Deming founded the Candy Shop, LLC to operate Candy Shop stores in Mississippi and North Carolina. The Candy Shop stores sold CBD and vape products.

In 2020, the Mississippi Bureau of Narcotics and Drug Enforcement Administration began investigating the Candy Shop. The investigation revealed that some of the vape products sold by the Candy Shops in Mississippi contained Schedule I controlled substances and controlled substance analogues. In 2022, the DEA also received complaints that some of the products at the Candy Shops were making customers ill.

Agents obtained search warrants for the Candy Shops located in Mississippi and North Carolina. They also obtained a warrant for Deming's residence. During the execution of the search warrants, law enforcement officers seized over $1.8 million in cash from Deming's residence and additional cash and controlled substances from his stores.

As the investigation continued, agents learned that Deming was aware that his vape additives did not contain CBD; rather, they contained synthetic cannabinoids. This was evidenced by group chats in which Deming's employees complained about how the additives were too strong and could hurt their customers. Despite this fact, Deming misbranded the additives as containing CBD.

As part of the plea agreement in this case, Deming agreed to forfeit a yellow Monster Truck with oversized tires and a lift kit and over $1.9 million dollars. His sentencing is scheduled for August 13, 2024. (Source)

SCHOOL SYSTEMS / UNIVERSITIES

Former School Board President Pleads Guilty To Soliciting & Then Stealing Nearly $40,000 Of Donations Intended Scholarship Fund - May 10, 2024

Louis LaPolla served as the Mayor of Utica, New York from 1984 to 1995. He served as President of the Utica City School Board from 2018 to 2022, following 21 years of service as a member of the board.

LaPolla admitted that he set up a scholarship fund in honor of his late wife, Andrea LaPolla, after she passed away in 2018, with the stated intention of benefitting Utica City School District students who planned to pursue post-secondary education in health-related fields. LaPolla further admitted that he received nearly $40,000 in donations intended for the scholarship fund from individuals and businesses and that he spent nearly all the donated money on himself rather than depositing it into the scholarship fund. (Source)

CHURCHES / RELIGIOUS INSTITUTIONS

No Incidents To Report

LABOR UNIONS

Boilermakers Union Chief Of Staff Pleads Guilty To Racketeering Conspiracy For The Misappropriation Of Union Funds - May 23, 2024

Tyler Brown was employed by the Kansas City, Kansas, headquarters of the International Brotherhood of Boilermakers, Iron Ship Builders, Blacksmith, Forgers, and Helpers (Boilermakers Union) as Chief of Staff of the Boilermakers Union and special assistant to the International President of the Boilermakers Union.

From 2013 through October 2022, Brown reported directly to the International President and carried out his directives. Between those dates, Brown was involved in numerous instances of unlawful misappropriation of union funds, including:

1) Purchasing merchandise and hundreds of restaurant meals for the International President and his wife in their hometown that were not necessary to conduct union business or benefit the union or its members.

2) Employing several family members of international officers who received several hundred thousand dollars in salary, reimbursed expenses, unearned vacations, and benefit contributions for minimal or no productive work.

3) Paying for dozens of international trips to Europe, Asia, and Australia for large entourages of international officers and employees of the Boilermakers Union, their families, and outside guests whose travel was not necessary to conduct union business or benefit the union or its members. (Source)

BANKING / FINANCIAL INSTITUTIONS

Former Bank Executive Pleads Guilty To Embezzling $47 Million+ Causing Bank To Collapse - May 23, 2024

Shan Hanes pleaded guilty to using his position as a bank executive to embezzle millions of dollars causing the bank to fail at a complete loss of equity for investors.

Hanes previously served as Chief Executive Efficer (CEO) of Heartland Tri-State Bank (HTSB) in Elkhart, Kansas.

From May 2023 to July 2023 Hanes initiated a series of 10 outgoing wire transfers totaling $47.1 million of Heartland's funds to a cryptocurrency wallet. The funds were transferred to multiple cryptocurrency accounts controlled by unidentified third parties during the time HTSB was insured by the Federal Deposit Insurance Corporation. (Source)

Bank Employee Charged With Stealing $2.1 Million From Customer Accounts - May 8, 2024

Between approximately May 2022 to April 2023, Yue Cao allegedly engaged in a scheme to defraud the Ohio-based bank where he worked, and its customers, by transferring funds from those customers' accounts to ones that Cao controlled, including accounts he had established in the customers' names, all without their knowledge or authorization. He diverted the money stolen from the customer accounts for his personal use.

Cao was a quantitative modeling analyst at the bank and used his position to locate customers who had not yet enrolled in online banking services, primarily targeting elderly customers as identity theft victims. Without the victims' knowledge, Cao created email addresses in their names and enrolled their accounts in online banking without their knowledge. By setting up online banking, he both obtained control of the victims' accounts and ensured that bank statements and other notices about the accounts would be sent to the email addresses he controlled.

Cao then used the victims' personal identifying information to open unauthorized bank accounts and brokerage accounts in their names. Cao used his control of these accounts to set up at least $2.1 million in unauthorized online transfers from the victims' true accounts to the unauthorized accounts he had opened in the victims' names and to Cao's own financial accounts. (Source)

Credit Union Employee Sentenced To Prison For Role In Stealing $2 Million+ From Members' Accounts - May 15, 2024

From 2016 through August of 2019, Jose Prado-Valero served as the Automated Clearing House Coordinator. His duties included posting and coordinating transactions into and out of the accounts of credit union members, which gave him access to members' personally identifiable information, including Social Security numbers, date of birth, home address and telephone numbers. Prado-Valero also had access to members' account numbers and account balances.

Prior to February 14, 2019, Prado-Valero was approached by individuals not employed by the credit union who sought his assistance in conducting a scheme to defraud the financial institution and steal money held in member accounts. The co-conspirators promised to pay Prado-Valero a portion of the fraud proceeds if he stole members' identity and account information.

Prado-Valero agreed to join the scheme and used his position to access members' account information and steal their money.

Between February 14, 2019, and August 16, 2019, Prado-Valero and accomplices successfully made 34 fraudulent transfers to themselves out of credit union members' accounts, in the aggregate amount of $2,078,725. Prado-Valero was paid over $100,000 by his co-conspirators for his role in the scheme. (Source)

Former Bank Vice President Pleads Guilty To $1.5 Million+ Fraud Scheme / Used Funds For Personal Use - May 9, 2024

Stacia Wilson admitted that she created $1,528,321 in false and fictitious loans, using bank customers' information without their knowledge.

Wilson had authority as a loan processor to access and create loans within the bank's computer system. She created numerous false and fictitious loans, then diverted the loan proceeds to her own personal use. Under the terms of today's plea agreement, Wilson must forfeit to the government a money judgment of $1,528,321, which represents the proceeds she obtained as a result of her fraud scheme. (Source)

Mortgage Loan Officer Sentenced To Prison For Embezzling $66,000+ - April 30, 2024

Mackenzie Meggison was employed as a Mortgage Loan Officer at Malvern Bank and was also the Treasurer for the Malvern Area Betterment Association (MABA) who maintained their accounts at Malvern Bank. Using her position at the bank, from July to October, 2020, Meggison conducted 57 unauthorized transactions on four separate MABA accounts totaling at least $66,175.42. (Source)

Former Bank Employee Charged With Stealing & Selling Customer Account Information - April 30, 2024

From about March 30, 2022, until on about August 30, 2023, Kalien Frazier used his position as a Customer Service Representative at a bank, to obtain the account details, debit card details, card verification value (CVV), and personal identifying information of customers. Frazier would ask for this information from customers, even if not required to complete the customer service request, while on recorded customer service calls.

After Frazier had obtained this information, he advertised in group chats that he had bank account information for sale due to his position at a financial institution. When advertising the information for sale, Frazier warned potential customers that they would have to stay under certain monetary thresholds to avoid detection.

Frazier sold or transferred information on hundreds of bank accounts to third parties. As a result of Frazier's scheme, unauthorized electronic payments and transfers were made from hundreds of bank accounts. (Source)

TRADE SECRET & DATA THEFT / THEFT OF PERSONAL IDENTIFIABLE INFORMATION

No Incidents To Report

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

No Incidents To Report

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

U.S. Companies Tricked Into Hiring Over 300+ North Korean IT Workers Who Used Stolen Or Borrowed U.S. Person Identities / DOJ Unveils Complex Fraud Network - May 17, 2024

As if taken from a Hollywood script, the DOJ shared publicly how an Arizona woman and three unidentified foreign nationals placed overseas information technology workers, posing as U.S. citizens and residents in remote positions within U.S. companies. In a nutshell, the quartet put together a scheme where they hoodwinked over 300 companies into hiring North Korean (DPRK) IT workers who used stolen or borrowed U.S. person identities in order to raise hard currency revenue for the DPRK. The scheme ran from at least October 2020 through October 2023.

Separately, yet remarkably similar, the DOJ also shared data concerning the arrest of Ukrainian national, Oleksandr Didenko who ran a years-long scheme creating fake identities on U.S. IT search platforms with U.S. based money service transmitters. Didenko, then sold these accounts to foreign nationals outside the United States who used these identities to apply for jobs. Some of those identities, Didenko advises, were used by the DPRK.

The U.S. citizen, Christina Marie Chapman, identified in the unsealed indictment was arrested on May 15 in Litchfield Park, AZ. Ukrainian citizen Didenko was arrested on May 7 in Poland and the United States is seeking his extradition. There is a $5 million reward for information leading to the arrest of Chapman's three co-conspirators.

According to the DOJ, "The overseas IT workers gained employment at U.S. companies, including at a top-five major television network, a Silicon Valley technology company, an aerospace manufacturer, an American car manufacturer, a luxury retail store, and a U.S.-hallmark media and entertainment company, all of which were Fortune 500 companies."

Chapman ran a "laptop farm" hosting a multitude of IT workers "company issued" computers inside her home. These computers provided the U.S. presence for the "employees" and would then interconnect the overseas IT workers into her home and then via their company issued device into their employer's network. Chapman used her residence to receive checks, correspondence, etc, and charged a monthly fee to the workers for the service. As noted, over 300 companies were impacted and over 60 U.S. identities of U.S. persons were stolen or borrowed. The scheme generated over $6.8 million in revenue for the overseas workers laundered through Chapman's laptop farm. (Source)

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

Former Chief Operating Officer For Hospital Sentenced To Prison For Role With Family In Embezzling $622,000+ - May 1, 2024

Robert Spadondi was an attorney who worked as a Vice President and COO of the hospital.

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

Spadoni obtained approximately $622,500 in payments from the hospital. Spadoni used the money for his own benefit, including restaurant meals and hotel stays, as well as transferring $225,805 into a 401(k) account he controlled. (Source)

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

Bookkeeper For Business Pleads Guilty To Stealing $2.5 Million & Diverting To Funds To Accounts She Controlled - May 16, 2024

Shavonda Chambers was employed as a Bookkeeper for a local business and was apprehended submitting false electronic payroll authorizations to an out-of-state payroll processing company. As a result of her false submissions, Chambers was able to steal and fraudulently divert more than $2.5 million dollars from her employer to financial accounts she controlled. (Source)

Former Cyber Security Consultant Arrested For $1.5 Million Extortion Scheme Against IT Company After Being Terminated - May 1, 2024

Vincent Cannady was assigned by a staffing company to work on an engagement with the victim company.

Under the engagement, Cannady's responsibilities included assessing and remediating potential vulnerabilities that an unauthorized party could use to access the victim's information systems.

As a result, Cannady had access to the victim company's sensitive and proprietary information. After about a year, Cannady's engagement was terminated. Days after, and while he still had access to the company's information, Cannady
downloaded the company's sensitive and proprietary information without its authorization and uploaded the information to a personal cloud storage account.

Cannady then demanded that the company settle unspecified discrimination and emotional distress claims. He threatened to "upload all of the documents in his possession immediately once the case is filed" if the company did not settle his claims for $1.5 million. He added, "As we all know those documents will imperil the company's reputation and shake investor confidence."

He specifically demanded "a 10 year Certificate of Deposit for 1.5 million dollars," which would "buy an attestation that all files destroyed by me and a gag order preventing me from ever talking about what I saw or the documents I had in my possession or the documents I had created at [the company] or downloaded." (Source)

Individual Charged For Using Non-Public Information From Employee For Stock Trading Purposes That Netted Him $823,000+ - May 10, 2024

Frank Poerio used sensitive, material non-public information (MNPI) obtained from a Dick's Sporting Goods employee to engage in nearly 200 trades of the company's securities on the New York Stock Exchange, including the purchase of individual shares and call option contracts.

The trading allegedly occurred between August 2019 and May 2021 when the insider worked in a data analytics role at the company's corporate offices in Moon Township, Pennsylvania. The trades allegedly netted approximately $823,000 in profit for Poerio. As alleged, Poerio knew the Dick's employee and spoke often with the employee about finances and investing. Several of the alleged trading incidents occurred in the days immediately preceding Dick's release of periodic earnings statements—so called "blackout" periods, when Dick's employees were prohibited from trading in the company's securities. (Source)

Employee Admits To $487,000+ Overtime Fraud Scheme - April 30, 2024

From January 2018 through April 2020, Joseph Ferrara submitted fraudulent claims for compensation related to work performed on the Hudson Bergen Light Rail (HBLR) Projects on which he had worked as an employee of a subcontractor specializing in electrical work.

The HBLR maintains approximately two dozen stations throughout Hudson County and serves more than 50,000 passengers each weekday. Ferrara, who supervised numerous workers on HBLR projects, was compensated at a regular rate for normal workday hours, at an elevated overtime rate for work performed during non-regular weekday hours and Saturdays, and at a double time rate for work performed on Sundays.

During a more than two-year period, Ferrara submitted claims for compensation covering hundreds of hours relating to work allegedly performed during regular, overtime and double time hours knowing that he had not actually performed that work for his employer or on HBLR projects. For example, Ferrara admitted that he spent approximately 10 days vacationing in Florida in both late December 2018 and late December 2019 during which he performed no work for his employer or upon HBLR projects. Nevertheless, Ferrara submitted fraudulent claims representing that he had worked more than 200 hours at regular, overtime and double time rates during those periods. In total, Ferrara admitted to receiving $487,899 in compensation for hours during which he performed no work. As part of his plea agreement, Ferrara agreed to forfeit this amount. (Source)

Company Bookkeeper Pleads Guilty To Stealing $120,000+ - May 3, 2024

Mary Katicich used her position as Bookkeeper with J&J Diving Corporationm to fraudulently divert funds to her benefit from the company's Regions Bank account. Further, Katicich willfully filed a tax return for tax year 2016 that she did not believe to be true and correct because it failed to report approximately $120,190.58 of income. (Source)

Bookkeeper For Funeral Home Pleads Guilty To Embezzling $50,000+ - May 21. 2024

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

Starting in 2015, and continuing until it was discovered in January 2023, Simmons employed a scheme to embezzle funds from the company. On more than 100 occasions, she either made unauthorized wire transfers of funds from the funeral home's bank account to her own account, or drafted unauthorized checks which she deposited by electronic wire transfer into her own account. She would often describe these checks as "commissions" or "consulting fees." She embezzled more than $500,000 over the course of the scheme. (Source)

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

Employee Sentenced To Prison For Role In $12 Million Dollar Insider Trading Ring / Used Funds To Buy Homes - May 21, 2024

Through his employment at TIAA-CREF, Lawrence Billimek had advance access to certain of TIAA-CREF's anticipated trades. Due to the size of certain of these TIAA-CREF trade orders, they often caused market movement in the securities they traded. From at least 2016 through his arrest in December 2022, Billimek abused his insider access and provided inside information about these trades to his co-conspirator (CC-1) who then bought or sold the same securities in advance of the TIAA-CREF trading. CC-1 then provided Billimek with a portion of the profits on these trades.

Billimek and CC-1 engaged in these front-running trades on over a thousand occasions between in or about 2016 and December 2022.

In an effort to hide their scheme, Billimek used prepaid, unregistered "burner" phones to communicate with CC-1 throughout the trading day. Billimek and CC-1 also lied to various financial institutions about the source of funds they received during the scheme, claiming that they were, among other things, gifts. In total, Billimek and CC-1 generated tens of millions of dollars in profits. Billimek bought multiple homes and funded an active social lifestyle through the proceeds of his criminal scheme.

In addition to a prison term, BILLIMEK, 52, of Hailey, Idaho, was sentenced to three years of supervised release and ordered to pay forfeiture of $12,249,000. (Source)

Diversity Program Manager For Facebook & Nike STP For Role In Stealing $4.9 Million+ / Used Funds To Live Luxury Lifestyle - May 13, 2024

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

Smiles used her position at Facebook to cheat and defraud the company. She caused Facebook to pay numerous individuals for goods and services that were never provided and then directed those individuals to kick back the fraudulent proceeds to her, often in cash.

Smiles recruited numerous individuals to participate in the scheme. These individuals included friends, relatives, former interns from a prior job, nannies and babysitters, a hair stylist, and her university tutor. She also caused Facebook to make payments for her benefit to others who did not pay kickbacks. For example, Furlow-Smiles caused Facebook to pay nearly $10,000 to an artist for specialty portraits and more than $18,000 to a preschool for tuition.

As she had done at Facebook, Smiles circumvented the vendor process at Nike to commit fraud. She linked her Nike corporate card to her PayPal and Venmo accounts. She then paid her associates with PayPal and Venmo, causing fraudulent charges to her Nike card. The associates kicked back portions of the payments to Smiles, who submitted fraudulent expense reports to Nike to cover her tracks. The expense reports falsely claimed that the payments were related to the Juneteenth event.

In total, Furlow-Smiles stole more than $4.9 million from Facebook and over $120,000 from Nike based on fictitious charges and fraudulent invoices. She used the money to fund a luxury lifestyle in California, Georgia, and Oregon. (Source)

Construction Company Project Supervisor Charged For Defrauding His Employer Of $920,000+ / Used Funds For Personal Use - May 17, 2024

Jonathan McCormack was employed as a Project Supervisor for BluRoc, LLC., a construction company based in Northampton, Mass. McCormack also owned and operated JDM Site Services, LLC (JDM), a Michigan-based company that heavy rented equipment to BluRoc.

Between January 2019 through January 2021, McCormack devised a scheme to defraud BluRoc by various means, including submitting materially false JDM invoices for purported equipment usage and by diverting BluRoc labor, equipment and materials for his own personal use and benefit.

McCormack allegedly entered fraudulent employee time and JDM equipment usage data in BluRoc's tracking system that overstated both the number of hours the employees, including himself, were working on BluRoc projects as well as the number of hours JDM equipment was actually used. McCormack emailed false JDM invoices to BluRoc personnel for inflated amounts that substantially overstated the number of hours the equipment was actually used. McCormack deposited payments received for these false invoices into a JDM bank account and used the proceeds for his own personal use and benefit – including to purchase and renovate a luxury hunting lodge; make improvements to his personal residence; purchase recreational vehicles including snowmobiles; and repay a loan to his uncle.

Lastly, McCormack allegedly directed BluRoc workers to conduct work at the luxury hunting lodge he purchased, including clearing an area between the lodge and an adjacent property owned by his uncle; laying timber mats that McCormack had stolen from a BluRoc worksite; and haying and seeding the area with material that he had also stolen from a BluRoc worksite. McCormack then allegedly electronically approved the workers' time and equipment usage in BluRoc's tracking system – so that BluRoc, rather than McCormack, paid for their work.

In addition to the charges, the indictment seeks forfeiture of $920,716, the hunting lodge and six Polaris recreational vehicles. (Source)

Office Manager Charged With Embezzling $650,000+ From Medical Practice / Used Funds For Personal / Family Enrichment - May 1, 2024

Kathleen Libby was a former Office Manager at medical practice. She embezzled $650,000+ over several years.

Libby stole from the medical practice in a variety of ways, including by transferring funds from the practice to a personal PayPal account she established named "Medline Surgical Supplies." In doing so, Libby allegedly created the false impression that transfers from the medical practice to the PayPal account were expenses the medical practice had incurred for supplies.

Libby used the medical practice's bank account to make payments toward purchases she had made at a variety of retailers, including Louis Vuitton, Bloomingdales, Best Buy, Target and travel-related websites. The charging documents also allege that Libby placed two of her relatives on the medical practice's payroll and used its credit cards for her own personal benefit. (Source)

Former Air Lines Office Manager Sentenced To Prison For Embezzling $600,000+ / Used Funds For Personal Use - May 6, 2024

Beginning in September 2015 and continuing until December of 2018, Sung Hwang engaged in a scheme to defraud his employer and to embezzle over $600,000.00. Hwang was an administrator in the Korean Air Lines (KAL) Guam office at the Guam International Airport (GIA).

As an administrator at the Guam KAL office, Hwang's duties included reporting the number of passengers and paying the corresponding Passenger Facility Charge (PFC), procuring, and paying for other office supplies and services, and acting as one of two co-signatories on KAL Guam's business checking account at the Bank of Guam.

Hwang underreported the PFC owed to GIA and kept the difference between the actual PFC owed and the PFC paid for himself. Over the course of the three-year scheme Defendant Hwang deposited over $3.5 million in KAL funds into his personal bank account and diverted over $600,000.00 in KAL funds to his own personal use. (Source)

Employee Charged With Embezzling $440,000+ From 2 Different Employers / Used Funds To Make Payments For Credit Cards & Auto Loan - May 8, 2024

Between September 2017 and April 2020, Jasmyne Botelho stole at least $280,000 from her employer. Specifically, it is alleged that Botelho directed payments purportedly intended for the company's vendors to bank accounts she controlled and used company funds to make payments on personal credit cards and an auto loan. To hide her scheme, Botelho allegedly falsified her employer's books and records to make it appear as though the payments had in fact been sent to legitimate vendors rather than to Botelho.

It is further alleged that, between May 2022 and December 2023, Botelho improperly inflated her payroll from another employer by more than $160,000. Botelho allegedly concealed her scheme by manipulating her employer's payroll and accounting software to hide her inflated payroll as well as phony "reimbursements" she paid herself. (Source)

Office Manager Sentenced To Prison For Embezzling $250,000 / Used Funds For Gambling - May 6, 2024

Teresa Chiappone admitted she had worked as the Office Manager for a small business since 2014.

Between September 2020 and September 2022, Chiappone embezzled approximately $250,000 from the small business. Chiappone abused her position of trust at the small business to write over $160,000 in unauthorized checks drawn on the small business's bank account for her own benefit.

Chiappone also intercepted at least $50,000 in cash deposits, and she made no less than $3,000 in unauthorized credit card charges. Chiappone gambled away thousands of the small business's moneys at Iowa casinos. As a result of the fraud, the small business had to take out a loan to cover its losses, contract with a local accounting firm to conduct a forensic audit, and max out its line of credit at a local bank. (Source)

Office Manager For Real Estate Sentenced To Prison For Stealing $250,000+ For Personal Use - May 14, 2024

A real estate company started an investigation after a missing cash deposit led to the discovery of discrepancies in their financial records.

FBI investigators determined that Tabitha Dobi, the company's Office Manager for four years, used her position to steal cash deposits intended for the company's property rentals, then manipulating the company's accounting system to conceal the thefts.

Dobi also instructed one rental tenant to pay her directly through an online payment app and used the money for her personal benefit, and allowed friends to stay at the company's rental properties without charge and without the company's authorization. As a result of those schemes, the company lost $251,569. (Source)

Employee Extradited From Scotland To Face Charges Of Embezzling $165,000 From Employer / Used Fund For Luxury Lifestyle - May 3, 2024

Sarah Tweedie previously worked as a controller of a St. Louis area publishing company. She was responsible for payroll processing, expense reimbursements and paying all company bills, including company credit cards.

From July through January of 2018, Tweedie stole from her employer in multiple ways. She used her company credit card and a card belonging to a former employee to make $138,137 in purchases, a Scottish kilt and a $1,239 premium seat upgrade on her flight from Chicago to Glasgow. She used the corporate account to purchase $6,400 in Amazon gift cards.

Tweedie also fraudulently increased her annual salary from $80,000 to $110,000 and triggered $16,086 in expense reimbursements to which she was not entitled.

Tweedie began a long-distance relationship with a Scottish man in 2015, according to extradition documents, and they became engaged in March of 2017, the month before she began working for the publishing company.

A motion seeking to have Tweedie held in jail until trial says she told her employer in December of 2017 that her fiancée had been injured in a car accident and that she needed to leave to be with him. In reality, Tweedie had applied for and received a visa to live in Scotland and did not plan to return. She was arrested on July 9, 2019, but fought extradition. In March her final appeal was denied and United States Marshals escorted her to St. Louis. (Source)

SHELL COMPANIES / FAKE OR FRAUDULENT INVOICE BILLING SCHEMES

Outside Individual Found Guilty For Role In Defrauding Company Out Of $5.8 Million Using Fake Invoice Scheme For 18 Years / Was In Collusion With IT Director - May 14, 2024

From February 2000 to April 2018, Kevin Horton schemed with Tony Rawlings, the Information Technology (IT) Director at Melissa's World Variety Produce Inc., to defraud Melissa's out of its money through the approval of payment of invoices for IT services that were never provided.

Horton created a shell company called Creative Network Solutions (CNS), whose purpose was to send fraudulent bills to its sole client, Melissa's. In consultation with Rawlings, Horton created two fictitious invoices per month, in which CNS billed Melissa's for IT services that CNS did not provide, for approximately 18 years, through February 2018.

Horton provided the fictitious invoices to Rawlings, who approved them, vouched for their operational necessity, and then forwarded them to a Melissa's executive who was asked to have Melissa's pay CNS the amounts listed on the sham invoices.

Horton, along with Rawlings, caused Melissa's to send CNS payment in the form of checks mailed through the U.S. Mail to a post office box to which Horton had sole access. Horton deposited the checks he received through the scheme into a bank account that he exclusively controlled. Horton then funneled Rawlings a portion of the money that Melissa's paid to CNS, in the form of checks sent via U.S. Mail to addresses where Rawlings lived.

In total, Horton, along with Rawlings, caused Melissa's to pay CNS approximately $5,852,604 because of the fictitious invoices. (Source)

Two Former Executives Sentenced To Prison For Roles In $4 Million+ Fake Vendor - Invoice Scheme - April 30, 2024

Shawn Rains and Joseph Maharaj were sentenced to prison, for their participation in a scheme to steal millions of dollars from a company where they were formerly high-ranking executives.

Rains and Maharaj designed and executed a scheme to defraud OrthoNet of over $4 million and to launder the fraud proceeds. Rains and Maharaj conspired with others to create fake vendors that purported to do work on behalf of OrthoNet. Rains, Maharaj and their co-conspirators then signed invoices approving payment for the fake work, and OrthoNet sent payments to the fake vendors.

Rains, Maharaj and their co-conspirators then converted the money to cash to hide the source of the fraud proceeds and split it up amongst themselves. (Source)

Salesman For IT Company Sentenced To Prison For Embezzling $700,000 Using Fake Invoice Scheme - May 13, 2024

Thomas Syddall was a salesman for Information Technology Corporation.

From about March 2020 to about August 2021 in Helena, Syddall embezzled money through multiple means, including creating bogus purchase orders and invoices, stealing inventory and directing payments to fictitious companies and unauthorized vendors. Syddall then sold the inventory, none of which was authorized, on eBay and KSL Classifieds. When questioned by other employees about the discrepancies in orders and payments, Syddall sent lulling emails attempting to cover up and prolong the fraud. Syddall concealed financial transactions by laundering proceeds from the wire fraud into third-party accounts.

Syddall then directed the transfer of the money into accounts over which he had control. Syddall must pay approximately $700,000 in restitution. (Source)

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

No Incidents To Report

THEFT OF ORGANIZATIONS ASSESTS

Former Augusta National Golf Club Employee Pleads Guilty To Stealing Gold Tournament Memorabilia For 13 Years & Selling To Online Broker For $5.3 Million - May 15, 2024

Richard Globensky is a former warehouse coordinator at Augusta National who was in charge of overseeing the vast array of Masters merchandise and memorabilia sold annually.

Globensky admitted he repeatedly stole the merchandise and memorabilia from 2009 to 2022. The merchandise included Masters shirts, hats, flags, watches, and other goods, while the memorabilia included historically significant items such as the Green Jackets won by Arnold Palmer, Gene Sarazen, and Ben Hogan, and documents and letters written and signed by Bobby Jones. Globensky sold the merchandise to the online broker in Florida for a total of approximately $5.3 million. He sold the historically significant memorabilia to the same broker, as well as to the broker's associate, for nearly $300,000, the plea agreement states. (Source)

EMPLOYEE COLLUSION (WORKING WITH INTERAL OR EXTERNAL ACCOMPLICES)

No Incidents To Report

EMPLOYEE DRUG RELATED INCIDENTS

4 Flight Attendants Charged In Connection With Smuggling $8 Million In Drug Money To The Dominican Republic - May 8, 2024

4 flights attendants are being charged with various offenses in connection with their years-long participation in smuggling narcotics trafficking proceeds from the United States to the Dominican Republic on commercial flights.

Homeland Security Investigations Special Agent in Charge Ivan Arvelo said: "As alleged, the defendants knowingly smuggled large amounts of illicit money linked to the sale of narcotics, to include fentanyl, and took

advantage of airport security checkpoints by using their trusted positions as flight attendants. This investigation has exposed critical vulnerabilities in the airline security industry and has illuminated methods that narcotics traffickers are utilizing.

All of the defendants were employed as flight attendants with different international airlines that operated routes between New York City and the Dominican Republic. All of the defendants had "Known Crewmember" ("KCM") status with the Transportation Security Administration, which allowed them to pass through a special security lane at John F. Kennedy International Airport and other airports with less scrutiny than normal passengers. In total, the defendants smuggled approximately $8 million in bulk cash from the United States to the Dominican Republic. (Source)

Flight Attendant & 2 Bank Employees Charged In Mexico Drug Trafficking Organization Involving 15 Other Individuals - May 21, 2024

A flight attendant and two bank employees in Indiana have been charged in a federal indictment that accuses a Mexico-based drug trafficking organization of moving thousands of kilograms of cocaine into the United States and laundering tens of millions of dollars in proceeds. 15 other individuals have previously been charged.

Flight attendant Glenis Zapata is charged with assisting the traffickers in the transportation of drug proceeds on commercial airline flights. Zapata possessed a "Known Crew Member" badge and used her authority to help the traffickers move cash drug proceeds from the Midwest to the southern part of the U.S. and into Mexico. The traffickers also allegedly used other means to ship the money, including semi-trailer trucks and a private charter airplane that was seized by federal authorities in 2021 at the Gary / Chicago International Airport in Gary, Ind.

The two bank employees Ilenis Zapata and Georgina Banuelos helped launder the drug proceeds by exchanging lower denominated bills for higher denominated bills. Ilenis Zapata and Banuelos, who worked together at a bank in Lafayette, Ind., also knowingly and willfully failed to file currency reports for the transactions, as required under federal law, the indictment states.

The superseding indictment added Glenis Zapata, Ilenis Zapata, and Banuelos as defendants and renewed conspiracy and money laundering charges previously filed against 15 others, including the alleged leader of the drug trafficking organization, OSWALDO ESPINOSA, 41, of Mexico; the organization's primary manager, JORGE BORBON-OCHOA, 46, of Mexico; and the head of its Chicago operations, RICARDO TELLO, 37, of Mission, Texas.

Espinosa's organization allegedly transported the cocaine in wholesale quantities from Mexico to various U.S. cities, including Chicago, from 2018 to 2023. The traffickers used warehouses, garages, and stash houses in Chicago to receive and store the cocaine and cash, the indictment states. (Source)

OTHER FORMS OF INSIDER THREATS
No Incidents To Report

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'
No Incidents To Report

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 (**5,000+ 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 Is Our Business

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